Individual or group. (131 Responses)
Name (86 Responses)
Organization (86 Responses)
Group Name (45 Responses)
Lead Contact (45 Responses)
Question 1 (119 Responses)
Question 1 Comments (131 Responses)
Question 2 (123 Responses)
Question 2 Comments (131 Responses)
Question 3 (120 Responses)
Question 3 Comments (131 Responses)
Question 4 (110 Responses)
Question 4 Comments (131 Responses)
Question 5 (93 Responses)
Question 5 Comments (131 Responses)
Question 6 (110 Responses)
Question 6 Comments (131 Responses)
Question 7 (114 Responses)
Question 7 Comments (131 Responses)
Question 8 (111 Responses)
Question 8 Comments (131 Responses)
Question 9 (114 Responses)
Question 9 Comments (131 Responses)
Question 10 (113 Responses)
Question 10 Comments (131 Responses)
Question 11 (115 Responses)
Question 11 Comments (131 Responses)
Question 12 (92 Responses)
Question 12 Comments (131 Responses)
Question 13 (115 Responses)
Question 12 Comments (131 Responses)
Question 14 (112 Responses)
Question 14 Comments (131 Responses)
Question 15 (110 Responses)
Question 15 Comments (131 Responses)
Question 16 (112 Responses)
Question 16 Comments (131 Responses)
Question 17 (109 Responses)
Question 17 Comments (131 Responses)
Question 18 (114 Responses)
Question 18 Comments (131 Responses)
Question 19 (120 Responses)
Question 19 Comments (131 Responses)
Question 20 (92 Responses)
Question 20 Comments (131 Responses)
Question 21 (109 Responses)
Question 21 Comments (131 Responses)
Question 22 (104 Responses)
Question 22 Comments (131 Responses)
Question 23 (84 Responses)
Question 23 Comments (131 Responses)
Question 24 (119 Responses)
Question 24 Comments (131 Responses)
Question 25 (105 Responses)
Question 25 Comments (131 Responses)
Question 26 (108 Responses)
Question 26 Comments (131 Responses)
Question 27 (90 Responses)

Question 27 Comments (131 Responses)
Question 28 (108 Responses)
Question 28 Comments (131 Responses)
Question 29 (110 Responses)
Question 29 Comments (131 Responses)
Question 30 (107 Responses)
Question 30 Comments (131 Responses)
Question 31 (109 Responses)
Question 31 Comments (131 Responses)
Question 32 (114 Responses)
Question 32 Comments (131 Responses)
Question 33 (89 Responses)
Question 33 Comments (131 Responses)
Question 34 (109 Responses)
Question 34 Comments (131 Responses)
Question 35 (110 Responses)
Question 35 Comments (131 Responses)
Question 36 (111 Responses)
Question 36 Comments (131 Responses)
Question 37 (88 Responses)
Question 37 Comments (131 Responses)
Question 38 (108 Responses)
Question 38 Comments (131 Responses)
Question 39 (108 Responses)
Question 39 Comments (131 Responses)
Question 40 (109 Responses)
Question 40 Comments (131 Responses)
Question 41 (86 Responses)
Question 41 Comments (131 Responses)
Question 42 (111 Responses)
Question 42 Comments (131 Responses)
Question 43 (101 Responses)
Question 43 Comments (131 Responses)
Question 44 (112 Responses)
Question 44 Comments (131 Responses)
Question 45 (86 Responses)
Question 45 Comments (131 Responses)
Question 46 (106 Responses)
Question 46 Comments (131 Responses)
Question 47 (101 Responses)
Question 47 Comments (131 Responses)
Question 48 (85 Responses)
Question 48 Comments (131 Responses)
Question 49 (104 Responses)
Question 49 Comments (131 Responses)

Individual
Doug Peterchuck
Omaha Public Power District
Yes
Definition Concerns: 1. BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. Please define or clarify the term “adversely”. Requesting clarification or suggest just using impact. Term “adversely” is subject to interpretation. 2. BES Cyber Security Incident: The term “suspicious” is open to interpretation and very vague. Suggest rewording to “intentional malicious act”. 3. Control Center: As defined, control

centers are as follows: one or more facilities “Hosting” a set of one or more BES Cyber Assets OR BES Cyber Systems performing one or more of the following functions that supports real-time operations by System Operations for two or more BES Generation facilities or transmission facilities, at two or more locations. While the definition of entities control centers (e.g., control centers monitoring and controlling generation and transmission facilities) are being interpreted by this definition, the control room for generation facilities could be interpreted to adhere to the same CIP standard requirements. Requesting a clear interpretation of control center, with examples for CEA’s and entities or a clear definition of generation control rooms and the separation of the two definitions in relation to CIP v5 standards. 4. Cyber Assets: Programmable electronic devices, including the hardware, software, and data in those devices. Does programmable devices include legacy Remote Terminal Units (RTU's) with eeproms? Some may not consider them as Cyber Assets. Because not all industrial devices are IT based, suggest thorough research be performed within the industry before declaring specific devices.
Yes
CIP-002-5: Attachment 1: Medium Impact Rating; 2.13: Clarification needed within the definition of (2) Generation control centers that control 300MW or more of generation. As stated within question one of this document, the definition of control center and generation control room needs to be defined separately. Entities and Compliance Enforcement Authority (CEA’s) are interpreting no difference in control centers and generation control rooms.
Yes
Yes
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes
Yes
Yes
Yes
Yes
Yes
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes
No
CIP-004-5 R2: Requirement 2.10: Role based training on the BES Cyber System’s interconnectivity and interoperability with other cyber systems. The understanding of this requirement is to perform annual training to those entities interdepartmental personnel who are responsible for implementing, maintaining and securing the interconnectivity and interoperability BES impacted networks. Many mid-range to small entities that will be impacted by CIPv5 have small internal departments controlling the CIP networks. The reality of performing training on personnel whom maintain the systems is very confusing, time consuming and redundant. Establishing training for those individuals who are so involved with the infrastructure or protecting the asset seems ineffective in protecting the reliability of

a BES Cyber System.
Yes
Yes
Yes
Yes
No
While understanding the justification of minimizing the risk scope and implementing logic from NIST 800-53 version 3 segments, clarification is needed for all requirements within CIP-004-5.R7. For example, R7.1 – HIGH & MED asset designation- individuals who resign or are terminated must have revocation of unescorted physical access and interactive remote access to BES Cyber Systems at the time of the resignation or termination. Request a sufficient timeframe (e.g., xxxx hours to complete the access revocation of physical and remote access) as entities processes may adhere to the standard, however, the phrase “at the time of the resignation or termination” is subject to interpretation. CIP-004-5.R7.2 – HIGH & MED asset designation – For reassignments or transfers, revoke the individuals unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day. Request a longer timeframe to complete the task of having a full assessment for reassignments or transfers. Recommend seven days for reassignments and transfers as too many variables may inhibit next calendar day completion.
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
No
CIP-005-3 Requirement 1.1: Define technical and procedural controls to restrict unauthorized electronic access. With entities identifying assets High, Medium and Low, anticipation of many BES Cyber system assets being categorized as low should be considered when establishing criteria which are enforced. Assets that are categorized as Low could be into the thousands for any registered entity. Resources could be allotted toward High and Medium BES Cyber Systems as opposed to Low categorized BES Cyber Systems. CIP-005-3 Requirement 1.5: A documented method for detecting malicious communications at each EAP. The implementation of IDS systems at each identified ESP (internal and external), along with current security methods of deterring malicious intent seems to be extensive and very costly to entities. Recommend a re-write of the requirements to “a documented method for deterring malicious communications at each EAP”. Otherwise, if IDS is absolutely required, please consider IDS implementation on external outbound EAP’s. Internally identified EAP’s located within DBP’s, already enforced with ACL’s and logging should not be subjected to IDS implementation.
No
CIP-005-5 Requirement 2.2: Require encryption for all interactive remote access sessions to protect the confidentiality and integrity of each interactive remote access session. One element that needs to be addressed is contracts with the various service vendors and contractors that maintain systems from remote locations. Current contracts from vendor to owner have established terms and conditions that could negate the contact and void the service agreements. Also, if entities are utilizing vendor support to maintain a deemed BES Cyber System, how can entities implement encryption into vendor network, all the way to vendor end point (console)? Clarification is needed on where encryption needs to start and stop accordingly.
No
While it’s completely understandable the VSL’s are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL’s for all requirements.
Yes

Yes
No
CIP-006-5 Requirement 3.2: Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year. Clarification on the term “outage” is needed. If outage is referring to downtime that was unwarranted or unscheduled; suggest “maintenance and /or unscheduled operational downtime”.
Yes
Commend SDT on developing VSL’s for all categories.
No
CIP-007-5 Requirement 1.2: Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. Requirement itself is too vaguely written, subject to interpretation. Request clarifications on the following terms: “console commands” and “signage” used in the measures section. Entities may have difficulty disabling or restricting the use of unnecessary physical input/output ports used for console commands, as multiple operating systems are being utilized throughout the industry, not just Microsoft. Due to the Stuxnet vulnerability, entities must be proactive and protect themselves by disabling the removable media ports (USB), however, restricting and disabling physical ports for console commands (basically serial ports), is not exactly logical.
No
CIP-007-5 Requirement 2.3: A process of remediation, including any exceptions for CIP exceptional Circumstances. Recommend changing the term “remediation” to “mitigation” this change will cause less ambiguity and will be consistent with terminology currently established. Also, measurements for compliance seem to exceed the requirements. Entities are performing these tasks (measures) on a monthly basis in conjunction to their security patch management programs. The current list of measure to meet this specific requirement does not improve security or the reliability of the BES Cyber Systems or BES Cyber Assets. Recommend scaling down the measures.
No
CIP007-5 Requirement 3.1: Deploy method(s) to deter, detect or prevent malicious code. Recommend re-wording the requirement as it’s subject to interpretation. Entities and CAE’s alike, view this requirement as a “either or” statement. Recommend utilizing “where technically feasible” as not all BES Cyber Systems are designated as computers utilizing Microsoft technology, (e.g., relay’s, PLC’s, Controllers, etc.) CIP-007-5 Requirement 3.1 through 3.4: Unfortunately, the manufactures that have developed industry hardware and some software do not view malicious software to be a legit issue. Recommend adding “where technically feasible” to requirement. Substation relays, Programmable Logic Controllers (PLC’s), Printers, controllers, controller cards, etc. are a few examples that cannot adhere to the malicious software requirements. TFE’s will be abundant.
No
CIP-007-5 Requirement 4.1: Measures: Evidence may include, but not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. Recommend redefining measures as UNIX systems and other systems outside of Microsoft environment do not have “event classes”. CIP-007-5 Requirement 4.1.1: Any detected failed access attempts at Electronic Access Points. Request implementing this requirement within CIP-005-5; Separating EAP and BES Cyber System requirements is essential and adds clarity within the requirements. Previous NERC CIP revisions failed to separate requirements which led to more confusion. CIP-007-5 Requirement 4.3: Detect and activate a response to event logging failures before the end of the next calendar day. Clarification needed on this specific requirement; is it the expectation of automated detection? If so, from a technical standpoint, not all operating systems are capable of detection of failed logging. Entities would have a real hard time meeting compliance with this requirement. CIP-007-5 Requirement 4.5 – HIGH asset designation: Review a summarization of sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. Clarification needed for the term ‘summarization of logs’.
No

CIP-007-5 Requirement 5.4: Procedural controls for initially changing default passwords. Recommend the enforcement of the requirement be established for designated high and medium BES Cyber systems as low assets will be in the thousands requiring maximum resources protecting assets (LOW) that do not affect BES as established High and Medium BES Cyber Assets.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
Yes
No
CIP-008-5 Requirement 2.1: The incident response plans must be used when incidents occur and include recordings of deviations taken from the plan during the incident or test. The requirement to record the "deviations" from the incident response plans offers no significant improvement in the reliability of the BES Cyber Assets or BES Cyber Systems. This can be documented within the entities internal processes as lessons learned. Deviations can be a subject to an interpretation by CEA's.
No
CIP-008-5 Requirement 3.2, 3.4, 3.5: Recommend adjusting the time frame from 30 days on 3.2, 3.4 and 3.5 to match Requirement 3.3, 60 days. Unified representation adds clarity.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIP-009-5 Requirement 1.4: Backup media shall be verified initially after backup to ensure that the backup process completed successfully. Recommend removing the term "initially" or adding a footnote establishing a realistic timeframe in which backup can be validated. Backups can take hours and last into late evenings. Not all entities have 24/7 coverage within their establishments. Requirement is subject to interpretation. CIP-009-5 Requirement 1.5: Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. Recommend merging this requirement into CIP-008-5, Incident Response Plans. The theory of preserving data at the time of the incident as opposed during the recovery of a BES Cyber Asset seems to be logical. If needed, lessons learned from the incident can be used to update the BES Cyber System recovery plans.
No
CIP-009-5 Requirement 2.3: Test each recovery plan referenced in R1, initially upon effected date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. The requirement itself is extremely stringent in regards to performing an operational exercise on "each" recovery plan for BES Cyber assets and BES Cyber Systems. The definition of "operational exercise" is also subject to interpretation as every entity performs this function differently and CAE's may interpret differently. Request removing operational exercise or designating this requirement for High designated assets. Depending on the amount of Medium and High BES Cyber Systems are designated, entities could be performing operational exercises on a bi-weekly basis just to meet the 39 month requirement.
No
CIP-009-5 Requirements 3.2 through 3.5: Added time frame to current revision is 30 days. Suggest establishing 60 days to complete requirements 3.2 through 3.5. Entities impacted by CIPv5 may establish a substantial amount of High and Medium BES Cyber assets and BES Cyber Systems. Thirty days seems a bit strenuous and may produce a high failure rate. Also, recommend this requirement be enforced to only High and Medium BES Cyber Assets and Systems.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and

Severe VSL's for all requirements.
No
CIP-010-1 Requirement 1.1: Baseline configuration of BES Cyber Systems. With the understanding that this particular requirement was derived from the DHS catalog for control systems security, how does an establishing specific field within a baseline record and those records being auditable increase security and therefore the reliability of the BES Cyber system? Establishing a baseline on each BES Cyber System has been established for the prior requirements that pertain to CIP-007. Entities should have the freedom to create and maintain baseline configurations that impact their assets. With that said, sub-requirement 1.1.4 is very vague. These systems may contain thousands of scripts and the documentation of these to this level is not practical. Also, Requirement 1.1.6, "any patch levels", UNIX and other operating system outside of Microsoft do not have patch levels. Recommend updating the requirement without sub-requirements 1.1.1 through 1.1.6 and leaving the base requirement of Requirement 1.1. The specific requirements 1.1.1 through 1.1.6 provide no added security or reliability to BES Cyber Assets and BES Cyber Systems. CIP-010-1 Requirement 1.2: Measures: A record of each change performed along with the minutes of a "change Advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance. Establishing a "change advisory board" for changes to BES Cyber System baseline configurations and recording the minutes and attendance records is completely non-productive and brings no significant security or reliability to BES Cyber Systems. This requirement maybe needed within larger entities with separate divisions performing multiple functions, however, midrange to small entities have established effective processes through various methods of change control. This particular requirement establishes that NERC CIP requirements are not a "one size fits all" methodology.
No
CIP-010-1 Requirement 2.1: Where technically feasible, monitor for changes to the baseline configuration and document and investigate the detection of any unauthorized changes. This specific requirement seems to be redundant to the requirements set forth in CIP-007-5 R4.1 through 4.5. Why add more responsibility to monitoring BES Cyber Systems outside of the requirements in CIP-007?
No
CIP-010-1 Requirement 3.1: ...conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as design. The term "security controls" is subject to interpretation. Recommend clarifying the term or designating areas within security that need to be assessed.
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIP-011-1 Requirement 1.1: Measures, bullet 2: Training materials that provide personnel with sufficient knowledge to recognize BES Cyber Security Information. Not sure if SDT meant BES Cyber System Information?
Yes
No
While it's completely understandable the VSL's are needed within compliance, not all entities are built equally. Therefore, the entities impact upon the BES varies. Recommend Low, Medium, High and Severe VSL's for all requirements.
No
CIPv5 implementation plan may need to be revised based on FERC's non-approval of CIP v4. OPPD would prefer FERC to approve CIPv4, which would allow entities to comply with the "bright-line" criteria, which is similar to CIP-002-5 Attachment 1. In the future, CIPv5 can be gradually implemented, while allowing entities to meet the "bright-line" criteria, which has been approved in CIPv4 by the NERC balloting body. We recommend CIPv5 be introduced in stages or establishing an implementation cycle as opposed to bypassing the CIPv4 and implementing directly into CIPv5.

Introducing CIPv5 in stages will allow entities who are not in scope to implement CIPv4 “bright-line” criteria and establish a sound level of protection to Critical Cyber Assets. Those entities that are currently in scope will continue to adhere to the CIPv4 standards while preparing internally, financially and structurally for the implementation cycle of CIPv5. Also, would like to note that while the intent of the CIPv5 is to increase security and reliability to the BES, meet FERC Cyber security order 706, and present entities with guidance to enhance their own assets, CIPv5 requirements will take a heavy financial toll on our medium sized utility. Additional resources and infrastructure modifications may cost millions to meet compliance requirements. Additionally, entities impacted by natural disasters (e.g., flooding, tornadoes) are currently recovering and rebuilding their establishments, which only add to ongoing operational cost. Please remember these elements when defining the CIPv5 implementation process.
Group
Dominion
Connie Lowe
Yes
General Comments: The following comments are general in nature and do not apply specifically to Definitions. 1. Dominion supports the approach outlined in Mid-American’s January 3, 2012 document titled “Recommended Change Priorities for CIP Version Five” and does not believe that approach would disrupt Drafting Team efforts and the development of CIP Version Five (V5). The Drafting Team should review Mid-American’s approach and incorporate the recommendations set forth therein. 2. As part of adopting V5, existing CANs must be retired by incorporating the associated requirements and measures into V5. A reconciliation is required to determine which CANs are expected to be retired as a result of the adoption of V5 or may still be applicable at the time V5 is adopted. This information should be incorporated in either the “Reference to Prior Version” of each applicable requirement or through the “Guidelines and Technical Basis” of each applicable Standard. The associated CANs are: a. CAN-0005 b. CAN-0007 c. CAN-0010 d. CAN-0012 e. CAN-0016 f. CAN-0017 g. CAN-0024 h. CAN-0030 i. CAN-0031 Definitions Related Comments: • Annual: The term “Annual” should be created and defined as “At least once per calendar year, not to exceed 15 calendar months between occurrences.” In the requirements listed below, the phrase “on an Annual basis” should replace the phrase “initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences”. This change applies to: o CIP-002-5: R2 o CIP-003-5: R3 o CIP-004-5: R3.2, R6.5, R6.6 o CIP-008-5: R2.2, R3.1 o CIP-009-5: R2.1, R2.2, R3.1 o CIP-010-5: R3.1 o CIP-011-5: R1.3 The definition of “Annual” tracks the language already set forth in Version 5. Implementation of the definition of “Annual” simplifies the language in 13 requirements and reflects the retirement of CAN-0010.
No
No comments.
No
It is not clear how the retirement of CAN-0005 is being addressed in V5.
No
Consistent with the previous response, R2 should be modified to read “The Responsible Entity shall have its CIP Senior Manager or delegates approve the identification and categorization required by R1 initially upon an Annual basis, even if it has not identified High or Medium BES Cyber Assets or BES Cyber Systems.”
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
The numbering scheme of the sub-bullets does not match the numbering scheme used in the other standards. It is recommended that “1.x” subtopics listed under CIP-003 R2 be renumbered as follows: 2.1. Personnel Security 2.2. Electronic Security Perimeters 2.3. Remote Access 2.4. Physical Security

2.5. System Security 2.6. Incident Response 2.7. Recovery Plans 2.8. Configuration Change Management 2.9. Information Protection 2.10. Provisions for declaring and responding to CIP Exceptional Circumstances
No
No comments.
No
No comments.
No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
Yes
No comments.
No
No comments.
No
No comments.
No
• It is not clear how the retirement of CAN-0012 is being addressed in V5 or how it applies to Personnel Risk Assessments (PRAs). • The implementation plan for V5 should address how Personnel Risk Assessments are to be conducted during the implementation period. • PRAs completed prior to V5 should be acceptable until the next time a PRA is required in the 7 year cycle. The following paragraph should be added as the last paragraph to the “Guidelines and Technical Basis” section for CIP-004-5 R4: Personnel Risk Assessments which were completed prior to the effective date of Version 5 of the CIP Standards are acceptable as evidence of completion of a Personnel Risk Assessment even though all of the requirements of Version 5 may not have been met. All Personnel Risk Assessments started after the effective date of Version 5 of the CIP Standards must address all of the sub-requirements in Table “CIP-004-5 Table R4”. • PRAs conducted in support of other compliance programs, such as compliance with requirements for the Nuclear Regulatory Commission (NRC), should be considered acceptable when an individual transfers from one compliance program to another. • The “Guidelines and Technical Basis” section should include a paragraph about “locations” to ensure time and money isn’t wasted on criminal history checks. While the PRA should include details of where an individual resided as part of the seven year criminal history check, we have concerns over the requirement to capture the location of prior employment and school attendance for periods greater than 6 months without further qualification. An individual may attend an on-line school or perform temp work remotely. In these cases, the location of the school and employer are less important to the evaluation of the individual than the location in which the schooling was completed or the work was performed. Dominion is concerned that unnecessary time and costs could be incurred in conducting PRAs without a qualification that the primary physical location of where the individual resided while performing school and work related activities is what needs to be investigated as part of the criminal history check—not the physical location of school or employer. • The requirements for original investigations and reinvestigations should be addressed separately. Reinvestigations should only be relevant for the time period after the original investigation was conducted.
Yes
No comments.
No
No comments.
No

No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
Dial-up is addressed in other requirements and should be explicitly excluded from this requirement.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
CAN-0031 should be retired as part of V5. The “Guidelines and Technical Basis” section contains requirements reflective of CAN-0031 that should be removed entirely.
No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
No
No comments.
No
• CIP-007-5 R5.1 needs to be qualified as being applicable to individual accounts. Credentials cannot be validated with shared accounts. • CIP-007-5 R5.5.1 and R5.5.2 provide that password length and complexity could be the maximum supported by the BES Cyber System. A BES Cyber System is a collection of assets that make up the system. The maximum supported password length and complexity of the system would therefore be driven by the maximum password length and complexity of the device least able to comply with the minimum requirements. The language of the requirements should be modified to read: o 5.5.1. Password length that is the lesser of at least eight characters or the maximum length supported by the Cyber Asset within the BES Cyber System. o 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset within the BES cyber system. • CAN-0017 must to be incorporated into the standard or retired. CAN-0017 indicated that both technical and procedural controls are required; however, the language of V5 indicates that either technical or procedural controls are required to address password complexity.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No

No
No comments.
No
No comments.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
No comments.
No
No comments.
No
No comments.
Yes
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.
No
In contrast to previous versions of the requirement, the language in CIP-011-1 R1.1 is confusing and may unintentionally reduce the level of information protection afforded to BES Cyber Systems. CIP-011-1 R1 should more closely reflect the intent of the Version 3 and Version 4 versions of the CIP-003 R4 requirements. CIP-011-1 R1.1 states that “One or more methods to identify BES Cyber System Information”. This suggests the overt labeling of information associated with BES Cyber System information with a tag that identifies it as BES Cyber System information. The standard should not require the overt labeling of such information with a BES Cyber System tag; rather, it should allow the flexibility described in the Change Rationale associated with having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business. To this end, the language should be modified to read: “One or more methods to label BES Cyber System Information to ensure the information can be associated with an appropriate access control and handling procedure.”
No
• The standard does not specifically address backup or copies of media. If the standard is modified to address backup or copies of media, such modification should be placed in the “Guidelines and Technical Basis” section of the standard. • Application to “any media” known is too broad. Clarity on the intent and applicability of the requirement is necessary. • It is unclear how hardcopies of information are to be disposed of in the new version of the standard.
No
A clear rationale has not been provided in the Table of Compliance Elements within each of the draft standards. To better support the VRF and VSLs, a risk based rationale as it pertains to the Bulk Electric System should be provided for the risk and severity measures.

No
No comments.
Individual
Jennifer Wright
San Diego Gas & Electric
Yes
San Diego Gas & Electric's (SDG&E)'s proposed definition revisions are as follows: BES Cyber Security Incident- Any malicious act or suspicious event that: •Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or a BES Cyber System, or, • Disrupts, or was an attempt to disrupt, the operation of an Electronic Security Perimeter or BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. In general, the proposed definitions are too long, general or arbitrary. The changes to the definitions from Version 3 to Version 5 may greatly change the interpretations; and hence force changes to system design architectures which currently exceed CIP standards. For example, with respect to a BES Cyber Asset, Information Systems designs and architectures best practices include Availability and Reliability as a basis to eliminate risk and increase Availability. The proposed standard definition eliminates Redundancy as a form of risk reduction and renders useless a potential design implemented to increase Availability. Redundancy is implemented to retain availability and should be considered a security measure. Additionally, terms such as Electronic Access Point (EAP) are now greatly different from Access Point to the ESP/PSP. These terms now require major changes to documentation, procedures and evidence. It would be more efficient and cost effective to build upon the existing definitions.
Yes
In general, the criteria should continue to align with NIST standards. Section 2.1 identifies as Medium Impact Rating, generation equal to or exceeding 1500 MW. Yet, 2.13 identifies generation control centers that control 300 MW or more of generation. It's unclear why the first only considers those of 1500 MW or greater, yet drops down to control centers for much less generation (300 MW). It would seem that 2.13 should also be 1500 MW since the impact to the BES would be the same. Sections 2.8 and 2.9: Should there be a requirement that the RC, PA, or TP notify the TOP/TO that they have designated the facility as critical. It's done in Section 2.3 for the GOP/GO. Guidelines and technical basis section: It's unclear how one would interpret the use of "Operational directives" in regards to Reliability Operations Services. Could NERC provide more guidance as to their intent? Additionally, SDG&E has comments regarding the Applicability Section. In Section 4.2.2, NERC identified as an included facility, those systems or programs designed, installed, and operated for the protection and restoration of the BES to include "Its transmission Operator's restoration plan". It would seem that this should have greater details as to what that includes. For example, does it include all of distribution system assets that are used to restore system load. That effectively makes the standards applicable to all distribution, which seems unnecessary.
No
SDG&E recommends expanding the requirement to 60 days due to potential changes in project schedules and ordering or delivery of equipment.
No
SDG&E recommends that the Senior Manager could approve "prior to or initially upon". In general, with regard to the proposed CIP Version 5 Standards, it is unclear whether all the requirements have to have been completed at least once prior to the effective date? In some cases, the standard requires that the entity perform some function initially upon the effective date and then have a follow-up requirement (e.g. update cyber security incident plan within 30 days). NERC should provide further guidance in regards to implementation of CIP Version 5 in this regard.
No
SDG&E recommends that the SDT provide examples of how and when an entity would provide proof of such awareness.

No
It is unclear which “approvals” and “authorizations” are being referenced in the language “shall be responsible for all approvals and authorizations required in the CIP standards.”
No
The training program first needs to identify the roles and the training required by each role. It then requires that each person have training in each of the areas which doesn’t seem then to make a distinction in roles. Shouldn’t the training be able to be different for the different roles?
No
SDG&E recommends language for Part 6.5 which lists all “systems accounts/groups…”
No
Regarding CIP-004-5 R7.2, revoking access due to reassignment or transfers by the end of the next calendar day seems unreasonable. This doesn’t take into consideration the fact that personnel that are reassigned or transferred may have a need to provide support during the transition to new personnel. The original language in Version 3 seems more logical that when access is no longer required, it should be revoked within 7 days. However, determining the date of transfer should be dependent on the type of transfer. For example, where transfers occur outside the department, a 7-day window may be reasonable. Where a change of role occurs within an organization, a 30 to 90 day window may be reasonable due to the time needed to hand-off responsibilities.
No
SDG&E recommends in Part 1.3 to define access permissions and provide examples.
No
For R1.1, SDG&E seeks clarification from NERC regarding how one would restrict access to unnecessary logical network accessible ports that can’t be disabled?
No
SDG&E recommends rewording the language for Transient and Maintenance Cyber Asset. Logging each transient asset connection may not be possible when considering USB or serial connections. This type of activity is better employed using technologies or policies.
No
The term “log generated events” is incorrect. A log is a type of output of a system that is generated by the system. A log, unless scripted by a system sub-process, cannot generate a log, and therefore requires a system process to generate the log. A better term would be a system event log, or system log. Secondly, some legacy or specific machines may not issue a log which can be a) accessed or b) may not meet the parameters of the standard.
No
The proposed language in the standard is unclear and provides little inherent benefit to a security program. SDG&E suggests that the language in R5.5.2 be changed from “the maximum complexity supported by the BES Cyber System” to “the maximum complexity of the above that can be supported by the BES Cyber System”. In R5.5 and 5.6, process or procedural based controls provide

limited security, and to limit unsuccessful authentication attempts or alerts may only be achieved through additional technologies – not procedures. In a Generation environment, for example, small engine and generator cyber assets exist, which do not support authentication or alert for authentication failures.
No
With regard to CIP-007-5 generally, the term “where technically feasible has been removed in many cases where they existed in Version 3. Systems may still have those technical limitations. Is its NERC’s intent that entities can meet these requires with non-technical solutions (e.g. procedural)?
No
SDG&E suggests that the language in R2.2 be changed from “initially upon the effective date” to “prior to or initially upon the effective date”.
No
SDG&E suggests that the language in R3.1 be changed from “initially upon the effective date” to “prior to or initially upon the effective date”.
No
The term "security controls" may not be universally understood within a change management structure. SDG&E recommends including examples of "security controls" and the nature of potential changes impacts to security controls.
No
The issue with the existing language regarding Configuration Monitoring is one where, in a normal systems operating environment, certain changes may not require change processes, and hence change monitoring which is predicated on identifying unauthorized changes fails. An example of this is a change to a data set point, or password change. Each is a general operational change to a system, and affects the configuration of a BES Cyber Asset or System, however may be operationally infeasible - due to the amount and effort of process required to monitor, track and schedule this type of activity.
No
The Vulnerability Assessment tasks listed in the table include the assessment of a test BES cyber system and a comparison of the VMA results against the production environment. Creating a test BES cyber system which models a baseline configuration of the production environment may not be feasible, and in some cases broadly expensive. Some environments rely on older or newer technologies and equipment, and some on a variety of equipment. In addtion, a baseline of the production environment may not be accurate without a VMA against the production system. SDG&E's suggestion is to retain the Version 3 VMA process.
Yes
Group
PacifiCorp
Sandra Shaffer
Yes
As a general, overarching comment, PacifiCorp is concerned about the new direction and definitions prescribed by Version 5, particularly with respect to CIP-002-5. Rather than clarifying and building

upon the existing methodology for identifying critical assets and related critical cyber assets, CIP-002-5 attempts to create a new and unproven methodology for identifying in-scope devices that introduces several procedural and interpretation flaws, rendering the proposed methodology less straightforward than the existing standards. PacifiCorp believes the primary problem with the CIP-002-3 methodology was a failure to clearly identify critical asset facilities, and not a failure to identify related critical cyber assets. This flaw (arising from the discretionary nature of self-determined risk assessment) was corrected by the bright-line criteria introduced as the foundation of CIP-002-4 which was approved by the industry in 2010. PacifiCorp strongly recommends that CIP-002-4 be used as the basis for identifying in-scope cyber devices. This approach would provide consistency and reduce confusion, cost and administrative burdens which would accompany the new regime outlined under CIP-002-5, and adversely impact the registered entities that have already established robust NERC CIP compliance programs based on the CIP-002-3 methodology and defined terms. If CIP-002-4 is used as the basis for identifying in-scope cyber devices, Version 5 of CIP-003 through CIP-011 could be adopted with necessary changes to reflect the preservation of CIP-002-4. Rather than building upon existing definitions that have been implemented and revised by the industry for several years as part of the prior versions of the CIP standards, Version 5 introduces new and problematic definitions. PacifiCorp recommends that the SDT go back to the definitions used in Version 4, and modify those definitions to add clarity. As an example, the new Version 5 definition of BES Reliability Operating Services introduces more problems than it resolves and is not necessary for Version 5 to be effective. Instead, we propose that the terms BES Reliability Operating Service, BES Cyber Asset and BES Cyber System not be implemented and the use of existing terms such as Critical Asset, Cyber Asset and Critical Cyber Asset be retained and modified as needed. As an example, the existing definition of "Critical Cyber Asset" could be revised as follows: "A Critical Cyber Asset is a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact the reliability of the Critical Asset facility where it is located and used." In the alternative, if there is consensus that the term BES Reliability Operating Service adds clarity to which cyber assets should be regulated by the CIP Standards, the definition should be properly incorporated into the definition of Critical Cyber Assets as follows: "A Critical Cyber Asset is a Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact the capability of the Critical Asset facility where it is located and used to perform a BES Reliability Operating Service."

Yes

One of the key problems with Version 5 is that the methodology does not follow a logical "general to specific" categorization process. To generate a list of "qualified" Cyber Assets/Systems, the first logical step is to distinguish between what elements in the universe of potential regulated Cyber Assets are relevant and which can be ignored. The current draft of CIP-002-5 begins with the entire universe of a regulated entity's Cyber Assets. The process then flips back and forth between applying general and specific filters or qualifiers (including bright line criteria that only make sense when applied to a facility and not an individual Cyber Asset associated with a facility) to finally derive a list of BES Cyber Assets. PacifiCorp recommends that the SDT return to the current CIP-002-4 process of first identifying a critical facility, and then identifying the Cyber Assets and Critical Cyber Assets that are relevant to the operation of that critical facility. In the event that the new Impact Categorization criteria outlined in Attachment I of the proposed CIP-002-5 are adopted, we propose the following modifications: 1. In Section 2.1, the Attachment I bright line criteria of 1500 MW is an appropriate threshold if one is assessing generation facilities, but is not an appropriate criteria to assess BES Cyber Assets. This is because a 2000 MW generating plant is likely to have two to four separate control rooms that run units at that plant. On the other hand, it is highly unlikely that there are many generating facilities for which a single BES Cyber Asset affects 1500 MW. Once again, we recommend that entities start with a determination of Critical Asset facilities which will reduce the universe of Cyber Assets to those that are potentially relevant to the functioning of those facilities. 2. In Section 2.7, the Weight Value per Line of 700 should be replaced with a value in the range of 500 – 600, which is more representative of typical rating of 230 kV lines. PacifiCorp operates over 3,000 miles of 230kV line and only a small percentage of them have a peak rating of over 700 MW. 3. In Sections 2.8, 2.9 and 2.11, the table titled "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clear identified basis for why certain paths are included in this table. Rhetorically, it has been mentioned that many of the paths on the table were included for economic / marketing reasons rather than reliability impact. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to

or greater than 1,500 MW." This catalog is actively maintained by WECC and the 1,500 MW value ties much better to other items in Table 1. 4. In Section 2.11, the table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC and there is no clearly identified basis for why certain Special Protection Systems (SPS) are included in this table. As an alternative, we suggest "each SPS categorized as a 'Wide Area Protection System' by WECC. This is the newly created mechanism within WECC to identify SPS of significant importance. 5. The opening paragraph of the definition of Medium Impact Rating should be revised as shown below to correspond with the wording for High Impact Rating: "Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at the following Facilities:"
No
PacifiCorp strongly recommends the removal of any requirements for defining or otherwise addressing Low Impact BES Cyber Assets from the current draft standard. The volume of Low Impact assets is an order of magnitude greater than Medium and High assets for most entities and poses a tremendous compliance burden. While we recognize that there may be security issues that need to be addressed with these assets, we recommend that they be addressed in a separate standard than Medium and High Impact assets. This would allow the industry to initially focus on the more important assets and provide time for further discussion and clarification with respect to Low Impact assets. R 1.1 of CIP-002-5, which requires an update to the status of a BES Cyber Asset within 30 days of a change to that BES Cyber Asset that changes its impact, is a good illustration of the problem with the Cyber Asset-first approach described above in our response to Question 2. Since the most common changes and the changes that are most relevant to the standard's intent, will be to BES Cyber Assets in the Low Impact category, to ensure compliance with the requirement, a regulated entity will have to track all changes to BES Cyber Assets in the Low Impact category – this is despite the current draft's express acknowledgement that Low Impact Cyber Assets are not relevant to the BES. So, even if this requirement can be audited via a spot check of Cyber Assets, compliance likely cannot be achieved without monitoring changes to every Low Impact BES Cyber Asset. In reality, all that really matters are changes made to BES Cyber Assets within a critical facility identified via Attachment I. Again, the starting point should be changes to a critical facility, and then to related critical cyber assets, which follows the methodology of Version 4. As currently drafted, R 1.1 of CIP-002-5 could only be audited through a highly ineffective spot check process, consisting of an auditor pointing out a specific Cyber Asset and asking about the nature of any changes made to that device. In general, PacifiCorp believes that Version 5 will be extremely difficult to audit and will lead to a wide spectrum of audit approaches, rather than a clear and consistent audit approach. Since CIP-002 is the linchpin standard for the entire suite of the CIP Standards, this standard must be clear and concise, with compliance or non-compliance easily determined. It is unlikely that an auditor would point to a Cyber Asset at a generation plant to challenge a regulated entity's determination of whether the mis-operation or non-operation of that individual BES Cyber Asset would or would not adversely impact the plant. It is much more likely that the auditor would look at the generation facility first to determine what impact the loss or mis-operation of the facility would have, and then determine what potential impact the individual BES Cyber Assets have on the plant's performance. Again, since this is the logical process for the analysis, the standard should be changed to reflect this.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No

PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Yes
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Yes
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.

No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No comment.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
No
PacifiCorp supports the comments submitted by EEI in response to this question.
Individual
Roger Pan
Emerson Process Management
No
The 15-minute criterion in BES Cyber Asset definition should be eliminated. This criterion should be only used in the high or low impact rating in CIP-002-5 Attachment I. Rationale: Therer are many auxiliary control sytems in power plants that will not adversely impact one ore more BES Reliability Operating Services within 15 minutes after rendered unavailable, degraded or misused. Based on the current definitions, these sytems will be totally out of CIP requirements, and not even being considered Low Impact systems. However, their continue unavailability after 15 minuts without successful recovery will have a devastating effect on sustaining continuous power generation. Also, most of them are indeed interconnected with main boiler control systems which shall be BES Cyber Systems. Excluding those auxiliary control sytems from the minimum security erquirements may be proven fatal if and when they are compromised.
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Could Remote Access cause "aggregation of enough low impact BES Cyber Systems at various locations to a degree that can cause higher level impacts to the BES" as stated in the Change Rationale for Part 1.1? If this rationale is justified, R2 should also be applicable to Low Impact BES Cyber Systems.
Yes
Yes
Yes
Yes
Yes
Yes

No
This requirement does not address the situation when legacy systems are not supported by OEM, have no security patches, but are still vulnerable to malicious exploitaton. The guideline for this requirment only requires a note "in your source document." A more proactive mitigation should be mandated such as an upgrade plan so that the assset or system has on-going support from the OEM, industry and governments. The guideline for 2.2 suggests the "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control System" by DHS as a source. Instead of patching the BES Cyber Assets or Systems monthly, this new requirement essentially relaxes it to a quarterly basis. It does not seem properly addrssing increasing malicious attackes mostly exploiting zero-day vulnerabilities.
No
Part 3.3 significantly relaxs the signature or pattern update from weekly to monthly. Thie relaxation only puts BES Cyber Assets or Systems more vulnerable to malicious attacks if there is no proactive and preventive protection in place.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Part 3.1 requires "a paper or active assessment of the security controls..." Preseumably, it is on the actual BES Cyber Asset or system. Part 3.2 requires "an active vulnerability assessment in a test enviornment..." It seems that Part 3.1 should only require a paper assessment, while 3.2 required an active assessment.
Yes
No
BES Cyber System Information has been defined in the Definitions of Terms Used in Version 5 CIP Cyber Security Standard. Does Part 1.1 allow to identify more BES Cyber System information beyond what has been included in the official definition? Is the intent really for "marking" the identified BES

Cyber System Information?
Yes
Yes
Yes
Group
Tennessee Valley Authority
Brian Millard
Yes
1) BES Cyber Security Incident - be more specific regarding a “suspicious event” (list examples?) 2) BES Cyber System - be more specific regarding a “Maintenance Cyber Asset.” 3) It says that a Maintenance Cyber Asset is not part of a BES Cyber System. If a misused Maintenance Cyber Asset could adversely impact one or more BES Reliability Operating Services, would it still be considered a "BES Cyber Asset"? What takes precedence? 4) BES Reliability Operating Services - it says “Activities, actions and conditions necessary to assess the current condition of the BES…” What defines what is "necessary"? 5) CIP Exceptional Circumstance - would it be appropriate to also add situations that pose risks to the environment, significant damage to the system, or loss of crucial data/information? 6) CIP Exceptional Circumstance - be more specific regarding what “emergency services” are. 7) Control Center - the definition of "control center" seems to be too open, which may lead to unintended interpretations of the standard. Would any location with the ability to control more than one generation facility, regardless of size, be considered a “control center”?
Yes
Criterion 2.6 (Transmission Facilities operated at 500-kV or higher) should have an exception for radial Transmission Facilities used only to connect “Low Impact” generation to the transmission system. If the generation itself does not merit a Medium Impact designation, the associated transmission facilities should not be categorized as Medium Impact. Attachment I, 2.13 - "Generation control centers that control 300 MW or more of generation" are considered Medium Impact. The 300 MW figure seems very low, especially considering 2.1, which cites a 1500 MW figure for Real Power capability. Should these not be similar? That is, "Generation control centers that control 1500 MW or more of generation" for Medium Impact?
Yes
Yes
Yes
Yes
Yes

No
Yes
Yes
Yes
Yes
Yes
No
Table R3 - Malicious Code Prevention, Part 3.3 "Update malicious code protections within 30 calendar days of signature or pattern update availability..." Clarify that only those pattern updates that the entity chooses to apply (according to the entity-defined frequency) are within scope, rather than every single pattern update that a vendor might have available.
Yes
Yes
Yes
Yes
Yes
Yes

Group
Northeast Power Coordinating Council
Guy Zito
Yes
Refer to additional comments submitted for Question 49. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation”. For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber

Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
No
Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of

R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a

mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.
No

Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of

the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request that footnote 2 in 2.1 be moved into that Requirement.
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If

true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.
Group
Turlock Irrigation District
John Souza
Yes
The definition of a BES Cyber Asset leaves room for interpretation. The major problem is in the use of the words “adversely impact”. These words are only slightly better than the words “would affect” which are used in the definition of Critical Assets in version 3. In effect, version 5 will reinstate one of the problems that version 3 has by using an undefined phrase open to interpretation. (Although Version 4 retains the definition of Critical Assets using the words “would affect”, it does not leave these words open to interpretation because of its pure use of “bright line” criteria for determining Critical Assets. Likewise, Attachment 1 of CIP-002-5 uses the words “adversely impact”; however, it also uses “bright line” criteria including MW, MVAR and kV levels to determine the specific level of adverse impact.) Although “bright line” criteria have been included in CIP-002-5, such criteria are only used for determining Impact Levels (High, Medium and Low), and not for defining a BES Cyber Asset. Even the definition of BES Reliability Operating Services does not take the place of “bright line” criteria as long as the unqualified words “adversely impact” are retained in the definition of BES Cyber Asset. One suggestion is to create bright line criteria for determining what a BES Cyber Asset is. For example, there are different levels at which a Cyber Asset could “adversely impact” the BES Reliability Operation Services. These different levels could be translated to MW levels that could be used to create bright line criteria for defining BES Cyber Assets. The definitions of External Connectivity and External Routable Connectivity are also confusing. They are both defined as routable communications between a BES Cyber Asset and a Cyber Asset external to the ESP. The only difference we can see is that External Connectivity includes dial-up communications and, presumably, External Routable Connectivity does not?
Yes
Attachment 1, Part 1.2 criterion is based solely on the functional obligations of a Balancing Authority, whereas the criteria in the other Parts of Attachment 1 are based on the characteristics of a facility/system or on a combination of functional obligations and characteristics of a facility/system. This inconsistency in the criterion of Part 1.2 could result in a distortion of the proper placement of risk to the reliability of the BES. For example, based on these criteria, a relatively small Balancing Authority with less than 700 MW of generation and less than 700 MW of peak load would be required to categorize their BES Cyber Assets at their Control Center as High Impact. In contrast to this, a Generation Operator with twice as much generation (1400 MW) would be required to categorize their BES Cyber Assets at their Control Center as Medium Impact. This inconsistency could be remedied by adding “where the peak load or maximum generation capability within the Balancing Authority area exceeds 1500 MW” to the end of Attachment 1, Part 1.2. This modification would be consistent with the 1500 MW criterion placed on Generation capability in Attachment 1, Part 2.1. Then all Control Centers performing the functional obligations of a Balancing Authority below the 1500 MW level could

be included in the Medium Impact category under Attachment 1, Part 2.13 by adding “Balancing Authorities” to the list of functional obligations in Part 2.13.
No
CIP-002-5 Requirement 1 contains the word “owns” in the first and second sentences, there by limiting this requirement of indentifying and categorizing BES Cyber Assets to the actual owner of the BES cyber Asset. We would like confirmation that this was the intention of the SDT. If it was not intended, then the word “owns” should be changed to “operates”, “uses”, “maintains” or combinations of these words, depending on the actual intentions of the SDT. Actually, we believe that keeping the concept of ownership as the sole deciding factor in determining the Entity that is responsible for indentifying and categorizing BES Cyber Assets is the best concept to use. If multiple concepts such as “owns, operates, uses or maintains” are used then you could end up with more than one Entity responsible for applying security controls to a single BES Cyber Asset or System, which could cause a host of problems. The CIP-002-5 Application Guidelines, Attachment 1 section, Overall Application sub-section, last bullet item, gives some support for maintaining ownership as the sole deciding factor in determining the Entity that should be responsible for performing R1 of CIP-002-5. However, if the concept of ownership is used as the sole determining factor then clarification should be included in the Application Guidelines stating that “owns” includes concepts such as “leases, rents, or maintains ownership-like control”, in order to accommodate unusual cases where the actual “owner” of the BES Cyber Asset is not a registered entity. Another concept of CIP-002-5 that bothers us is the idea that you do not need to discretely identify BES Cyber Assets and Systems that fall into the Low Impact category, however, presumably, you do need to apply appropriate security controls to such assets. When a Cyber Asset or System drops into the Low impact level, it just gets that much more difficult to determine it the Cyber Asset or System is a BES Cyber Asset or System at all, there by exacerbating the problem of trying to determine if a Cyber Asset is a BES Cyber Asset that the entity neglected to apply the appropriate security controls to, or the Cyber Asset was not considered to be a BES Cyber Asset at all. The definition of BES Cyber Asset is not explicit enough to resolve this problem (see response to question 1). One solution is to create bright line criteria for the definition of a BES Cyber Asset based on the MW level that the BES Cyber Asset could “adversely effect” one or more of the BES Reliability Operating Services.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
Generally we agree with R5, however, since R5 is tied closely to R4, the Applicability column for Table R5 should be the same as the Applicability column for Table R4.
Yes
No
It appears that Requirement 7 has been written to satisfy FERC Order 706 at the expense of adopting sound security practices. The circumstances of an individual's termination or transfer should be taken into consideration when determining how long the Entity has to remove physical or electronic access. Versions 3 and 4 did a better job of addressing this by specifying different conditions such as "for cause" terminations.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
We agree with most of the implementation plan, however, leading up to the day that version 5 becomes effective, we assume that it will essentially be necessary for entities to be compliant with the current version (either version 3 or version 4) and version 5 at the same time. Is this a correct assumption in the opinion of the SDT? Has thought been given to any potential problems that this may cause? We suggest that during the implementation period, entities should be allowed to be compliant with either the current version or version 5 (on the basis of individual requirements and on the basis of individual BES Cyber Assets/Critical Cyber Assets), but not necessarily both versions at the same time. In other words, during the implementation period after regulatory approval, the entity should be deemed to be compliant if it meets the requirements of either the current version or version 5, and the entity should be able to make the selection of which version it is compliant with based on individual BES Cyber Assets/Critical Cyber Assets.
Individual
Jianmei Chai
Consumers Energy Company
Yes
We do not agree with the “Definitions”. The definition of “BES Cyber Asset” is not thoroughly defined. Using the word “adversely” makes the definition vague; i.e., how adverse? As a minimum, it should be replaced with “Adverse Reliability Impact”, from the NERC glossary, but even that may not remove all the uncertainty as to the extent a less than significant impact must be considered.
Yes
We have suggestions and do not agree with the criteria. The SDT is incorrect in stating that “most of these criteria are similar… as part of Version 4”. Version 4 provided the “bright line” criteria for defining “Critical Assets”, not cyber assets. Further tests (routable, dialup, etc.) were applied following that. The new criteria has the possibility to create substantially additional cyber assets requiring CIP compliance. Additionally, creation of the “Low Impact” category further blurs any “bright-line” concept in that nearly all other entity assets end up as “low” and under some CIP compliance. As such, the “similar” criteria is far from it.
No

We do not agree, as R1 invokes Att 1 for classification. Att 1 implies that all Blackstart resources identified in the TOs plan be categorized as medium impact. Previously, only those resources comprising the initial or primary cranking path were required. Rev 5 should reflect the same categorization philosophy. There is no justification for secondary and alternate sources to meet the compliance requirements and measures dictated by a “medium” categorization.
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
Yes
Yes
Yes
Yes
Yes
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
Yes
Yes
Yes
Yes
Yes
Yes
No

Confusing Access Revocation sub-requirements on resignations or terminations. Suggest combine all relevant sub-requirements into one with one defined access revocation period. Too short of a window for Access Revocation sub-requirement on reassignments or transfers. Suggest seven calendar days or at least three calendar days.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.

Yes
Yes
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.
No
This comment is not directly related to proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1, but related to the proposed Evidence Retention in the standard that states “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.” This Evidence Retention guidance simply infers that entities need to keep six years (or three years, depending on the entities’ CIP audit schedule) compliance records even though a shorter retention period is stated in the requirement(s). Because of contradictory guidance, we do not agree with the proposed Evidence Retention for the standard.

Group
Idaho Falls Power
Richard Malloy
No
No
No
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
I can forsee a conflict with BES definition criteria, which excludes generation that is less that 75 MVA on an LN. What of the generation assets that fall between the 20 MVA registry criteria for GO / GOP registration and 75 MVA that lie on a Local Network? These assets would be responsible for the version 5 CIP standards yet are excluded in the BES definition? Would the generator be a cyber asset island? Perhaps threshold criteria for generation assts that match the BES exception criteria be

drafted into the low impact requirements.
Yes
Yes
No
Again a conflict with the BES exception criteria exists. Generation assets below 75 MVA are excluded on Local Networks, however no such provision is made in the CIP version 5 standards, thus a 20MVA generator must comply with the low impact criteria. A problem could arise where physical security is established around the generator but the transmission feeds, being a part of the excluded Local Network under the BES exception criteria are not, therefore rendering the physical security around the 20 - 75 MVA generator on an LN imaterial.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Group
PPL Corporation
Brent Ingbrigtson
Yes
The PPL Companies suggest the follow changes: • For the definition of Inter-Entity-Real-Time Coordination and Communication in the bullet points use the term Reliability Directive" in lieu of "Operational directives" (this should mirror the efforts of Project 2006-06, COM-002-3.) • Formal definitions should be provided for the terms Impact and Adverse as these are used throughout the other standards. See current and proposed change. Current: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Proposed: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the ability of a BES Element or Facility with which it is associated to perform one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the ability of the BES Element or Facility with which it is associated to perform the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Rationale: Clarify that the BES Cyber Asset is associated with a BES Element or Facility.
Yes
Comments: See current and proposed change. Current: 2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. Proposed: 2.1. Generation Facilities with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. Rationale: Editorial comment for consistency with similar language, e.g. generation Facilities, Transmission Facilities, etc. found elsewhere in Attachment 1, Part 2.
No
Current: "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." Further, part 1.1 of R1 states "Update

the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Proposed: Change the current part number “1.1” to “1.2” and add part 1.1 as follows: “Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.” Further, part 1.1 of R1 states “Each Responsible Entity shall identify and categorize its BES Elements and Facilities in accordance with CIP-002-5 Attachment 1.” Part 1.2 states “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Rationale: It is important to identify the applicable Elements and Facilities and their impact categorization for consistent auditing purposes. The PPL Companies request clarification of the apparent inconsistency in the standards where the requirement states that each Responsible Entity shall identify and categorized its High and Medium Impact BES Cyber Assets and Systems and state that Low Impact do not require discrete identification. However, in later standards (CIP-005-5 Requirement 1.1 for example) applicability applies to Low Impact BES Cyber Systems. This inconsistency occurs when other standard require specific identification of low impact facilities but the CIP-002 specifically states that there is no need to identify the Low Impact facilities This inconsistency needs to be addressed. PPL Companies suggest that Low Impact BES Cyber Systems not be subject to the requirements as they have already been defined as Low Impact.
Yes
No
The PPL Companies request clarification on the wording “…15 calendar months between reviews and approvals”. This apparently assumes that both a review and approval needs to be done, but if no changes are made would not a review of the policy suffice? The PPL Companies suggest that the standard language be changed to eliminate the need for approvals to be required when no changes have been made.
No
See response to question 3. The PPL Companies seek clarification on: Does the term “ALL” imply that people who only have access to Low Impact BES Cyber Systems be included?
No
The PPL Companies suggest that the term Storage Media be defined as discussed in the Rationale discussion.
No
See response to Question 3 The PPL Companies suggest the following changes to the standard. The

“bolded” words are the suggest changes. R1.1 requirement defines technical or procedural controls and the measure states to provide documentation of technical and procedural controls – suggest the two match. R1.2 should be all external routable and dial-up connectivity – add the word external The PPL Companies suggest that in R1.3, which requires a listing of inbound and outbound traffic be changed tip indicate that it would be appropriate to list outbound rule set and continue to the current deny all for inbound
No
The PPL Companies suggest the following changes be made: R1.1 uses operational or procedural controls, and the measure states operational and procedural controls, the two should match. R1.3 needs to be adjusted. The term ‘complementary and different” are both included, in the requirement but the measure only uses the term “different”.
No
The PPL Companies suggest removing the last sentence of the measure for R1.2 as it provides no benefit The PPL Companies also request clarification on the definition of “defined timeframe” in the last sentence of R2.2.
No
The PPL Companies request clarification on: R3.1 applies to BES Cyber Systems and not assets, does this allow for router and switches to not require TFE. R3.3 does not include testing for the installation of signature files, should this not be in the requirement R3.4 does this requirement reach all removable items, just as wireless mouse, keyboards, PKI devices, etc. Does an inventory of all transient cyber assets need to be maintained.
No
The PPL Companies suggest that in R3.2 adding additional wording so the 30 day clock starts after the actual incident has completed, instead of 30 days from when the incident is first reported. During those 30 days the process to return to normal operations should occur before the clock begins on the review and lessons learned activities.
No
The PPL Companies have the following concerns about the scope of the requirement: R1.3 is adding information protection to a requirement, keep information protection requirement all within CIP-011-5. R1.4 the verification of each backup upon completion seems to well exceed the order, consider that verification should be completed after major system changes or upgrades The PPL Companies suggest adding to R1.5 the following language “Preserve data, where technically feasible and critical to cause determination, for analysis…”
No
The PPL Companies observe that in requirement and measures for R2.2 the requirement and the measure are just the same wording. The PPL Companies recommend that the requirement be changed so that backup media is “…tested initially upon major system changes and at least once each calendar year…” The PPL Companies seek clarification on R2.3. Does a representative environment match what has been defined to the test environment as required in CIP-010-5 R1.5?
No
The PPL Companies suggest the following wording changes: In R3.1 suggest adding the wording

"…when BES Cyber Systems that have an effect on the recovery plan are replaced…" For R3.2 consider adding wording that 30 days after a recovery plan exercise, but 30 days after an incident is not enough time, so the wording should be after incident recovery as restoring operations should be the priority. R3.4 consider adding the following wording "…any organizational or technology changes that have an effect on the recovery plan within thirty days…"
Yes
No
The PPL Companies seek clarification on: In R1.4.1 should not all security controls be tested instead of "determining" what controls, how do you determine what controls might change with the change. R1.5.2 requires that entities document the test environment with every change that is tested. PPL suggests that only when the test environment changes should an entity be required t document the testing environment
No
The PPL Companies request clarification as to in R3.2 Can the testing be completed in a passive mode in production vs. an active test in the test environment?
No
The LSE should be removed from the Applicability Section (remove entire section 4.1.6 and 4.2.1) of all CIP Version 5 standards. With the NERC BOT approval of PRC-006-1 and subsequent FERC filing (Docket No. RM06-16-000), NERC has recognized that LSEs have no role in UFLS/UVLS programs. The Applicability Section for CIP Version 5 Standards includes LSEs with UFLS/UVLS equipment. This is inconsistent with NERC BOT's recognition that LSEs do not serve a role in such programs. Therefore it is unnecessary to include such a qualified LSE in the Applicability Section. NERC's reasoning was stated in their filing for FERC approval of PRC-006-1 and EOP-003-2: Some comments suggested potential confusion with existing programs or identifying responsibility for providing load shedding. The SDT believes these concerns are addressed in the continent-wide standard by assigning applicability to "Distribution Providers" and "Transmission Owners with end-use Load connected to their Facilities where such end use load is not part of a Distribution Provider's load." We [NERC] believe this covers all load and eliminates potential confusion regarding Load Serving Entities. See Petition of the North American Electric Reliability Corporation for Approval of Proposed New Reliability Standards and Implementation Plans Related to Underfrequency Load-Shedding, FERC Docket No. RM06-16-000, at p. 273. The SDT has revised the applicability [of PRC-006-1] to include both Distribution Providers and Transmission Owners as UFLS entities that may be designated by Planning Coordinators to implement a UFLS program. The interim changes to the NERC Statement of Compliance Registry were made to reflect concerns about the definition of the LSE as a "facility owning entity" as opposed to the Distribution Provider. As demonstrated in the NERC LSE workshop, currently approved Functional Model and the interim Registry Criteria changes, for standards purposes the DP is the "wires" connection to the electric system and owner of the UFLS tripping equipment. This may be inconsistent with previous usage of the same terms in some parts of the country. The Version 0 applicability for UFLS was set prior to the Registry and determined on the then general understanding of the Functional Model and industry usage. The current Functional Model is much clearer on this issue and designates the DP as the facility owner. Since NERC has stated that the Registry Criteria now has an interim step to correct the issue, it is expected that the Registry Criteria will change as the standards are re-evaluated for appropriateness. The SDT believes that this standard is in line with the direction taken by the interim changes and the approved Functional Model. See Petition of the North American Electric Reliability Corporation for Approval of Proposed New Reliability Standards and Implementation Plans Related to Underfrequency Load-Shedding, FERC Docket No. RM06-16-000, at p. 331. This position is consistent with NERC's reasoning throughout the development of PRC-006-1: The SDT recognizes that the Functional Model Version 5 and the Statement of Compliance Registry cause confusion regarding the involvement of the LSE in UFLS

programs but the SDT refers to the section covering the Roles in Load Curtailment in Version 5 of the Functional Model Technical Document; “For non-voluntary curtailment, such as automatic underfrequency and undervoltage load shedding and manual load shedding, the Load-Serving Entity identifies which critical customer loads should be excluded from curtailment for public health, safety and/or security reasons.” See Consideration of Comments on Initial Ballot — Project 2007-01 Underfrequency Load Shedding Date of Initial Ballot: July 7-17, 2010 at p. 4.
Individual
Tom Bowe
PJM
Yes
• An explicit and exact definition of what a BES Cyber System is and what components are included in a BES Cyber System would be helpful here. Some examples may aid in this understanding. • What is the starting point for CIP 002-5 . Do we start with ALL cyber systems and then group them into 3 categories based on impact? Or do we identify ONLY those cyber systems that are used in an entity’s mission (in other words exclude payroll etc) and then classify them based on impact.
Yes
In section 2.3--Define what BES Adverse Reliability Impacts means (Adverse). Section 2.8, define derivation in “critical to the derivation of IROLs.” Is this meant to be definition instead of derivation? In section 2.10, more information is needed on Nuclear Plan Interface Requirements.
No
• Following statement not needed “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.” While PJM appreciates the attempt to lessen the paperwork around this requirement, entities will still need to maintain this list inherently when the listing of BES Cyber Systems is created and each system is classified. • Section 1.1 – “Update the identification and categorization within 30 calendar days”. Does this update require sign-off from Sr. Manager or delegate? • Section 1.1 ‘…categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category’ –What if the change is from higher impact to lower impact category – is that expected to be captured in the annual review ?
No
• In M2. Reference to CIP Senior Manager should include “and delegate”. • In section 1.2 (Evidence Retention) change for retaining evidence is to three years from previous plus current year. Three years can add significant amount of data retention, not necessarily for CIP-002 but for other standards. Our preference is to not change to 3 years. • Section 1.2 the word compliant is mis-spelt as complaint.
Yes
No
• Should include “document CIP Senior Manager” as noted in R6. • This should be a Low Violation Risk Factor, not a Medium. This requirement and rationale is administrative and does not pose a medium risk factor
No
• Following statement should include “minimum” “…protection of its BES Cyber Systems and addresses, at a minimum, the following topics”. • In the list in 1.1 – 1.10, what about these topics should be included in policy? Topics better suited might be common domains of security. • In M2—with a numbered listed the statement should read “Evidence must include…”. • In the second measure in M2 implemented should be replaced with documented.
Yes
• In the M2—with a numbered listed the statement should read “Evidence must include…”. • Dated signature in M2 should be updated to include, electronic approval and workflow evidence.
No
• “Elements of” in the requirement should be removed. “Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function”.

Yes
No
• In R6, formatting error in copy reviewed. “Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change2”. The “2” should be a super script. • In M6, any acceptable form of evidence in M5 should be acceptable in M6. • In Part C, section 1.2 (Evidence Retention) change for retaining evidence is to three years from previous plus current year. Three years can add significant amount of data retention, not necessarily for CIP-002 but for other standards. Preference is to not change to 3 years.
No
Violation Risk Factors for R1 should be Low—see comments in #6 above
Yes
No
• For R2, are all of the roles expected for training included in the table? Is an entity expected to have separate training for each of the items listed in the table, or can the training be all inclusive and given to everyone? • For R 2.5 Visitor Control Program – what are the requirements for such a program • In Part 2.10, is this referring to general networking concepts and the network layout of an entity? Is vendor training sufficient for this area (i.e. Cisco training)?
Yes
No
• Part 4.2 – This requirement appears to lessen the requirements for international individuals. While we appreciate the standards drafting team’s considerations, it seems that when dealing with security some restrictions need to be applied around using the exception process. • Part 4.3 –We believe that the term “criteria” should be left out of the requirement. Reviewing PRAs is a highly subjective process that is handled on a case by case basis, and we believe that only a process that helps drive decisions should be included here.
Yes
R 5.2 Update each personnel Risk Assessment at least once every seven calendar years. Is it OK if the repeat PRA is not within 7 years of the original PRA as long as it is within seven calendar years?
Yes
R 6.1 and R 6.2 - ‘CIP Senior manager or delegate shall authorize’ - Most organizations have defined processes for who can authorize this type of access. Adding the phrase above only increases administrative overhead to sign and maintain delegation letters. Can these requirements be reworded so that CIP Senior manager does not have to be involved in authorizing –either directly or through delegates? Measures for R 6.1 and R 6.2 have numbered list of acceptable evidence. The heading should read ‘Evidence must include’. Otherwise the list should be a bulleted list and entities can choose to maintain one more items from the list.
No
• Part 7.2 –In reassignments or transfers knowledge transfer can take extended period of time (some positions that are recently vacated also are not immediately filled when transfer/reassignment is completed). Stipulations should be present to allow for this knowledge transfer to ensure that access is not revoked before it is truly not needed any longer. • The change rationale does not match part 7.2. As stated above, the requirement in the table currently reflects the need to cut access immediately as of the transfer, rather than allowing for proper transition plans to be executed. • Measures for 7.2 contain numbered list. The opening line should read ‘Evidence must include’. Or the list should be changed to a bulleted list.
Yes
No
• Part 1.1 – Examples of topics to cover/address should be listed. Requirements state “define technical or procedural”, while the measures state “documented technical and procedural controls”.

For an application “either or” would be needed. • Part 1.5 – In measures section a grammar update for, “configuration files of an intrusion detection system(s)” • The measures section is a bulleted list – implying an entity can choose which evidence measures to maintain. It should actually be a numbered list – entities should have all items listed in this section. • There should be clarity on the location of intrusion detection systems. In the current version there is no consistency of interpretation among the CEAs.
No
• Part 2.1 – Source is not clear. In network terminology, defining the source would be helpful. Examples of User Interactive Remote Access would also be helpful for this requirement. Examples of acceptable ‘Intermediate Devices’ would be helpful too. • Part 2.3 - What is the SDT definition of multi-factor authentication? This would be helpful for the requirement.
No
All VSL’s are listed as severe. A defined range or breakdown of levels of non-compliance would be better suited for R1 and R2.
No
• Part 1.1 – Applicability: A list of what “Low Impact BES cyber systems “are, is needed. - Requirements: What is the difference between “operational and procedural controls”? “ Define operational or procedural” is listed as “ define operational and procedural” in measures column, should be consistent. - Measures: What type of evidence does the measure require? • Part 1.2 – Requirements: “ Defined Physical Boundaries”, terminology needs to be used in Measures, for consistency. • Part 1.3 – Should we have separate ESP access point for Low and High impact BES Cyber systems? • Part 1.5 – Why are the requirements between 1.4 and 1.5 separated?
No
• Part 2.1 – Requirements: Define “continuous” • Part 2.2 – Requirements: “Defined Physical Boundaries” should be added to “A process requiring manual or automated logging of the entry and exit”, in order to match the Measures.
No
• Part 3.1 – Requirements: What would be the requirements for systems already in place at time of commissioning? • Part 3.2 – Applicability: Clarify what is meant by “Physical Access”
Yes
No
• Part 1.1 – Requirements: Clarify what “restrict access” means. • Part 1.2 – Requirements: Clarify what restrict means in “restrict the use of unnecessary…” The change description and justification appears weak on the basis the SDT was encouraged to address unused physical ports. A better defined position would be helpful to understanding of 1.2.
No
• Part 2.1 – Requirements: This needs to be written in the form of a requirement. (not a statement) • Part 2.3 – Requirements: “Execute the remediation plan” should be added to this requirement. These requirements aren’t matching up with the “Change Rationale”. • Part 2.3 - Measures – Acceptable evidence should also include workflow evidence from the Change Management system.
Yes
Requirement: Clarify what type of “connection"
No
• Part 4.1 -Requirements: 4.1.1 – Clarify whether it’s just only for Electronic Access Point for 4.1.2 – 4.1.4. 4.1.4 – This is too broad. Defining potential malicious activity would be helpful to understanding of 4.1.4. Metrics around successful or failed attempts would benefit and provide clarity to requirement. • Part 4.3 - Doesn’t match up with 4.5. (Clarity to review summary of two weeks by next calendar day or next calendar day for reviews of failures). • Part 4.5 – Requirements: Clarify what “a summarization or sampling” means.
No
• Part 5.2 – Most organizations have a process for who can authorize use of shared, default, administrator or generic accounts. Adding the phrase ‘CIP Senior Manager or Delegate’ only adds

administrative overhead. Consider rewording this phrase. • Part 5.3 – Requirement does not match to change rationale. • Part 5.4 – Requirements: Move “BES Cyber Assets, Electronic Access Control or Monitoring…” to the “Applicability” section
Yes
Comments: Consider adding a sliding scale of percentage of assets where an entity failed to document ports, monitoring etc. rather than classifying everything into High or Severe VSL.
No
• Requirements: Generally 1.1 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have…” • Measures: the use of the word “targeting” implies pulling in other than CIP related impacts to the BES. Reference in measures section should only be for CIP. • Generally 1.2 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have • 1.1, 1.2, 1.3 Applicability section should list the types of assets to which this requirement applies. ‘All responsible entities’ seems to broad, and can be interpreted to include assets not in the high, medium or even low impact BES cyber systems
No
• 2.1 Clarify “deviations” (…”recording of deviations taken from the plan”…. • Also clarify if the deviations should be recorded in real time or can that be done after the incident is complete • 2.2 Clarification is requested regarding the statement of “initially upon the effective date.” Does this mean that the plan has to be effective on the effective date but not before, can the plan be effective prior to the standards effective date, etc.
No
• 3.2 – The following statement from R2.1 “recording deviations from the plan” appears to align in 3.2. Clarification on why it is in R2.1 would be helpful. • 3.4 - Organizational changes should be responsibility or role changes
Yes
No
• Part 1.1 – Requirements: Examples of conditions are needed. • Part 1.3 – Requirements: “backup, storage,..” what can be acceptable as documentation of storage? This can become cumbersome when dealing with virtual environments. • Part 1.4 – “Part” in the first, second and third column should be “Applicability”, “Requirement” and “Measures” respectively. Requirements: “initially after backup” terminology needs further clarification. This seems to give no window of failure. Typically, we would investigate if a successful backup has not occurred within 48 hours. • Part 1.5 – Requirements: More defined examples of preserved data are needed.
No
• Part 2.1 – Requirements: In the third bullet point, it is mentioned “operational exercises.” But in the Rationale “Functional exercises” is defined. Clarification is requested regarding the statement of “initially upon the effective date.” Does this mean that the plan has to be effective on the effective date but not before, can the plan be effective prior to the standards effective date, etc. • Part 2.2 – Clarification on configurations is needed (compared to baseline)? • Part 2.3 – If calendar year is defined not to exceed 15 months, how does 3 calendar years translate to 39 calendar months?
No
• Part 3.1 - Measures- ‘or when BES Cyber systems are replaced’ –This should be reworded to the effect that when there are updates to High or medium impact BES Cyber Systems or assets, the recovery plans should be updated within 30 days of update to the list. • Part 3.4 - “Part” in the first, second and third column should be “Applicability”, “Requirement” and “Measures” respectively. Organizational changes should be responsibility or role changes
Yes
No
• Part 1.1 – In requirements instead of “develop a baseline configuration” it should be read as “create and maintain a baseline configuration” ♣ 1.1.3. Non-commercial (open source) should also be tracked. ♣ 1.1.6. This is too broad. By “Any security-patch levels” does it mean security patch levels of the operating system or the version? • Part 1.2 – Requirements: Grammatical Error “Authorized”

should be “Authorize” • Part 1.3 – Requirements: “including identification and categorization of the BES Cyber Systems..” is not clear. How does this fit in with “updating baseline configuration”? Should this refer to specific assets as opposed to the system? Measures: Need examples of changes other than asset recovery plans. • Part 1.4 – Requirements: 1.4.1 – Define “cyber security controls”. • Part 1.5 - An entity may not have comparable test environment for every BES Cyber system of high , medium or even low impact. There should be room to use non-CIP assets (even if they are in production) for testing prior to implementing in a CIP environment.
No
• Part 2.1 – Requirements: add “to the baseline” at the end of the sentence. Measures: What is considered as “records of investigations..” (email chain, change record)?
No
In relation to the Compliance section Part 1.2 Evidence Retention, What does “since the last audit” refer to? Explanation is required (does audit refer to a regional entity)? Spelling error “complaint” should be “compliant” in last sentence of first paragraph Part 1.2 Evidence Retention.
Yes
No
• Part 1.1 – Requirements: Generally 1.1 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have …” ---“One of more methods..” is not suitable for a requirement. Need a clearer understanding of what identify refers to. Measures: These measures are weak. • Part 1.2 - Generally 1.2 is not posed as a requirement. Similar wording of other requirements is needed. “Responsible entity shall have…” --“Part” in the first, second and third column should be “Applicability”, “Requirements” and “Measures” respectively. - Requirements: “Access control..” is not suitable for a requirement - Measures: In the first bullet point for “the document process” there is no requirement specified. According to the second bullet point, it is read “Records from an…..need to know basis” should this be enforced in a need to know basis? There is no requirement on need to know basis Third bullet point—difficult to track authorized individuals to a locked file cabinet. • Part 1.3 – Again, in general 1.3 does not pose as a requirement. “Part” in the first, second and third column should be “Applicability”, “Requirements” and “Measures” respectively. - Requirements: Clarify the time frame on “Initially upon the effective date…” - “assess adherence to its BES Cyber System Information protection process” “its”, is vague in this wording, clearer meaning would be helpful. R 1.3 – ‘Initially upon the effective date’ – How far in advance can the assessment be completed ?
No
• Part 2.1 – Measures: The requirement for this measure needs to be clarified. • Part 2.2 – Measures: Update is needed to leave open to other ways to prevent unauthorized retrieval of Information (ie. Encrypting, locking in safe or other physical securing)
No
• R1 – Severe should be only if all three items identified are missed. If not all are missed, a lower VSL should be listed. • R2 – High VSL- severity should be based on number of occurrences. Severe VSL- there is no requirement to document. Only to take action or implement process should not be listed as severe.
No
Plan should be a rolling implementation.
Individual
Chris Higgins / BPA CIP Team
Bonneville Power Administration
Yes
1 - BES Cyber Asset A cyber asset that if rendered unavailable degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one of more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The time frame (15 minutes) is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive

instructions to operate, and the time in which the operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Comment: BPA believes the definition for BES Cyber Asset is very difficult to understand. BPA believes the author is trying to say, regardless of when the Cyber Asset actually broke, the Cyber Asset would cause an adverse impact to the BES within 15 minutes of when it is needed. Recommended Change: A Cyber Asset that if rendered unavailable, degraded, or misused would, when required for real-time operation, adversely impact one or more BES Reliability Operating Services within 15 minutes. The 15 minutes does not start at the time of unavailability, degradation, or misuse of the Cyber Asset. It starts when the Cyber Asset is next required to support one or more of the BES Reliability Operating Services. Redundancy shall not be considered determining the availability of the Cyber Asset. A Transient Cyber Asset is not considered a BES Cyber Asset. 2 - BES Cyber Security Incident A malicious action or suspicious event that: • Compromises or was an attempt to compromise the Electronic Security Perimeter, or • Disrupts, or was an attempt to disrupt the operation of a BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary Comment: BPA believes that malicious attempts are Cyber Security Incidents, regardless of their success. In addition, BPA believes that compromise of BES Cyber System Information should also constitute a BES Cyber Security Incident. Recommended Change: A malicious action or suspicious event which through an investigation and escalation process has been identified that: • Compromises or was an attempt to compromise the Electronic Security Perimeter, or BE Cyber Security Information • Disrupts, or was an attempt to disrupt the operation of a BES Cyber Asset or BES Cyber System • Results in unauthorized physical access into a Defined Physical Boundary 3 - BES Cyber System One or more BES Cyber Assets that are typically grouped together, logically, or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. Comment: BPA believes the CIP-002 Standard appears to allow the identification and categorization of BES Cyber Assets OR BES Cyber Systems. However, the definition BES Cyber Security Incident and most of the CIP Version 5 standards assume that every identified BES Cyber Asset is part of an identified BES Cyber System. There is no definition for Maintenance Cyber Asset. Can a BES Cyber System include Cyber Assets that are not BES Cyber Assets? One or two of BPA's current Critical Cyber Assets have non-critical Cyber Asset components. The Applicability section of the standards includes a definition for Associated Protected Cyber Assets that are associated with a corresponding High or Medium Impact BES Cyber System. BPA suggests that all BES Cyber Assets must be identified as a component of an identified BES Cyber System and whether a Cyber Asset that is not a BES Cyber Asset can be part of a BES Cyber System be added to the definition. Recommended change: One or more BES Cyber Assets that are typically grouped together, logically, or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. 4 - BES Cyber System Information Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. Comment: BPA infers that the large and chunky sentences are confusing and difficult to understand. BPA suggests bullet lists so the reader and implementer can wrap their arms around one or many of the concepts (requirements) in the standard or definition. Recommended change: BES Cyber System or BES Cyber Asset information that includes: • Security procedures developed by the responsible entity, including BES Cyber System disaster recovery plans and BES Cyber System incident response plans; • Network topology or similar diagrams; • BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); • Floor plans that contain BES Cyber System Impact designations; • Equipment layouts that contain BES Cyber System Impact designations. • BES Cyber System disaster recovery plans, or • BES Cyber System incident response plan 5 - BES Reliability Operating Services BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services: Comment: The definition says '…those services contributing to the real-time…' The word contributing is too broad and may encompass cyber assets/systems that do not significantly impact the reliable operation of the BES. Most of the verbiage in this definition should be included as an attachment in CIP-002 if it is only used

for identification of BES Cyber Assets and BES Cyber Systems. Inter-Entity Coordination and Communication is not a service but is a communication method for other Reliability Operating Services. Recommended change: BES Reliability Operating Service (ROS) is a service that is directly essential to the real-time, reliable operation of the Bulk Electric System (BES). BPA also suggests moving the services to an attachment or guidance document as indicated above, make each ROS Service its own definition, or put the definition of the specific service only in its own standard, where used. Remove Inter-Entity Coordination and Communication as a sub-definition of ROS. At a minimum, limit this to real-time ICCP data, which equals facility operational data and status. 6 - CIP Exceptional Circumstances A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability. Comment: BPA asks, "Should this not also include the threat of the risks that are defined?" This definition does NOT cover all exceptional circumstances. A Cyber Security Incident is limited to "a malicious act or suspicious event". It is possible that a BES Cyber Asset would fail in such a way that outside experts were needed to fix it. In most cases there is a reaction to a threat that would invoke exceptional circumstances until such time as it has been determined whether or not the threat is real. Recommended change: A situation (which includes the immediate threat or real event) that involves one or more of the following conditions: a risk of injury or death, a natural disaster, to public safety, health, welfare civil unrest, damage or destruction to Bulk Electric System equipment, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or the impediment of large scale workforce availability. 7 - CIP Senior Manager A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP Standards. BPA supports "7 – CIP Senior Manager" and has no comments or concerns at this time. 8 - Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. BPA supports "8-Control Center" and has no comments or concerns at this time. 9 - Cyber Assets Programmable electronic devices including the hardware, software, and data in those devices Comment: The term should be singular (Cyber Asset and device) not plural (Cyber Assets and devices). The word "programmable" is not definitive enough to clearly identify all the electronic devices subject to these Standards. Recommended Change: Cyber Asset - Electronic device including the hardware, software, and data in the device that is programmable or configurable. 10 - Defined Physical Boundary (DPB) The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled. Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter." Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security. Comment: BPA believes the wording is inconsistent with other usage in the standards. BPA suggests ensuring that the rational statement remains with the definition, or find some way of combining the two. Recommended change: BPA suggests adding "Monitoring" to produce the following: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems reside and for which access is controlled. 11- Electronic Access Control or Monitoring Systems Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems BPA supports "11-Electronic Access Control or Monitoring Systems" and has no comments or concerns at this time. 12 - Electronic Access Point ("EAP") An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets. Comment: Does this purposefully ignore serial communications in a continuation of the differentiation built into the original

CIP-002 R3. Recommended Change: Any interface to an ESP which provides access to BES Cyber Systems or BES Cyber Assets which control or restricts Electronic (routable or dial-up) communications to those assets. 13 - Electronic Security Perimeter ("ESP") A collection of Electronic Access Points that protect one or more BES Cyber Systems. BPA support "13 – Electronic Security Perimeter ("ESP")" and has no comments or concerns at this time. 14 - External Connectivity Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter. Recommended change: Routable or dial-up data communication through an Electronic Access Point into an Electronic Security Perimeter between a BES Cyber Asset and a device external to the Electronic Security Perimeter. 15 - External Routable Connectivity The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol. BPA supports "15 – External Routable Connectivity" and has no comments or concerns at this time. 16 - Interactive Remote Access Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors or consultants Recommended Change: Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and that is not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Interactive remote access can be initiated from: Cyber Assets used or owned by the Responsible Entity; Cyber Assets used or owned by employees; or Cyber Assets used or owned by vendors, contractors, or consultants. 17 - Intermediate Device A Cyber Asset that: 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network. Comment: INTERMEDIATE DEVICE: Again, BPA applauds the inclusion of this definition. However, as stated, BPA believes a Cyber Asset can fail all the conditions and still be considered an Intermediate Device. Recommended Change: A Cyber Asset that meets one or more of the following conditions: - Is used to provide the required multi-factor authentication for the interactive remote access; - Is a termination point for required encrypted communication; and/or - Restricts the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate devices may be located outside the Electronic Security Perimeter, as part of the Electronic Access point, or in a DMZ network. BPA also believes the last sentence could be deleted. If it is not deleted, it should be reworded to make it clear that the three locations listed are not the only possible locations. BPA suggests; The intermediate device locations may include: - Outside the Electronic Security Perimeter, or - As part of the Electronic Access Point, or - In a DMZ network 18 - Physical Access Control Systems Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers. BPA supports "18 – Physical Access Control Systems" and has no comments or concerns at this time. 19 - Protected Cyber Asset A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset. Comment: BPA believes this definition relies on the definition of "Electronic Security Perimeter". Given that definition, the definition of Protected Cyber Asset becomes "A Cyber Asset connected using a routable protocol within a collection of Electronic Access Points that protect one or more BES Cyber Systems that is not part of the BES Cyber System." This implies that a Protected Cyber Asset is an Electronic Access Point. Recommended change: A Cyber Asset located within an Electronic Security Perimeter, but which is not a part of an associated BES Cyber System but is routably connected to an associated BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset. 20 - Reportable BES Cyber Security Incident Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service. Comment: BPA suggests rewording this definition for clarity. Recommended change: Any BES Cyber Security event that has been officially escalated to the level of a Cyber Security Incident which has compromised or disrupted a BES Reliability Operating Service. 21 - Transient Cyber Asset A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset 2) used for

data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System. Comment: BPA believes this should include devices such as sniffers and scanners on a temporary basis. In additions, the references to "Maintenance Cyber Assets" in the standards need to be replaced by "Transient Cyber Assets". Recommended Change: A Cyber Asset that is: 1. Located on a network segment protected by one or more Electronic Access Points protecting BES Cyber Assets or directly connected to a BES Cyber Asset, and 2. Connected to such a network segment or BES Cyber Asset for 30 days or less. Transient Cyber Assets are not considered Protected Cyber Assets. Terms to be Retired Comment: BPA believes that a Cyber Security Incident should be included in the list since the BES Cyber Security Incident is being added. Additional Comments Definitions in general: BPA believes that if a term applies to more than one standard, then it should be a defined term; however, if a term is used exclusively with a specific standard, then leave it in that standard only. Effective dates: Suggest making the Effective Dates paragraphs easier to decipher. These paragraphs are in every standard. They are extremely confusing to read and require further explanation in footnotes. Recommendation: 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later date: January 1, 2015; or the first calendar day of the seventh calendar quarter after the applicable regulatory approval date. However, if Version 4 CIP Cyber Security Standards do not become effective, Version 3 CIP Cyber Security Standards remain in effect until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

Yes

BPA suggests the following recommendations to High Impact: • Modify sentence to say "Each BES Cyber Asset or BES Cyber System used by and located at:" as the definition would already address the 15 minute consideration and no need for duplication here. • BPA suggests applying this to the Medium Impact sentence as well, but include the "not included in Section 1 above" portion. BPA recommends that 2.7 should have increased values assigned to lines with power transformer installations above a predefined nameplate rating at those 200kV and above substations since they are extremely important to the BES, extremely expensive, and have a very long lead time. Or revert back to the version 4 bright line criteria statement addressing number of 300kV lines only. Under the Transmission portion of Medium Impact the total aggregated weighted value indicates "3 connected 345 kV lines and 5 connected 230kV lines"–should that say "or" rather than "and" since then the aggregated totals would be 7000 rather than 3000 which I believe is the threshold desired. BPA also requests that the drafting team provide direction on how this apparent inconsistency in time horizons should be addressed in the cyber system categorization process. In Attachment I of CIP 002-5, there appears to be a conflict in time horizons for applicability of the standard. There are several references to the 15 minute "adverse impact" criteria. However, in the first sentence under Balancing Load and Generation in the Guidelines and Technical Basis section, the language suggests the need to include systems involved in monitoring and controlling generation and load "in the operations planning horizon". In the Situational Awareness section, there is also mention of Current Day "and Next Day" planning systems. Moving from a 15 minute impact criteria to the operations planning and next day planning horizons would significantly increase the scope the standard for BPA and likely for many other entities as well.

No

BPA asks, "Does this mean that we only have to update the list within 30 days if both conditions are true?" BPA believes that R1 should be broken into more requirements, one to address identification of the BES Cyber Assets and BES Cyber Systems and one or more to address updates due to changes to BES Elements and Facilities. CIP-002-5 R1 reads, "Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment 1 - Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification." (Emphasis added) BPA interprets CIP-002-5 to limit responsibility for compliance with the CIP standards for any BES Cyber Asset or BES Cyber System to the owner of that asset or system. It follows that the inverse is also true: i.e. only the owner of a BES Cyber Asset or BES Cyber System can be responsible for CIP compliance. Responsibility for CIP compliance will always fall to the asset owner. BPA believes this adds much needed clarity and strongly supports this position. BPA also supports the position that only one Entity be responsible for any BES Cyber Asset or BES Cyber System, and that the responsible Entity must be the owner or co-owner of the asset or system. BPA

supports this language because it clarifies responsibility and avoids potentially expensive and inefficient duplication of compliance efforts. BPA requests that the drafting team clarify whether they contemplate that scheduling systems would adversely impact one or more BES Reliability Operating Services within fifteen minutes if rendered unavailable, degraded, or misused. For example, does the potential for cyber attack on e-tagging systems before tags are loaded into EMS prior to the ramp suggest that scheduling systems should have a High or Medium Impact Rating? BPA requests that the drafting team define or clarify the term "generation control center" listed as having a medium impact rating in CIP-002-5 Attachment 1, at 2.13. Specifically, BPA requests that the drafting team clarify the extent of control over generation present at a "generation control center."
No
BPA would vote yes if the words “Initially upon the effective date of the standard” were changed to “within 12 months prior to effective date of the standard.
Yes
Yes
No
BPA believes that each organization should be able to create and implement cyber security policies that are suitable to their environment. The CIP version 5 standards assume a one size fits all approach across the industry. R2 Guideline: 2.3. Remote Access • Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access This line implies that VPN access is the only an acceptable interactive remote access method. Don't be so restrictive. Allow for Secure Shell, and Secure Socket Layer, and any other secure method we have available to us now and in the future. The standard is mandating an entity’s policy be too prescriptive and does not allow the usage of other technologies.
No
Comment: BPA believes that requiring a review upon the effective date of this standard ignores the fact that Responsible Entities already have Cyber Security Policies under Version 3 and are already reviewing them annually. BPA believes the statement, "initially upon the effective date of the standard" should be removed from the requirement. Recommendation: BPA recommends the following change: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
Yes
BPA believes the requirement is presently being completed under the current effective standards.
No
BPA believes the proposed VRFs and VSLs, associated with R2, assume all entities have implemented all mandated cyber security policies listed in CIP-003 version 5. BPA believes this does not take into account some entities may not have the need to implement certain cyber security policies based on current business practices and technologies in use (or not in use). BPA considers the level of the VRFs and VSLs are appropriate for R1, R4, R5, and R6.
Yes
BPA believes the requirement is acceptable as written and has no comments or concerns at this time.
Yes
Yes
The CIP004 R3.2 requirement states that training must be provided prior to access being granted and that training must be completed on an annual basis. However, it does not define what actions must occur if training is not completed within the stated timeframe. BPA recommends the inclusion of a

requirement specifying the actions to be taken with regard to authorized electronic or unescorted physical access in the event of an individual exceeding the annual timeframe for annual training.
No
BPA believes the additional language within R4.4.2 regarding assessment of residence, schooling and employment falls outside the boundary of a criminal history check. Verification of schooling, employment and residence is typically a function of employment eligibility verification and should not be considered as part of the assessment processes for risks associated with access to sensitive areas. Such risk analysis is typically based on character, trustworthiness and any revealed patterns of adverse behavior, which are only able to be assessed in reviewing the criminal history check. It is the opinion of BPA that items and issues that fall outside the scope of a criminal background investigation are not relevant when contrasted against the risks to BES Cyber Systems. Further, it is imprudent to require entities to perform positive and negative personal risk assessments based on the location of an individual's school, residence, and employment history. BPA recommends making the following change to CIP-004 R4.4.2: • A criminal history check must be performed prior to granting authorized electronic access or authorized unescorted physical access to BES Cyber Systems. Assessment of the criminal history check must be conducted to assess character, trustworthiness and any revealed patters of adverse behavior.
Yes
No
BPA believes that R6.4 could be improved and suggests making the following change: • Verify at least once each calendar quarter that individuals currently provisioned for unescorted physical access or electronic access to BES Cyber Systems are authorized for such access. BPA believes that R6.6 could be improved and suggests making the following change: • Verify at least once per calendar year, but not to exceed 15 calendar months between verifications to confirm that access privileges to "BES Cyber System Information" are correct and the minimum necessary for performing assigned work functions
No
BPA believes that significant issues and problems are created by the proposed requirements throughout CIP-004 R7 and its sub-requirements. BPA believes that R7.1 should require Responsible Entities to establish documented timelines for access revocations. This presents a potential for violations due to ambiguity. BPA recommends making the following change to CIP-004 R7.1: • For resignations or terminations, the RE shall establish guidelines and processes that adequately protect Unescorted Physical and/or Interactive Remote access to BES Cyber Systems following the time of the resignation or termination • Remove section (ii) of R7.1, and section (ii) of R7.2 BPA recommends making the following change to CIP-004 R7.3: • Modify requirement R7.3 to read… For resignations revoke the individual's access to BES Cyber Systems Information within a timeframe defined by the Responsible Entity – not to exceed 30 days. For terminations, revoke the individual's access to BES Cyber Systems Information within a timeframe defined by the Responsible Entity – not to exceed 7 days. BPA recommends making the following change to CIP-004 R7.4 and 7.5 • Remove requirement R7.4 and R 7.5 altogether as it is impractical to implement. Given the number, type, geographical location, and the inability to centrally manage all the devices within scope of these requirements makes the enforcement of the requirement impractical to implement. Applying CIP-004 R7.4 and R.7.5 at the BES Cyber Asset level (i.e. relays) cannot be accomplished within the stated 30 day timeframe. To do so would require a series of approved outages for every relay designated as a BES Cyber Asset followed by individually changing the Access Level Codes to each relay. Bonneville and other region entities support each other which results in mutually shared access codes. This effectively means individuals may posses the ability to access BES Cyber Assets within several entities' operating areas. Therefore, if an individual moves out of a job that requires access to BES Cyber Assets, every relay in every operating area would require access codes to be changed, which would require a physical visit to every impacted relay.
No
As the Violation Risk Factors and Violation Severity Levels point to requirements and statements that are in question or require modification, BPA is unable to adequately answer this question until the standards are complete.
No

CIP-005 R1.2: No - BPA has concerns with the Applicability definitions. BPA requests clarification in the standard regarding the following questions: • If you can connect to a serial device through a device such as a terminal console that is connected to a routable network, does that cause the serial device to be in scope? • Would a serial device that is capable of "Reverse Telnet" be an included device? • Are EAPs required at points in the network where serial communications are bridged to Ethernet networks? CIP-005 R1.3: Yes - BPA supports CIP-005 R1.3 CIP-005 R1.5: Yes - BPA supports CIP-005 R1.5
No
CIP-005 R2.2: No - BPA also finds "Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session." to be too prescriptive. If the interactive session is only for the purpose of showing maintenance logs or locations of faults, confidentiality and integrity may not be a requirement. If only integrity is a requirement, this can be handled with a hash of the data, not necessarily full encryption. In this case, a blanket requirement for encryption is far too encompassing and would require limits and specifics on the types of remote sessions that should be protected before we would agree to this requirement. In the end, for this matter, BPA should be allowed to determine our confidentiality and integrity needs and apply the appropriate protections as necessary.
No
CIP Version 5 takes the important step of moving toward a risk-based assessment approach by requiring Entities to classify assets and systems as High, Medium and Low Impact to the BES. However, the VSLs and VRFs do not reflect this risk-based approach. For example, in CIP-005-5, all VSLs are classified as Severe, yet CIP-005-5 R1.1 applies only to Low Impact BES Assets and Systems. BPA believes that the VSLs and VRFs in all CIP Standards should be reassessed based on the impact classification of the Assets and Systems covered by each Requirement. As an example, the Severity Levels for CIP-005-5 R1 could be rewritten as shown below. Column Heading "Requirement" = R1 Column Heading "Lower VSL" = For Low Impact Systems, Responsible Entity failed to document procedural controls to restrict access to a specific System. Column Heading "Medium VSL" = For High and Medium Impact Systems, Responsible Entity failed to document method for detecting malicious communication at each EAP. Column Heading "High VSL" = N/A Column Heading "Sever VSL" = The Responsible Entity did not establish Electronic Access Points to control and secure access to its High and Medium Impact BES Cyber Systems
No
The guidelines cited in version 5 standards “CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems” Dated November 7, 2011, Page 22 and 23 “Guidelines and Technical Basis” state, in part: “Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary.” Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to “…96 square inches…” as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA’s service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: “The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:” • Physical measures: Bars, Wire Mesh, etc. • Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.
No
The guidelines cited in version 5 standards “CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems” Dated November 7, 2011, Page 22 and 23 “Guidelines and Technical Basis” state, in part: “Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary.” Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to “…96

square inches…" as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA's service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: "The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:" • Physical measures: Bars, Wire Mesh, etc. Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.
No
The guidelines cited in version 5 standards "CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems" Dated November 7, 2011, Page 22 and 23 "Guidelines and Technical Basis" state, in part: "Typically any opening greater than 96 square inches with one side greater than 6 inches in length would be considered an access point into the Defined Physical Boundary." Therefore, BPA votes no. In reference to the guidelines cited above which originated from CAN-0031 referring to "…96 square inches…" as an access point, this is an area of concern for BPA. In an effort to shore up each 96 square inch opening throughout BPA's service area, with either a physical barrier or intrusion detection system, the cost would significantly outweigh the value added for physical security protection. The challenge to utilities should be to prevent physical access to the BES Assets and to not gauge that access opportunity on 96 square inches. Accordingly, this provision will be unnecessarily costly to the utilities without an actual security benefit. BPA believes the language in the guidelines on pages 22 and 23 referring to 96 square inch access points needs to be removed from the standard, or: The proposed CIP 006 guidelines need to reflect reasonable dimensions, alternatives and language similar to other CIP standards for example: "The Responsible Entity shall document and implement physical or alternative measures for monitoring openings to the physical security perimeter greater than 150 square inches with no dimension less than 12 inches. The Responsible Entity shall implement one of the following methods:" • Physical measures: Bars, Wire Mesh, etc. Alternative measures: Motion Sensors, Vibration Sensors, Intrusion Detection etc.
No
Regarding R2, BPA would agree with the following concept: Failing to capture a single required logging data field, would be no violation at all. This is simply a failure to follow procedures rather than a material defect in, or lack of defined process. As an example, all data fields completed except "time of exit" would be no violation. Complete failure to log a visitor would be considered a Moderate violation because insufficient information exists to uniquely identify the visitor.
No
R1.1: The Guidelines state that ports that cannot be disabled are, by definition, needed. Therefore, BPA suggests that R1.1 be reworded to include the bracketed text as follows: • Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. [If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary]. R1.1 "Measures": CIP-010 R1.1.5 requires that all logical network accessible ports are documented as part of the baseline configuration. BPA is asking for clarification, "Is it expected that Responsible Entities would have different evidence for these two requirements, or would the same evidence suffice?" R1.2 "Measures": The phrase "and screen shots" implies that screen shots are required. BPA recognizes that screen shots are certainly useful, but may not apply to all systems. In addition, this does not follow the explanation in the third paragraph of the "Background" section. BPA suggests rewording the measure to include the bracketed text as: • Evidence may include, but is not limited to: o Documentation stating specific or types of physical input/output ports to restrict, or o [System-generated evidence] or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. R1.1 "Guidelines": The guidelines provide additional requirements. BPA believes these requirements should be in the standard, not in the guidelines. BPA believes that Guidelines should be exactly that: a guide to achieving compliance. BPA requests that all the guidelines for CIP-007 be

carefully examined to ensure that no requirements are inadvertently introduced. In addition, to be clear include the full sentence"… blocking ports at a perimeter does not satisfy this requirement" is unnecessary, as the "Applicability" column explicitly applies to devices beyond perimeter devices. BPA suggests replacing the sentence with: • Note that the requirement is applicable to BES Cyber Systems and therefore to the Cyber Assets within those systems. This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself.

No

R2.1 "Measures": "The list could be sorted by BES Cyber System or source." BPA believes this sentence is true; in fact the list could be sorted in any of a number of ways, depending on the needs of the entity. BPA believes the standard should not address the sorting of lists. BPA recommends removing the sentence. R2.3: The requirement defines a process, but does not require that the process be followed. The Guidelines for R2.3 establish addition requirements. BPA believes that the remediation process is most appropriately defined in the plans required by R2.2. BPA suggests rewording as follows: Completion of the steps in the remediation plan required in CIP-007 R2.2, including any exceptions for CIP Exceptional Circumstances. R2.2 Guidelines: BPA is concerned about the use of terms such as "…the remediation plan will include a timeframe." This strongly implies a requirement rather than mere guidelines. "…the remediation plan should include a timeframe" is more appropriate. R2.3 Guidelines: BPA believes this guideline establishes numerous requirements: "… that plan must be implemented", "… must be implemented by the timeframe the entity documented …" BPA believes that these requirements are appropriate, but they should be in R2.3 itself, not in the guidelines.

No

R3.1: BPA agrees with and applauds the decision not to require anti-malware tools on every Cyber Asset. However, "BES Cyber System" merely groups Cyber Assets for convenience. Therefore, R3.1 could be still be construed to apply to each Cyber Asset in the BES Cyber System. BPA believes that R3.1 needs to be very explicit. In addition, the Guidelines make it very clear that the Responsible Entity can determine that a particular Cyber Asset or group of Cyber Assets is not susceptible to malware and therefore needs little or no protection. BPA suggests rewording as follows: "For Cyber Assets within the scope of CIP-007 R4.1, and which the Responsible Entity has determined to be susceptible to malware intrusion, deploy method(s) to deter, detect, or prevent malicious code". BPA believes that these need not be deployed on every applicable Cyber Asset, as long as each applicable Cyber Asset is protected. R3.1 "Measures": BPA believes "Measures" should be reworded to incorporate the changes to R3.1. BPA suggests rewording to include the bracketed changes as follows: Evidence may include, but is not limited to: • [Documentation of any determinations that specific Cyber Assets or specific types of Cyber Assets are not susceptible to malware]. • Records of the Responsible Entity's deployment of these methods (i.e. through traditional antivirus, system hardening, policies, etc.). R3.3, "Measures": "Measures" starts "Evidence may include, but is not limited to, (i) current signature or pattern updates, and (ii)…" This does not follow the explanation in the third paragraph of the "Background" section. BPA suggests rewording to include the bracketed changes as follows: Evidence may include, but is not limited to: • Current signature or pattern updates, or • [System-generated evidence showing the configuration of signature], • Pattern updates for automated controls • Work logs showing the signature, or • Pattern updates for manual controls R3.4: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Assets, including Low Impact BES Cyber Assets, but excludes the associated access control systems. It also includes all Protected Cyber Assets, not just Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R3.4: BPA believes the requirement makes no provisions for Transient Cyber Assets for which no anti-malware is available. BPA suspects there may be circumstances when the use of such Transient Cyber Assets is necessary for the reliability of the BES. BPA suggests adding the following to the end of the requirement: For circumstances where such methods are not possible, document (i) Compensating measures taken to reduce the risk to the BES, and (ii) Justification that the risk to the BES of not using the Transient Cyber Asset is greater than the risk of using it without anti-malware protection R3.4 "Measures": Logging connections of Transient Cyber Assets is addressed in R3.5. In addition, it does not address whether adequate methods were deployed. BPA believes it should be removed from the "Measures" for R3.4. Reword measures to add "that show" as bracketed below: Evidence may include, but is not limited to, logs [that show] when Transient Cyber Assets and

removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. R3.5: BPA believes the requirement does not address how the connection is made. In particular, depending on the device, it is possible to use Ethernet or serial connections. Serial connections represent a much lower threat but also represent a much lower capability for things such as automated logging. BPA does not know the intent of the drafting team, so BPA cannot offer any suggestions other than to make it clear (either in CIP-007 or in the definitions) whether or not serial connections from a Transient Cyber Asset are within scope. R3.5 “Measures”: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Measures section includes all BES Cyber Assets, including Low Impact BES Cyber Assets, but excludes the associated access control systems. It also includes all Protected Cyber Assets, not just Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R3 Guidelines: BPA believes the guidelines require testing of signature updates, despite the lack of any mention of such testing in the requirements. BPA suggests removing the reference in the guidelines.
No
R4.1: BPA had difficulty determining the meaning of the first sentence. In addition, the requirement clearly states a minimum list of event types. BPA believes that there is no need to include “as a minimum”. With or without that phrase, the Responsibility Entity can choose to log additional types of events. Including it in similar situations in the current standards has led to confusion about what is required. BPA has no concerns with the list itself. However, the Guidelines for 4.1 state “It is not the intent that if a device cannot log a particular event that a TFE must be generated.” As presently stated, the requirement does not support this intent. BPA suggests replacing the initial paragraph with the following: Use technical or procedural means to log generated events for identification of, and after-the fact investigations of, BES Cyber Security Incidents. Log each of the types of events shown below that are applicable to and can be logged for the system or device. Document the reason for any event types not being logged. For the purpose of this requirement a Technical Feasibility Exception is not required for systems or devices that cannot log any or all the event types below. BPA believes the “Measures” should also be modified as follows: • Evidence may include, but is not limited to, a paper or system generated documentation of event classes for which the applicable system or asset is configured to generate logs, along with the justification for event types required in R4.1 not being logged. This documentation must address the required event types. R4.2 “Measures”: BPA believes that screen shots may not be applicable to all systems. BPA suggests replacing “Screen-shots” with “System-generated evidence”. In addition, the format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests rewording “Measures” with changes as bracketed below Evidence may include, but is not limited to, • Paper or system-generated listing of event classes and conditions which necessitate real-time alerts • Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert, or • [System-generated evidence showing] how real-time alerts are configured R4.3: BPA believes this requirement has a fundamental flaw: To satisfy it, Responsible Entities must have a technical or procedural control to monitor the status of the logging system. BPA asks, “What happens if that control itself fails? Must there be another system to monitor the system monitoring logging?” SP800-53 control AU-5, referred to in the Rationale, addresses this first by listing typical causes for logging failure, some of which can be detected easily, and second by allowing the organization to define which events require real-time alerts (Enhancement 2). In addition, despite the explanation in the rationale, the requirement itself does not prohibit a violation for a failure to log. BPA recommends rewording as follows: • Define event logging failures which require prompt notification and correction, either at a Cyber Asset level, Cyber System level, entity level, or in combination. • Detect and initiate a response to such event logging failures before the end of the next calendar day. Logging failures in and of themselves do not constitute violations of R4. R4.3 “Measures”: BPA believes that based on the requirement, the “Measures” should show that the event was detected, and that a response was activated. The proposed “Measures” section does not do that. In particular, (i) Configuration of real-time alerts is a means to detecting a failure, not evidence that a failure was detected. In addition, screen shots are not applicable to all systems. (ii) This requires one of two specific actions. Other actions may be appropriate. In addition, the format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests replacing (i) and (ii) with: • Documentation demonstrating how and when the failure was detected • Documentation showing when the response to the failure was activated. Examples may include, but are not limited

to, dated records that personnel were dispatched or a work ticket was opened to review and repair logging failures. R4.4: Applicability includes Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Systems, including Low Impact BES Cyber Systems, but excludes the associated access control systems and Associated Protected Cyber Assets. BPA cannot determine which is correct, but believes that the two lists must be consistent. R4.4: Despite the rationale for R4.3, BPA believes R4.4 still does not prevent a violation for a failure of the logging system. In particular, a hardware failure of media used to store logs would be a violation. In addition, the phrase "where technically feasible" forces Technical Feasibility Exceptions even in the case of a failure of the logging system. Technical Feasibility Exception should only be needed in the very rare cases of a logging system that is unable to provide for long-term retention of logs. BPA suggests rewording as follows: Unless prevented by a failure of system(s) used for logging, retain BES Cyber System security related event logs identified in 4.1 for at least the last 90 consecutive calendar days. R4.4 "Measures": "Measures" introduces a requirement that entities record what was done to the logs at the end of the 90 days. In many cases logs are removed automatically by the system at the end of some specified retention period. In these cases, there would be no "records of disposition". Furthermore, retention of disposition records should be addressed in data retention, if at all, and not in the "Measures". Finally, BPA believes the format conflicts with the explanation in the third paragraph of the "Background" section. BPA suggests rewording as bracketed below: Evidence may include, but is not limited to: • Security-related event logs from the past ninety days, • [Documentation of the process used to dispose of logs, or] • [Records of disposition of security-related event logs] R4.5: As stated, the requirement does not accommodate reviews in intervals less than two weeks. BPA suggests changing the first sentence to read "…of logged events at intervals of no greater than two weeks to identify…" In addition, the phrasing "sampling of logged events" leaves the possibility of having to review every log, despite the clear indications in the Justification that it is not feasible to review all systems logs. Furthermore, it is not clear whether the Responsible Entity is required to correct the deficiency within one calendar day, or merely begin the response within one calendar day. Also, "any deficiency" implies some type of system failure, when the event types listed in R4.1 all refer to security events involving actual or potential malicious action. Finally, response to logging failures is addressed in R4.3 and should not be addressed here. BPA recommends that the response to a significant event discovered in the review be addressed under CIP-008, not CIP-007. BPA suggests rewording as follows: • Define, document, and implement a process for reviewing security event logs that ensures that (i) Logs are reviewed, either by summarization or by sampling log-by-log or event-by-event, at intervals of no less than two weeks, and (ii) The Responsible Entity's Incident Response Plan, as defined under CIP-008, is initiated before the end of the next calendar day (or within the time constraints of the Incident Response plan, if longer) for any discovery of a potential security event defined under R4.1 of this Standard Perform the actions defined in the process, as applicable. R4.5 "Measures": "Measures", as stated, requires documentation of each of four different actions. Some of the actions may or may not occur. In addition, it is not clear what "documentation describing the review" means. Finally, the format conflicts with the explanation in the third paragraph of the "Background" section. BPA suggests rewording as follows: Evidence may include, but is not limited to; • Documentation describing the review process, • Findings from reviews, or • Signed and dated documentation showing the review occurred R4.1 Guidelines: The paragraph on page 41 states: User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped. The last sentence defines four types of events that must be logged, at least three of which are clearly not within the list in R4.1. This is an extension of the requirements. BPA believes this conflicts with the purpose of guidelines. If the requirements are valid, BPA believes the requirements should be moved to the requirements section. In addition, an earlier paragraph in the Guidelines makes it clear that it is not practical for the Standard to enumerate all events. BPA agrees with that earlier paragraph, and suggests not adding additional events in the Guidelines. Even if the paragraph is left in place (to which BPA is strongly opposed), there are other concerns, as well: • BPA believes "Account management" is not defined. Typically, it includes creation, deletion or changing of accounts or of privileges associated with those accounts. If that is the intent here, it should be stated explicitly. • BPA believes that requiring logging of object access and processes started and stopped will generate voluminous logs, to no real purpose. As an example, an active database can easily generate hundreds

of file accesses per second. There is little utility in logging these, or any other routine object access. BPA believes it makes more sense to log only failed object access or failed process start/stop. R4.2 Guidelines: BPA believes that “Alerts can be configured…” and “The log analysis rules can exist…” appear to be stating additional requirements, in that each sentence provides a closed list of actions. BPA suggests “Typically, alerts are configured…” and “The log analysis rules often exist…” as possible solutions to the issue. R4.3 Guidelines: In order to eliminate the possibility of the Guidelines appearing to expand on the requirements, BPA suggests the second paragraph be rewritten as: • For centralized logging systems, it should noted that if communication goes down between the cyber asset and the logging system, there is no logging failure as long as the cyber asset can store the logs locally for a period of time until the communication comes back up. R4.5 Guidelines: BPA believes the first sentence is unnecessary, as it merely restates the requirement.

No

R5.1: Applicability includes Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems, but excludes Low Impact BES Cyber Systems. Requirement includes all BES Cyber Systems, but excludes Associated Protected Cyber Assets and the associated access control systems. BPA cannot determine which is correct, but believes that the two lists must be consistent. R5.1: Based on the measures, the Rationale and the Guidelines, the apparent intent of R5 is to address user access only. To clarify this, BPA suggests modifying R5.1 to read “…granting users electronic access…” R5.1 “Measures”: The format conflicts with the explanation in the third paragraph of the “Background” section. BPA suggests modifying “and” to “or” as bracketed below. Evidence may include, but is not limited to: • Documentation describing how users are authenticated before being granted access, [or] • Demonstrations showing authenticated access enforcement of internal and remote paths to the BES Cyber System R5.2: Again, it is not explicitly stated that only user access is relevant. BPA suggests modifying R5.2 and change bracketed text to read “…other generic [user] account types.” R5.4: BPA recognizes that this is the only requirement in the standard that levies requirements on Low Impact BES Cyber Assets. It is also unusual in that it lists Responsible Entities in the “Applicability” section but lists the covered Cyber Assets in the requirement. Furthermore, it will require Technical Feasibility Exceptions that could be avoided. Finally, BPA believes this requires a procedure, but does not require that the procedure be followed. BPA suggests the following: • Applicability: o High Impact BES Cyber Systems o Medium Impact BES Cyber Systems. o Associated Physical Access Control Systems o Associated Electronic Access Control or Monitoring Systems o Associated Protected Cyber Assets Requirement: Define, document, and implement procedural controls for initially changing default passwords, unless - The default password is unique to the device or instance of the application on Cyber Assets or Cyber Systems involved, or: - The device does not allow the passwords to be changed For the purposes of this requirement an inventory of Cyber Assets is not required R5.5.3: The intent of “…or an obligation to the password…” is unclear to BPA and since BPA does not understand the intent of the phrase, BPA cannot suggest a correction. R5.3 Guidelines: This appears to apply to R5.4, not R5.3. In addition, in the first paragraph, “… passwords must be changed …” states a requirement. R5.4 adequately states the requirement. R5.5 Guidelines Table Comments: BPA does not understand all the columns in this table. In particular, BPA is uncertain of the meaning of “Significance of passwords …” and “Existing Service Agreements”. BPA suggest that the table be prefaced with a narrative describing the purpose of each column. In addition: • BPA does not understand the third and fourth entries, third column, reading “Local access path. Individuals must authenticate at an upstream device prior to gaining access.” Several things are not clear to BPA and BPA asks: • Do the two sentences refer to two independent conditions, with either or both being true, or are they both true? • What is an “upstream device”? Why must users authenticate at one? Is this a requirement for proper use of the password, or a technical issue defining when this particular entry is pertinent? • Why are there no other instances of shared passwords? • Fifth entry, third column: Is this a: o Requirement that remote users must authenticate using a different account prior to using the local account o Statement of two alternatives for using passwords, or o Definition of when the entry is applicable?

No

In the last condition for R2, Severe VSL: “except for CIP Exceptional Circumstances” is redundant, in the implementing the remediation plan is not required under those circumstances.

No

BPA believes there is a conflict in statements regarding Applicability - targeted at "All Responsible Entities" for CIP-008 R1.1 thru R3.1. Also in R3.2 thru R3.5 references High and Medium Impact

Cyber Systems. BPA does not does not understand the difference in Applicability; BPA believes it should be one or the other. Various incident response plans will need to be created and maintained. BPA believes this is a good approach both from a cyber security point of view and good business practice. BPA supports R1.0 as written and has no comments or concerns at this time. Add 1.3.4. Definition of process for documentation of allowable deviations from the plan and the documentation of those deviations. BPA supports R1.1 as written and has no comments or concerns at this time. R1.1 Measure: BPA suggests rewording to eliminate redundancy: Suggested Rewording: Evidence may include, but is not limited to, dated copies of BES Cyber Security Incident response plan(s) that include how to identify, classify, and respond to BES Cyber Security Incidents which target the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents and that impact the reliability of BES. BPA supports R1.2 as written and has no comments or concerns at this time.
No
While documenting an incident is good business practice, BPA believes the standard should not dictate what evidence needs to be captured during an incident response. The standard should restrict itself to requiring documentation be provided, but the content should be up to the Responsible Entity. Lessons learned documents are valuable for example, but some incidents may be minor and there are no "lessons learned" leaving a requirement to file a Null attestation for compliance. R2.1 BPA believes the requirement needs rewording and BPA suggests that it should be revised: Current wording: "When a BES Cyber Incident occurs the incident response plans must be used when incidents occur and include recording deviations taken from the plan during the incident or test." • Suggested wording: "The incident response plan(s) must be used when a BES Cyber Security Incident occurs or when the incident response plan is exercised. Deviations from the plan must be fully documented in accordance with the plan." Note: The current requirement uses the word "test"; BPA recommends changing "test" to "exercise". R2.1 Measures: BPA believes the wording of the measure should be changed: Current wording: "Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and documentation that lists and justifies deviations taken from the plan during the incident." • Suggested wording: "Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process. Documentation of any deviations taken from the plan during the incident." Note: BPA believes in the measures "…the incident." at the end of the paragraph should be changed to "…incident or exercise". R2.2 Comment: BPA believes the use of the term "implement" at the front of the requirement is unusual. The normal definition is the plan is implemented upon publication; the plan can be invoked through an actual incident or through an exercise. • Suggested wording: Implement the BES Cyber Security Incident Response Plan(s) initially upon the effective date of the standard or before and at least once each calendar year thereafter…"] • Additional wording suggestion to be added: Incident response plans must be used when responding to real incidents or exercises, and must include recording deviations taken from the plan during either a real incident or the exercise. R2.3 BPA believes rewording is needed and suggests that it should be revised: Current wording: "Retain relevant documentation related to reportable BES Cyber Security Incidents for three calendar years." • Suggested wording: "Retain documentation described in the Incident Response Plan related to reportable BES Cyber Security Incidents for three calendar years."
No
R3.1 The current wording requires the Incident Response Plan to be implemented upon the effective date of the standard. BPA believes that could cause some entities to fail compliance if they did not publish their documentation on that exact date. • Suggested wording: o "Review each BES Cyber Security Incident Response Plan for accuracy and completeness o Initially, 30 days prior to the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and update as necessary." R3.2 and R3.3: BPA believes these requirements are redundant and should be combined. The requirement assumes there will be a need for a revision which may not necessarily the case. BPA suggest that requirement R3.2 be rewritten as follows and that R3 be deleted: • Suggested wording: "Review the results of BES Security Incident response Plan(s) test or actual incident response within thirty calendar days of the execution. o Document any lessons learned within thirty days of the exercise or actual incident o Update the plan within sixty days based on the any changes suggested in the lessons learned document."
Yes
R1 High VSL for R1 states that the plan ".does not communicate the incident to appropriate

organizations." BPA suggests that the VLS be changed to read "…or does not define the internal staff or external organizations that should receive communication of an incident". R2 Replace "test" with "exercise" R1 Guidelines: Comment: The Guidelines establish a definition for "Reportable BES Cyber Security Incident". BPA has issues with that definition: 1. The definition should be identical to the one in the formal CIP V5 Definitions of Terms; the SDT should pick one or the other. 2. The guideline added a new term "response action" with a definition. It also should be cross referenced to the CIP V5 Definitions of Terms. The guidelines also state that a response action can either be "necessary or elective" without defining those terms. They also go on to use "precautionary" as a term that defines elective. BPA believes it is useful to have this guideline, although it may make more sense to move the definitions out of the guideline and into the definitions section while leaving the guidance as is.
No
BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard. o 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later date: January 1, 2015; or the first calendar day of the seventh calendar quarter after the applicable regulatory approval date. However, if Version 4 CIP Cyber Security Standards do not become effective, Version 3 CIP Cyber Security Standards remain in effect until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan. (Use this format Version # CIP Cyber Security Standards to refer to the complete set of standards rather than the harder to read, takes up more space: CIP-002-3 through CIP-009-3) • Many of the requirements include the words "upon the effective date of the standard". Many recovery plans are already on an annual cycle. Will all recovery plans have to be exercised again, if they have already been tested during the calendar year prior to the effective date of the standard. This wording doesn't really make sense for systems placed into operation after the effective date of the standard. Recommendation: o CIP-009 R2 should be "prior to the effective date of the recovery plan(s) The addition of this new requirement calls for the preservation of data for forensic analysis following all events that trigger the Recovery Plans. If this requirement is implemented as written, it may delay recovery of impacted systems, as our first priority will be data preservation. This may negatively impact system reliability. We can approve this requirement if it states explicitly that recovery cannot be hampered by attempts to preserve data.
No
BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard.
No
BPA would vote yes if the words "Initially upon the effective date of the standard" were changed to "within 12 months prior to effective date of the standard. Based on forensics and analyses it may take longer than 30 days to determine the cause of a failure. Please clarify if the expectation is that the analyses and updates are required to occur within this 30 day period.
No
BPA would change its position for the VRFs and VSLs if they Included the applicability of the requirements as an element. BPA believes the VRF & VSL should incorporate the risk to the BES Cyber System. As an example, High Impact BES Cyber System violation would result in a higher VRF & VSL. Likewise, a lower impact for applicability would result in a lower VRF &VSL.
No
Concerning R1.1 BPA recognizes that it would be overly burdensome to have to document every piece of software installed on an ACMS server, not just the major applications. There is some latitude available based on "specified grouping", but this continues to be a concern regarding maintaining compliance. We will address this from the "grouping" perspective and thus approve R1.1. Grouping is a software "package" or group of files. It is good requiring the differences in test vs. production to be documented demonstrates awareness that not all entities have test environments that model their production systems. This allows significant latitude that will enable us to remain compliant in the interim while we are working to enhance our test environments.
No
For the majority of programmable electronic devices in the field, especially devices that don't support routable protocols, it will not be technically feasible to monitor for changes to the baseline configuration. BPA assumes we will have to spend a lot of time submitting and managing Technical Feasibility Exceptions (TFEs) for each of these devices which does not increase reliability or cyber

security. BPA would vote yes if this requirement was not required for Medium Impact BES Cyber Systems and Associated Protected Cyber Assets.
No
BPA would vote yes if the words “Initially upon the effective date of the standard” were changed to “within 12 months prior to the effective date of the standard.
No
BPA makes the following recommendation for R2: BPA believes a 30 day window should be established to investigate and resolve the unauthorized change. Require that the unauthorized change be resolved either by formal approval of the change or that the change was backed out. The severity increases to Severe if not resolved after 30 days
No
R1.3: BPA believes the requirement needs to accommodate an initial assessment prior to the effective date of the standard. BPA suggests “Initially upon or no more than 15 months prior to the effective date…” R1.3: BPA believes the standard does not indicate what is meant by “adherence to its BES Cyber System Information protection process.” Reasonable interpretations could include any or all of: 1. Review of all BES Cyber System information to ensure it is properly labeled. 2. Review of a sampling of documents to ensure they are properly labeled. 3. Review of user access authorizations to electronic media storing the information
No
BPA believes that it is correct and true that data may be recovered from some media after erasure. However, it is also true, that for some media, erasure is fully adequate. BPA recommends the following change: Reword the requirement to make allowances for media reuse within the same control zone. In such cases, where the media stays at the same security level, there should be no need to cleanse the media prior to re-use. R2.2: Yes R2.1: There have been varying usages of the term “redeploy” in CIP-007-3 R7. In particular, there have been violations found when a change in an ESP leaves Cyber Assets that were once within an ESP (and therefore subject to CIP-007-3) outside the ESP. BPA suggests the following be added to the end of CIP-011-1 R2.1: This requirement does not apply to instances where the media remains in the Cyber Asset, but the Cyber Asset undergoes a change in status such that CIP-007 R2.1 is no longer applicable. R2 Guidelines: The last paragraph allows for the removal of a BES Cyber System from service to allow analysis of the media. BPA believes it should also point out that it may be appropriate to remove the media from the Cyber Asset to allow off-line analysis, as that would be neither reuse nor disposal.
Yes
Yes
General Comment on the Standards Development Process and Direction: The SDT has done an excellent job in capturing the weaknesses and problems that were included in the previous standards. The move toward a more FISMA/NIST based approach is obvious and should be applauded. However, this raises the question of why we are attempting another intermediate step rather than simply adopting the NIST FIPS and SP documents as our methodology for applying security. NIST has done an exceedingly good job of addressing Cyber Security for Federal systems for decades, and has taken steps to address the world of Industrial Control Systems. These standards and guides are strong yet flexible, allowing for application in many different environments. And the terminology and definitions used are already well understood industry standards. It seems that the scope of this (Version 5) change is broad enough that it would be a small step to skip over it and simply adopt the NIST Cyber Security Standards for our industry.
Group
Pacific Gas and Electric Company
Robert Mathews
Yes
Strike or revise bullets 3, 4 & 6 in the Control Center Definition
No
Criteria 2.13 in Attachment 1 is not acceptable because under 1) the functional obligations of TOP and TO is too vague and 2) 300MW of in many cases does not qualify as significant impact. Also 300 MW

of generation should not be equated to 300 MW of UFLS/UVLS. Intent of these criteria is not clear so suggested language is not provided
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R6.3 is unacceptable as it does not fit the stated rationale for R6. All requirements pertaining to Information Protection should be in CIP-011 not CIP-004.
No
R7.1 and R7.2 are potentially infeasible
Yes
Yes
No
R1.4 needs further specification (e.g. detecting unauthorized entry in real-time may not be feasible in certain situations)
Yes
Yes
Yes

Yes
Yes
No
R5.1 for local access (e.g. relays) is problematic
Yes
Yes
No
R3.4 and R3.5 are potentially infeasible
No
Comments: Revise R1.5 to “Preserve data, where technically feasible or operationally prudent….” to enable actions in the best interest of BES reliability.
No
R.2.2 What is “any information” defined as?
Yes
Yes
Yes
Yes
No
CIP-011 overall is unclear on the distinction of information about BES Cyber Assets and information residing on BES Cyber assets. Also the scope of CIP-011 to Low Impact Cyber Assets is unclear.
No
CIP-011 overall is unclear on the distinction of information about BES Cyber Assets and information residing on BES Cyber assets. Also the scope of CIP-011 to Low Impact Cyber Assets is unclear.
Yes
Group
SPP RTO and listed members
Lesley Bingham
Yes
he definition of BES Cyber Asset has caused confusion. On two recent presentations by the Standards Drafting Team, a clear definition was requested and could not be provided. Given that this is a fundamental definition used in defining other terms and is a core concept of the CIP standards, a clear definition is needed. The definition of BES Cyber Incident contains the word “suspicious”. Recommend a change to “intentional”. The definition of BES Cyber System contains the term Maintenance Cyber Asset, which is not a defined term. Should that be Transient Cyber Asset? The definition of BES

Reliability Operating Services is lengthy and confusing. There is concern that it will be difficult to audit to this definition and that it conflicts with the established bright line criteria. The definition of CIP Exceptional Circumstance should include the word “may” to read “A situation that may involve one or more….” The definition of Control Center does not explicitly include generator control rooms. Is it intended to cover these facilities? If not, does that term need to be defined for greater clarity?
No
No
No
Yes
Yes
No
The areas covered are certainly appropriate to protect BES Cyber Systems, but every entity may not have processes which would be covered by all topics. Should a policy be drafted or language included where a process does not exist?
Yes
Yes
Yes
Yes
Yes
No
Language around this requirement pertaining to which personnel need to be covered is confusing. Rationale discusses personnel who have electronic or unescorted access. Information in table does not specify who should participate in awareness activities. Table specifies that language was “Changed to remove the need to ensure everyone with authorized access receives this awareness”. If all personnel, as opposed to strictly those with authorized access, at a Responsible Entity are covered by this requirement, then that should be specified in the standard.
No
Comment is specific to Part 2.10 of Table R2. Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary. Recommendation is to strike item 2.10.
Yes
Yes
Yes
Yes
No
Terminations, resignations and transfers all have the same access removal requirement: one business

day. This does not appropriately gauge the level of risk with each. A termination, especially an involuntary one, can expose the Responsible Entity to much more risk than a transfer. Also, how should a Responsible Entity define when the “clock starts”? For a transfer, access may still be needed during the backfill/transition process or even for resource management after the transfer has formally been completed. Also, in the Change Rationale, there is a comment that “the SDT adapted this requirement from NIST 800-53 version 3 to review access authorizations on the date of the transfer” yet the requirement is to revoke access. Reviewing access is not mentioned in the table.
Yes
No
Part 1.1 Requirement is to define controls. Yet the measure requires evidence that the controls have been implemented. The requirement and the measure should be closer in language. Part 1.2 should include only High Impact BES Cyber Systems, not Medium Impact BES Cyber Systems as well. If Medium Impact BES Cyber Systems need more protection than a Low Impact BES Cyber Systems, that protection should be described more specifically. Medium Impact BES Cyber Systems and High Impact BES Cyber Systems seem to get same treatment on this provision. This section also impacts Registered Entities who haven’t had CIP requirements previously. Some of the requirements for Low Impact BES Cyber Systems will have a high paperwork factor and burden. Part 1.5: Measures are very technology-centric around one solution, Intrusion Detection Systems or IDS. Request clarification that IDS is not required and that specific technology isn’t sole means of compliance.
No
Part 2.1 Concept of “Associated Protected Assets” is not well-understood. Clarity needed here. If Associated Protected Assets need a significant level of protection, a more direct approach would be to classify them as Medium Impact BES Cyber Systems or High Impact BES Cyber Systems? Part 2.3: User ID as an authentication method is addressed in other NERC publications and should not be included in the measure for this standard.
No
All the VSLs for this standard are Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no permissions at an EAP. There should be a level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.2 and Part 1.3 contains language in the Measure of each to track egress, but the language of the standard does not specify this as a requirement. Standard includes language to restrict access (i.e. ingress) to those authorized. Egress language expands the standard and should be removed from the Measure. Part 1.3 also seems to set the stage for an additional number of Technical Feasibility Exceptions (TFEs). One of the goals of CIP Version 5 was to reduce TFEs in place of better security measures. The language “two or more…controls…where technically feasible” will lead to increased TFEs.
Yes
Yes
Yes
The VSL for CIP-006-5 is a good example of defining the appropriate degree of severity for noncompliance with a standard.
No
Part 1.1 indicates that the requirement is applicable to “systems”, but measure focuses on “assets”. Need a system approach if this requirement is intended to be applied at a broader level. The term “BES Cyber Asset” should be removed from measure if the requirement can be applied to “system”.
No
Part 2.1 Addition of “identified source” which can be final approver of patch, such as application vendor, is very helpful to Responsible Entities. Part 2.2 and Part 2.3 use the term “remediation plan”. Need clarification on when a “remediation plan” is needed. Is it required in delay between OS patch

release and vendor approval? When vendor will not approve patch? When there is a vulnerability for which no patch has been released?
No
Part 3.3 requires an update within 30 days. What “starts the clock” on this requirement? Is there an allowance for an approval step from a 3rd party vendor after the OEM has released the signature or pattern update? In some instances, a 3rd party vendor may have to approve prior to a Responsible Entity implementing a release and their delay could cause timing concerns. Part 3.5 requires logging each Transient Cyber Asset connection, but this would be captured in the Configuration Change Management requirements of CIP-010-1. As it is covered elsewhere, it should be removed from this section of the standard.
No
Part 4.1 includes the use of “any” in the list of activities to log. Not all activities require follow up or investigation and that is the purview of CIP-008-5. Specifically, “any” failed login may not be an indication of a problem. Certainly there is a threshold that deserves attention, but the broad use of the term “any” makes this requirement too broad. Part 4.3 sets a timeframe of “before the end of the next calendar day”. This is a very short timeframe. Certainly, logging failure should be addressed, but more time may be needed. Part 4.5 inserts a manual review when automation and alerting, both mentioned previously in the standard are much more effective and reasonable controls. If a Responsible Entity is compliant with Parts 4.1-4.4, then a manual review is a redundant effort which provides no additional security. Recommend that this Part be removed.
No
Requirement 5.5.3 is confusing and unclear, especially the license and service agreement language. Also, the inclusion of “based on the impact level of the BES Cyber System” is not helpful. Recommend that the impact phrase be stricken.
No
The VSLs for this standard are primarily High or Severe. A Responsible Entity with incomplete documentation is at almost as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.3, requirement 1.3.3 needs the addition of “BES Cyber Security Incident” to replace the undefined “incident”.
No
Part 2.1, the language regarding “deviations” is confusing. Plans should be written at a high enough level that a Responsible Entity has the flexibility to respond best to their situation. Documenting a deviation does not provide additional security control. Recommend that the deviation language be stricken. Part 2.2 requires a test of a Responsible Entity’s BES Cyber Security Incident Response Plan “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a test 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional retest on or about the effective date of Version 5?
No
Part 3.1 requires a review of a Responsible Entity’s BES Cyber Security Incident Response Plan “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a review 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional review on or about the effective date of Version 5? The timeframes within Requirement 3 vary from 30-60 days. A consistent 60 days for each item would be recommended. Requirement 3.4 does not specify that the technology changes referenced are ones the Responsible Entity has actually implemented. Recommend adding “implemented” prior to “technology changes”.
No
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5

provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
The purpose of CIP-009 in all versions has been to provide that a Responsible Entity had adequate recovery plans. However, some CEAs are interpreting this standard to require the full restoration of facilities, including blueprints to rebuild structures. The standard should include language to reinforce the concept of BES system recovery and to specifically exclude full facility restoration. To support the recommendation above, the word “restore” used in R1, Part 1.3 should be changed to “recover” in both Requirement and Measure. Part 1.5 should be stricken. While data preservation is relevant to incident response processes, it is not relevant to recovery efforts.
No
Part 2.1 requires a test of a Responsible Entity’s Recovery Plans “initially upon the effective date of the standard”. Is it proposed that if a Responsible Entity has completed a test 5 months prior to the effective date (complying with the “annual not to exceed 15 months” definition) that the Responsible Entity should do an additional retest on or about the effective date of Version 5? A full operational test of recovery plans as required in Part 2.3 will be burdensome and expensive for smaller entities.
No
A 60 day timeframe for items 3.2-3.4, to be consistent with the recommendation for CIP-008-5, is recommended.
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.
No
Part 1.1 requires a level of detail which is too granular for a baseline. Specifically, scripts and the physical location of a device, while certainly important, are not appropriate for a Change Management baseline. Part 1.2 requires that the CIP Senior Manager approve all changes. However, management approval is what is more appropriate in this instance. Recommend changing language from CIP Senior Manager to simply “Management approval”. Part 1.4 requires that “availability” is tested subsequent to a change. This should be stricken as availability of a BES Cyber System is not under the purview of CIP. Current language of CIP-007-3 R1 is preferable. Part 1.5 is duplicative of Part 1.4. Are Control Centers expected to perform dual testing procedures? This does not add to the security of a Control Center and simply adds additional work. Recommend striking 1.5.
Yes
No
An active vulnerability assessment of test environments as required in Part 3.2 will be burdensome and expensive for smaller entities. Additionally, requiring smaller entities to purchase a vulnerability assessment tool or contract for this service for every install is also burdensome and expensive.
Yes
No
The Measure for Part 1.1 contains the phrase “BES Cyber Security Information” and should be “BES Cyber System Information”.
Yes
No
The VSLs for this standard are either High or Severe. A Responsible Entity with incomplete documentation is at as much risk for penalty as one with no implemented controls. There should be a further level of gradation in the VSL to reflect differences in severity levels. The VSL for CIP-006-5 provides a good example of the appropriate level of VSLs to reflect different degrees of noncompliance.

No
Page 4 contains the phrase “CIP compliance program” yet that term is not defined. Is it intended that a Responsible Entity have a document describing their “CIP compliance program” as a part of their CIP-009-5 recovery documentation?
Individual
Daniel Duff
Liberty Electric Power, LLC
No
No
No
The wording of 1.1 is quite tortured, to say the least. It needs to be rewritten so that the action and triggers are clear.
Yes
Yes
Yes
No
CIP-003 R2 requires tracking of both exit and entry, as opposed to (for example) CIP-006 R1.6, which only requires tracking entry. The purpose of exit tracking is unclear, as is the reliability necessity of exit tracking. I would suggest deleting all reference to "egress" in CIP-003.
Yes
Yes
Yes
No
This time period should be lengthened to account for delays in personnel changes. A job search to fill a vacant position, including required background checks, takes significantly longer than 30 days in most cases. Using a 60 or 90 day window would be more appropriate, and would prevent needless paperwork where delegations are changed and then changed again simply to meet a paperwork requirement.
No
VSLs are not logically consistent - not naming a delegate for one function is considered a moderate VSL, but not changing that person within 30 days is a high VSL.
No
As written, the standard would prevent reasonable cyber access by vendors who maintain generator turbine controls. The standard requires 'individuals' to have site-specific cyber training on all aspects of the site security program. Vendors often have many agents who are capable of working on controls, and requiring each individual technician to sit through dozens of training sessions is not practical, nor does it enhance reliability of the BES.
Yes
Yes
No
See response to Q14.

No
See response to Q14.
No
See response to Q14.
No
The wording of this part of the standard should be "the effective day of the termination or resignation". Many individuals give significant notice of resignation, but would be expected to continue in their job function during the time between the resignation and actually leaving the position.
No
If failure to do a criminal background check on a single individual every seven years is a high violation, then not having background checks in the program should not be a moderate violation. Suggest breaking out this requirement so that one individual not having a complete update every seven years is a moderate, two or more a high VSL.
Yes
No
This section is too prescriptive. Cyber communication is a rapidly changing process, and including static requirements threatens to obsolete a standard, given the length of time needed to make changes to standards. Suggest rewording to "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement processes to mitigate unauthorized access".
Yes
Yes
No
Do not see the reliability gain from requiring exit logging on a "24-hour basis". Note that an individual entered a security perimeter should be sufficient.
No
Use of the electronic devices should be sufficient to demonstrate they are functional without a "test". Standard should be written stating testing is needed only for those security devices not active for a two-year period.
Yes
Yes
Yes
No
Some transient assets will not be under the control of the RE - the equipment used for relay calibrations, for example. There will be problems documenting the history of these assets, and whether they are compliant with this standard.
Yes
No
Password requirements will actually increase the risk to cyber systems, due to human response to strong passwords. The passwords will often be written down, which is the most common way passwords are compromised. Weaker passwords with sufficient bits of entropy will be safer in the long run than requiring 3 character types.
Yes
Yes

No
The RE should have the option of providing training in lieu of a test of the system.
Yes
No
Failure to provide the updated plan to a single individual should not be more severe than not updating a plan when significant faults have been discovered in the plan.
Yes
Yes
Yes
No
Same objection as CIP-008 - failure to notify a single individual of updates is treated as more severe than not updating a plan when faults are discovered.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Puget Sound Energy
Ed Croft
Yes
As criteria 1.4 and 2.13 part 2 read, a Wind Generation Control Center that controls 1500 MW or 300 MW of wind facilities may have associated High or Medium Impact BES Cyber Systems, respectively. Criteria 2.1 and 2.13 should distinguish between controllable generation and intermittent generation sources (i.e. wind and solar), since the loss of intermittent generation facilities happens naturally and regularly and is not viewed as an extreme event. Therefore, if this Control Center or generation's associated BES Cyber Systems are unavailable, degraded, or misused, the impact on the generation should not necessarily be viewed as high or medium impact. There is an overemphasis on Control Center impact versus large generation facilities. For example, a 1400 MW generation facility would only have associated Low Impact BES Cyber Systems (see 2.1), whereas a Control Center that controls 300 MW of generation may have associated Medium Impact BES Cyber Systems (see 2.13 part 2). The only material difference between these two facilities is that the Control Center controls multiple locations of generation, and the generation facility controls one. Part 2 of the Medium Impact criteria (2.13) for Control Centers should either be removed or the MW threshold should be raised

significantly to better match the Medium Impact generation criteria (2.1). Also, the enumeration in 2.13 does not make sense: "Control centers not included in High Impact Rating (H), above, that perform (1) . . , or (2) generation control centers that control 300 MW or more of generation."). The High Impact Generation Operator Control Center criteria (1.4) should be rewritten to clarify whether it is intended to include Control Centers that control one or more generation sites that each generate 1500 MW (2.1), or Control Centers that control a total of more than 1500 MW of generation. The latter meaning is suggested by CIP-002 Version 4 Attachment 1, criteria 1.15.
No
While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have “overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” would benefit from repetition within the R1 requirement itself. Standing alone after the removal of the rationale removal the requirement does not communicate the responsibility adequately.
No
Requirement R2 states that “Each Responsible Entity shall implement one or more documented cyber security policies…" and Measure M2, item 2 states that evidence may include "[r]ecords that indicate the required ten topics were implemented." We would like to see additional clarification of the meaning of the term "implemented". What evidence would be needed to show that the ten topics were "implemented"?
No
There needs to be additional clarity around the timing associated with the reviews and approvals. We believe what is intended is the review by the Responsible Entity and approval by the CIP Senior Manager is a combined event that must be completed initially upon the effective date of the standard and at least once each calendar year thereafter. A proposed content change might be: “Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter. For each cyber security policy, the annual review and approval cycle is not to exceed 15 calendar months.”
No
Proposed content change: Each Responsible Entity shall make its cyber security policies readily available to all individuals who have access to BES Cyber Systems or BES Cyber System Information.
Yes
No
The requirement includes a footnote that should be included within the requirement. Proposed content change: Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change. Delegations do not need to be reinstated with a change in the CIP Senior Manager position or other position with delegation authority.
No
R4 VSL This language cites a High VSL when ‘not all’ individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which ‘it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.’
No
The Measures for item 1.1 indicates that "Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed." The "must," "and" and "not limited to" (underlined above) could be read to imply that evidence above and beyond quarterly reinforcement material is required as evidence. We recommend the following wording change to clarify that, while the program documentation and some evidence of implementation are required as evidence, there is not a prescriptive requirement for what evidence of implementation must be

provided.. "Evidence must include the documented security awareness program, and additional evidence to demonstrate that this program was implemented. Evidence of implementation may include, but is not limited to, the quarterly reinforcement material that has been distributed and documentation of the mechanism used to communicate the awareness content."
No
The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" R2.6 – Requirement – Proposed word change Original - Training on handling of BES Cyber System Information and storage media. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. R2.2 – Should this specify both cyber and physical security controls or is that "just understood"? R2.3 & R2.4 – Should the wording of the requirement and the measure be the same for both sub-requirements, given that they are addressing the same thing for each type of access control system?
No
R3.2 – requirement wording is confusing. Draft "requires" training "at least once every calendar year but not to exceed 15 calendar months." If it can go to 15 calendar months, then it is NOT required at least every calendar year. Propose re-wording along the lines of, "Training should be completed every calendar year but is required at least every 15 calendar months."
No
4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7-year cycle background checks. Comments: R4.2 – The draft wording allows for gaps in the information required from an individual, as they would not need to provide information on where they lived, worked, or went to school (other than currently) if the duration was less than 6 months. Therefore, if someone moved/changed jobs after less than six months, that information could be excluded from the criminal history check. R4.4 – It is not clear why contractors must be separated out, rather than just having R4 be applicable to all individuals needing the access, regardless of their employer.
Yes
No
R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary'. Comments: R6.3 – The measure, which requires a list of authorized people for BCSI would be problematic, since a person on the list, who owns BCSI, could share that BCSI with someone not on the list but who met all the requirements of R4. "Need to know" can be determined on a dynamic basis, and it would seem to potentially hamper workflow, if someone had to run through a process to show a diagram to someone. [[SSB: this one is a stretch, but not much harm in trying]] R6.5 & R6.6 – Same comment about timeframes as listed in item #15 above.
No
7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). The requirement may better address this issue by changing the wording to something like "For reassignments or transfers, review the individual's electronic and physical access to BES Cyber Systems by the end of the next calendar day. Revoke access when it is determined to be no longer needed." 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.
Yes
No

R1.1 – This appears to address LIBCS & associated PACS; however, R1.2, R1.3 & R1.4 appear to address MIBCS, associated EACMS, associated PCA, but not associated PACS? Is this the intent? R1.2 & R1.3 –These requirements appear to now require the deployment of exit card readers at Medium and High sites – is that the intent? R1.4 – This requirement appears to address only actual access and eliminates access "attempts" – is this the intent? Also, how does this requirement apply to AEACMS or APCA, unless it is because they are required to located within a DPB? R1.6 – The change would make log retention duration 3 years. This is a big issue for video log storage . Also, this would seem to be both for authorized personnel and visitors? Since visitors are addressed in R2, this should probably say something like “Log (…) of individuals authorized unescorted physical access into each DPB….” to maintain consistency with the full definition of an authorized person, since a visitor can be an “authorized” person, they just can’t be unescorted. Also, the requirement does not appear to require tracking the time of entry into a DPB—is this the intent?? R2.2 –Requirement wording change for consideration: “A process requiring manual or automated logging of access by visitors into a DPB, which includes the date and time of first entry and last exit, the visitor’s name, and individual point of contact.”
No
R3 – Is this for commissioning the PACS or the DPB? Also, this would seem to imply that if you performed maintenance on a card reader, it would not need to be part of a later full system test?
Individual
Joanna Luong-Tran
TransAlta Centralia Generation
Yes
1. The criterion 1.4. There is no explanation why a BES Cyber Asset (BES Cyber System) located at the Control Center would have higher impact than another BES Cyber Asset (BES Cyber System) located outside the Control Center. In the case that the above two BES Cyber Assets (BES Cyber Systems), that if rendered unavailable, degraded, or misused, would have impact on the same

facilities identified in the criteria 2.1, 2.3, 2.4, or 2.12 in the same location, then, the impact on the BES would be same no matter where the locations of BES Cyber Assets (BES Cyber Systems) are. For example, an operator console is used solely to control/operate the Blackstart Resources in one location. If it is in a Control Center, it would be categorized as High Impact (criterion 1.4), while if it is outside the Control Center, for example, in a room at the Blackstart Resource's location, it would be categorized as Medium Impact (criterion 2.4). But if this console were rendered unavailable, degraded, or misused, the impact would be the same, i.e. the Blackstart Resources at this location would not be available. This case is different from another case that, if an operator console, located in a Control Center, controls/operates two Blackstart Resources, and these two Blackstart Resources are at two different locations, then the impact would be higher, i.e. affecting two Blackstart Resouces in two different locations, wider area impact. Based on the above argument, it is recommended the following change of the criterion 1.4, "Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator that includes control of one two or more of the assets identified in criteria 2.1, 2.3, 2.4, or 2.12, below, and these assets are at two or more location." 2. The criterion 1.4 has a reference to 2.12. But the criterion 2.12 is about the UVLS and UFLS. All the UVLS and UFLS standards are not applicable to GO/GOP. Generator Operators do not perform any obligation with UVLS and UFLS. Thus, it is recommended removing 2.12 in the criterion 1.4. 3. The criterion 2.13 (2), generation control centers that control 300MW or more of generation. We do not agree the 300MW number and justification in the guideline and suggest removing this 2.13 (2). The rationales are, a. In the case of a generation control center to control 300 MW, BES Cyber Systems (BES Cyber Assets), if rendered unavailable, degraded, or misused, would have an impact to cause the 300MW generation change. For a single unit of 500MW, its associated BES Cyber Systems (BES Cyber Assets) locally located at the plant, if rendered unavailable, degraded, or misused, would have an impact to cause the 500MW generation change. In the view of generation change, the second one has higher impact than the first one. But according to the criteria, it is opposite. Can the drafting team look at this situation and provide some explanation? b. The guideline says "The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold." We do not agree this statement here. The UVLS and UFLS are the last ditch efforts to save the BES, but the loss of 300 MW generation does not automatically trigger the 300MW load shedding (last ditch efforts). The UVLS and UFSL are triggered by the voltage and frequency, not directly by the generation loss. So the using the 300 MW from UVLS and UFLS is inappropriate for the generation loss. c. For the generation loss, the criterion 2.1 uses 1500MW. This number has been agreed by the industry during the version 4 standard development. In the view of generation loss, the BES Cyber Systems (BES Cyber Assets) in the generation Control Center should be categorized according the criterion 2.1, irrelevant to the BES Cyber System (BES Cyber Assets) location. Thus, there is no need to add a separate criterion to categorize the BES Cyber Systems (BES Cyber Assets) in the generation Control Center.
No

No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No
No

Individual
Mario Lajoie
Hydro-Québec TransÉnergie
No
since there is no place for on general comments, see responses in the to the last question (49) Under "BES Reliability Operating Services" • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary Term -- in “Facility operational data and status” under “Inter-Entity Real-Time Coordination and Communication” o Request clarification on the scope of this “Operational Directives”. Does it include company messaging system? Two way radios? What is the relationship with the new COM-002? o Request clarification that these Coordination and Communications are limited to Reliability not Market Systems • recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret
Yes
HQT recommends that CIP-002-5 allow the use of a risk-based methodology or the bright line criteria stated in Attachment 1to identify critical assets. To ensure consistency within the industry, the methodology used and the results should be subject to approval by a panel of expert (for example, the NPCC TFIST for the NPCC Region and equivalent Task Force for other Regions). HQT also note that inconsistencies may arise from V4 to V5 based on the fact that the concept of Critical assets no longer exist in CIP-002-5. So this is not true to state that “most of these criteria are similar to those approved in version 4” The 15 minutes windows is not a criteria that is repeatable as it may be influenced by system conditions. The following criteria will need to be improved: 2.2 “Net Reactive Power” should be read as “Absolute value of Reactive Power” to consider Static VAR compensator and synchronous condenser 2.3 What means this criteria? How will it apply? 2.7 How a weighted value of a line is related to reliability? The number or the operating voltage are not reliability criteria. IROL, system restoration, voltage control, frequency control, interchange, load/generation balance are reliability criteria to consider.
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation” For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities (” R1 : All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. In CIP-005-5 R1.1 and CIP-006-5 R.1.1, how can we define operational or procedural controls to restrict unauthorized electronic access or physical access if we didn't previously identified those assets either globally or specifically in CIP002-5 R1? R1 should required at least identification of type (or any other logical grouping) of LI BES CA (e.g. RTU-remote terminal unit) R1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. Transient Cyber Asset definition indicates a connection limit of 30 calendar days and here, we allow something to be considered in a lower impact category if it is intended to be in service for 6 calendar months or less. It seems to have a gap between 30 calendars days and 6 calendar months for these BES Cyber Assets. If these are LI BES CA, they could then easily pass under the radar, possibly not being identified (see previous comment on R1). M1. Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls. Does it mean the controls in CIP-005-5 R1.1 and CIP-006-5 R.1.1 could be used as evidence for CIP-002-5 R1? Isn't it like a circular reference? R1 Should add to R1, identification of "transient cyber assets". TCA could be a major threat source and should be "controlled".

No
For clarity in R2 and M2, request 1) using the term “annual” instead of all these extra words and 2) making “annual” a Glossary term
Yes
No
R1 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] According to Order on Violation Risk Factors, 119 FERC 61, 145 (May 18, 1907) and Guidelines for Developing Violation Risk Factors and Violation Severity Levels NERC (August 10, 2009), this requirement is administrative in nature, is in a operation planning time frame and if violated, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES, or under the emergency, abnormal, or restorative conditions anticipated by the preparations, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES. So this VRF should be "Lower" as it is for R3 and R6.
Yes
R2 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] Efficiency of a policy is not evaluated here. A bad policy is often not better or could be even worse than no policy at all. Thus, violating this requirement should not have a medium factor risk. Should be "Lower" as previous comment on R1… and the same VRF as R3.
Yes
The term “annual” is not used consistently in the Rational, Requirement and Measure. Request a consistent use of “annual” throughout R3.
No
M4’s last bullet on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4. M4. Evidence may include, but is not limited to: • Policies are accessible on the corporate Intranet site • Documented records that policies have been provided to contactors where access to BES Cyber Systems is authorized • Policies are posted on company bulletin boards Because policies would be accessible to everyone, particular attention should be taken to be those policies are exempt of BES Cyber System Information.
Yes
No
Requirement has a typo. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes? Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”
Yes
Yes
No
Request clarification of whether personnel with access to only protected information need training / awareness. SDT should include this as additional Requirement Should be able to exclude people using BES cyber system in consultation only and has no impact on the operability of it Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and (R2.3 and R2.4) Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
No
R3 Part 3.1 & 3.2 - Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets R3 Require completion of the training specified in CIP-004-5 R2… where applicability is limited to: - High Impact BES Cyber Systems - Medium Impact BES Cyber Systems So it is useless here to apply it larger. Should have the same "Applicability" for both

R2 and R3.
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to "grandfather" previous seven-year criminal checks executed for the previous versions of CIP Standards. The additional language should spell out when this "grandfathering" expires, which is also when new check will be required R4 [Violation Risk Factor: Medium] [Time Horizon: Operations Planning] According to Order on Violation Risk Factors, 119 FERC 61, 145 (May 18, 1907) and Guidelines for Developing Violation Risk Factors and Violation Severity Levels NERC (August 10, 2009), this requirement is administrative in nature, is in a operation planning time frame and if violated, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES, or under the emergency, abnormal, or restorative conditions anticipated by the preparations, would not be expected to affect the electrical state or capability of the BES, or the ability to effectively monitor, control, or restore the BES. Like it is for R6 "Access Management Program", this VRF should be "Lower"
No
For clarity, recommend changing 5.1 from "authorized electronic or unescorted physical" to "authorized electronic or authorized unescorted physical"
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information. Part 6.1 to part 6.6 – Applicability Associated Protected Cyber Assets Here the definition given in this CIP is too restrictive. Instead, we should used "Protected Cyber Assets" as given in CIP v5 Definition: meaning all cyber asset inside an ESP. R6 Part 6.5 – Requirements : Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. Before requiring some verification, the Access Management Program should require specification/identification of such accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. R6 Part 6.6 – Requirements : Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions.Before requiring some verification, the Access Management Program should require specification/identification of such access privileges are correct and the minimum necessary for performing assigned work functions. R6 Access Management Program Like R4 Personnel Risk Assessment, Program and R5 Personnel Risk Assessment, may be the R6 Access Management Program should be broke in 2 different requirements: "Access Management Program" and Access Management"
No
Request that 7.1's footnote be moved into the Requirement Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements Recommend changing 7.4 from "For

resignations or terminations," to "For terminations, resignations, reassignments, or transfers," What about the individual's user accounts on Protected Cyber Asset? It's possible that user have only user accounts on Protected Cyber Asset and any on BEC Cyber Assets. Should be reworded to: For resignations or terminations, revoke the individual's user accounts on Cyber Assets… Recommend changing 7.5 : Here the definition given in this CIP is too restrictive. Instead, we should used "Protected Cyber Assets" as given in CIP v5 Definition: meaning all cyber asset inside an ESP.
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Part 1.2 Applicability : High Impact BES Cyber Systems, Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Protected Cyber Assets Should add: "Associated Electronic Access Control or Monitoring Systems Following basic security principles, those cyber assets should have at least the same protection level that the cyber asset that they control. Because proposed revised (see comment) definition of Electronic Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems exclusive of Electronic Access Point composing the Electronic Security Perimeter", there will have no problems for that cyber asset to be protected by one Electronic Security Perimeter: it is not a fence over the fence situation. We have to keep in mind that AEACMS include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems. 1.1 Change Rationale: Entities are to document perimeter type security controls they have implemented to segment low impact BES Cyber Systems from public or other less trusted network zones and… What is the meaning of less trusted network zones? Is it all other network zones outside an ESP? Does the corporate network a less trusted network zones?
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete R2.2 ADD "if technical possible" meaning add the possibility to have a TFE for this requirement. When not possible to have log every day "Real time" systems R2 : hould add another part in R2 –Remote Access Management requiring the Intermediate Device should not be located within ESP. It is implied by definition of "protected cyber asset" are all those asset within the ESP that are not BES cyber asset and by R2.1 where it is specified that a Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset. If ID is implement within the ESP, it should be considered as a PCA and then not directly accessible. If it is not specifically required, then someone could implement the ID within the ESP and there is no violation of any requirement. Should add requirements, guidance or definition about Cyber Assets associated with communication networks and data communication links within Electronic Security Perimeters (like Ethernet switches and routers) because their misconfiguration or unavailability could have a direct impact to BES CA. Their management should be done thru an Associated Electronic Access Control or Monitoring Systems. Should add requirement to "issue real-time alerts (to individuals responsible for response) in response to detected malicious communication at any EAP of a Electronic Security Perimeter", as with CIP-006-5 R1.4, for physical counterpart This is included by CIP-007-5 R4.2, but is it the right place? Should add requirements for logging of electronic access thru EAP of a Electronic Security Perimeter", as with CIP-006-5, R1. 6 for physical counterpart. Partially included by CIP-007-5 R4.3 but is it the right place? Should add requirements for testing of the AEACMS at EAP of a Electronic Security Perimeter to ensure the required functionality is being provided, as with CIP-006-5 R3.1 for physical counterpart Should add requirements for logging dates, time, and duration for failures or outages of access control, logging, and alerting systems of the AEACMS at EAP of an Electronic Security Perimeter to ensure the required functionality is being provided, as with CIP-006-5 R3.2 for physical counterpart.

Yes
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request Requirement 1.2 be updated to allow "escored physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point" For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6 R1.3 The verification of outbound traffic is considered overkill since must attacked are from inside. For companies that have strong unions it could be difficult to be compliant to this requirement. Part 1.2 Applicability Medium Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Should add: Associated Physical Access Control Systems Because definition of Physical Access Control Systems: "Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." There are no problems for that cyber asset to be protected by one Defined Physical Boundaries: it is not a fence over the fence situation. Part 1.3 Applicability High Impact BES Cyber Systems. Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Should add: Associated Physical Access Control Systems Because definition of Physical Access Control Systems: "Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." There are no problems for that cyber asset to be protected by one Defined Physical Boundaries: it is not a fence over the fence situation.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1 Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, " Part 2.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Part 2.1 Requirements Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.Applicability column is wider than the requirement that limit the identification of source or sources that are monitored for the release of security related patches, or updates for all software and firmware only to those associated with BES Cyber System or BES Cyber Assets. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability.
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" R3.1: Return to 36 months. Require clarification on maintenance, can a normal maintenance on an appliance can be considered as maintenance.
Yes
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity chose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? R1 and R2: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement
No

Request clarification of "remediation" in 2.2 since it reads that the patch must be applied,which does not allow to have an exception when applying the patch is the worse scenario such as creating a denial of service For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied" What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process? R1 and R2: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement

No

Request allowances in 3.3 for signatures/pattern updates that cause trouble Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media" The Measure for 3.4 does not match the Requirement R3.3: Signature that require “Engine restart may ne require for version. 30 days is short for “Real time systems” and a different delay (longer) for Medium since the High will go first. Part 3.3 – Requirement Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). As for R2 Security Patch Management, and demonstrated by event McAfee DAT 5958 (2010-04-22), applying an update of malicious code protection without prior verification of signatures or patterns file could jeopardize the availability or integrity of the control system. This requirement should be reworded to handles the situation where malicious code protections updates can come from an original source (such as an ant-virus vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. As again R2, timeframe should run from availability from this second source. R3.5: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. If we have a paper log it does not prove anything. Part 3.5 Requirements Log each Transient Cyber Asset connection. This requirement should be move to CIP-005-5 because it is more related to Electronic Security Perimeter than this CIP more oriented about "system". (see comment in CIP-005-5)

No

Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". We recommend one month as a compromise between the prior version's 90 days and the suggested one week R4.1.4: Any detected malicious activity is too wide. Need to be clarified (double avec TFIST) R4.3: ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. When not possible to have log every day “Real time” systems We consider it to be not required. 24hr delay is short and too many operational and temporary situation may arise which come back to normal shortly after(24 – 48hrs) R4.5: Every 2 weeks does not match with timeframe of R4.3.When we have automatic events correlation, the 4.5 should not be required every 2 weeks. We suggest 60 days. Part 4.1 Requirements Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: Cyber Security Incidents is capitalized here and not defined in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" but BES Cyber Security Incidents and it seems having some discrepancy between the meanings of these terms. Should be revised. Part 4.1 Requirements 4.1.1. Any detected failed access attempts at Electronic Access Points This requirement should be move to CIP-005-5 because it is more related to Electronic Security Perimeter than this CIP more oriented about "system". (see comment in CIP-005-5) Successful access thru an EAP should be logged too. In fact, it should be reworded to include all inbound and outbound successful or failed access thru an EAP.

No

For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses." R5.5: Why the TFE was removed? ADD “if technical possible” meaning add the possibility to have a TFE for this requirement. When not possible to have log every day “Real time” systems. Part 5.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or

Monitoring Systems Associated Protected Cyber Assets Part 5.1 Requirements Validate credentials before granting electronic access to each BES Cyber System. Applicability column is wider than the requirement limiting to validate credentials before granting electronic access only to BES Cyber Systems. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability Part 5.4 Requirements Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. This requirement should be reworded as "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" be placed in "Applicability" instead of "All Responsible Entities"
Yes
No
Part 5.1 Applicability High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets Part 5.1 Requirements Validate credentials before granting electronic access to each BES Cyber System. Applicability column is wider than the requirement limiting to validate credentials before granting electronic access only to BES Cyber Systems. Should be reworded to remove this limitation to be sure that is applicable to all cyber asset indicated in the column Applicability Part 5.4 Requirements Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. This requirement should be reworded as "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" be placed in "Applicability" instead of "All Responsible Entities"
No
2.1 is a new Requirement. Request the rationale for this new Requirement Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." For 2.2, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard"
No
For 3.1, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Recommend that 3.2 wording be consistent with the 2.2 wording For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2"
Yes
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process.
Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification , is “full operational exercise” the same as “functional exercise” as described in the rational? For 2.1 and 2.3, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative

environments". What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing "or when BES Cyber Systems are replaced" as it addressed in CIP-009 R3.4 and 2) removing "and document any identified deficiencies or lessons learned" as they are addressed in CIP-009 R3.2 and R3.3. For 3.1, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
Yes
No
Recommend changing 1.3 to avoid double jeopardy from "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets" Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold R1.1.4: We consider that baselines for "scripts" is a little extreme, need clarification on the type of script required R1.1.5: The requirement is redundant and is already documented in CIP-007-5 R1 R1.4.2: Add to this requirement the possibility to add the level of criticality. Not all changes require the verification. Have the possibility to classify the changes by type and level
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception
No
For 3.1 and 3.2, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard" Recommend changing 3.2 from "in a production environment." to "in a production environment, or a production environment." to allow Entities more flexibility in meeting this Requirement
Yes
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. For 1.3, see the general comment on "initial bookend" aka "Initially upon the effective date of the standard"
No
Request that footnote 2 in 2.1 be moved into that Requirement R2.2: Suggestion of wording for the requirement " Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media". The objective of this requirement is to ensure that the data is not readable, the use of destroy is a little "over kill"
Yes
No
We understand that the table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Since Version 4 is not FERC approved, we are concerned about the possibility of version 4 being effective

while version 5 is in implementation, resulting in version 4 being effective for only a few months. Since there is no place for general comments, we provide them here • We understand that the auditors are not bound by the Measures. Request an explanation on the need for Measures if auditors are not bound by the provided Measures? What is the benefit to these Measures? Should the SDT's time be better invested elsewhere? • Recommend removing the "initial bookend" from the Requirements that specify period because eight activities (CIP-008 2.2, CIP-008 3.1, CIP-009 2.1, CIP-009 2.3, CIP-009 3.1, CIP-010 3.1, CIP-010 3.2, CIP-011 1.3) in these Standards that are unnecessarily burdensome to Entities. Another reason to remove these initial bookends is that the initial bookend's language forces the Entity to be compliant with two Versions of the Standards at the same time. We are not objecting to the initial bookend in other Requirements which are policy-oriented. The effective date should be the start of the period. Initial bookend typically says "Initially upon the effective date of the standard". • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different than other Standards. • Request clarification of the capitalized term "Facilities." Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Individual
Annette Johnston
MidAmerican Energy Company
Yes
GENERAL DEFINITIONS COMMENTS: Version 5 proposes retiring three definitions and creating or revising 21 definitions. The NERC request form for development or revision of a definition for a term states the development of new definitions should be avoided unless absolutely necessary. The majority of these changes are not required to address FERC Order 706 directives or improve security and in a number of cases the changes introduce ambiguity instead of clarity. NERC's first annual report to FERC on TFEs was filed in September 2011 and noted that 241 entities had declared Critical Cyber Assets. These entities are complying with all of the CIP standards. Changes in terms require extensive resources to modify existing compliance programs. Proposed changes that are not for a directive and/or don't improve security should not be made. CRITICAL ASSETS and CRITICAL CYBER ASSETS COMMENT: Do not retire Critical Assets or Critical Cyber Assets. MidAmerican Energy supports retaining CIP-002-4, the legacy framework for identification of Critical Cyber Assets and adding impact categorization. Renaming the concept of Critical Cyber Asset serves no security purpose and only increases implementation costs and confusion for personnel trained in and operating CIP programs in place today. MidAmerican Energy supports a separate standard to identify which Critical Cyber Assets are designated as high impact and what additional controls they receive. As a result, Critical Cyber Assets would be either medium or high impact. MidAmerican Energy supports a separate standard to identify low impact Cyber Assets. The standard for lows would not use the term Critical Cyber Asset. PHYSICAL SECURITY PERIMETER COMMENT: Do not retire Physical Security Perimeter. Version 5 renames the term and revised the term's definition. Renaming the term serves no security purpose and is not a directive. It increases implementation costs. If it can be demonstrated that it will not reduce security, the definition for the term could be revised to drop "six-wall" in order to provide more flexibility (without changing the name for the term). BES CYBER ASSET COMMENT: Retain Critical Cyber Asset. Do not create this new definition. FERC Order 706 did not direct changes to Critical Cyber Asset. See Order 706 paragraph 284, where FERC "declined to direct that such a method" (for identifying Critical Cyber Assets) be incorporated in the standards. See also paragraph 285, where FERC "did not find sufficient justification to remove this provision" (Critical Cyber Asset must either have routable protocols or dial-up access). Industry produced a guidance document for identifying Critical Cyber Assets. The proposed definition has many ambiguous terms and references another new, ambiguous definition for BES Reliability Operating Services. Version 5 materials have not identified what delta (or difference in outcome) is intended by the proposed definition versus the existing framework. BES CYBER SECURITY INCIDENT COMMENT: Retain the current definition of Cyber Security Incident. Addition of "BES" in the term name is not a directive, adds no security and increases implementation costs. As commented elsewhere in this question, MidAmerican Energy supports retaining Critical Cyber Asset and Physical Security Perimeter, which are included in the existing definition, and does not support creating the new term of Defined Physical Boundary. BES CYBER SYSTEM COMMENT: MidAmerican Energy supports retaining CIP-002-4 and the legacy framework for identification of Critical Cyber Assets and does not support the CIP-002-5

framework for identification. However, MidAmerican supports the concept of grouping one or more Cyber Assets for flexibility so that some controls can be addressed at a "system" level. If a new definition is created, it should be based on grouping Cyber Assets for purposes of applying security controls at a system level. Do not use "BES." Consider what Cyber Assets can be grouped. The draft definition only included 15 minute impact (BES Cyber Assets) and did not include the option of grouping "Protected Assets." Why not? Aren't there any controls that could be applied to those assets at a "system" level? The concept of excluding Transient Assets from the system is important to retain. BES CYBER SYSTEM INFORMATION COMMENT: The draft definition uses reworded content from CIP-003-4 R4.1 and adds "BES." There is no directive, it does not increase security and does increase implementation costs. MidAmerican can support creating a definition from the CIP-003-4 R4.1 language unchanged. This language is: "The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information." BES RELIABILTY OPERATING SERVICES COMMENT: Drop this draft definition. It is 736 words full of ambiguity and lacking clarity. It creates multiple dependencies on other NERC Glossary terms and other NERC standards. It is not a directive. Version 5 materials have not identified what delta (or difference in outcome) is intended by the proposed definition versus the existing framework or if it improves security. Consideration could be given to comparing the content of the draft definition, the 2009 concept paper, ACTUAL identified Critical Cyber Assets and the NERC guideline to determine if there is a gap or lack of clarity, and the guideline could be revised. CIP EXCEPTIONAL CIRCUMSTANCE COMMENT: Version 4 requirements in CIP-004-4 R2 and R3 refer to specified circumstances such as an emergency. Start the definition with "One or more of the following circumstances, or other conditions of similar nature." CIP SENIOR MANAGER COMMENT: No comment. CONTROL CENTER COMMENT: Delete the bullets for presentation and display of BES reliability or operability data and the bullet as too ambiguous. Delete the bullet for coordination of BES restoration activities as too ambiguous. Clarify the modifying phrases as follows: "two or more transmission facilities at two or more locations or for two or more BES generation facilities at two or more locations where the aggregated generation is 300 MW or more." Ensure substations are not swept in as control centers just due to data concentrators. Revise BES Cyber Asset to Critical Cyber Asset to correspond to retaining CIP-002-4. CYBER ASSETS COMMENT: Keep Cyber Assets revision as it aligns with FERC Order 706 paragraph 285 where FERC "did not find sufficient justification to order the inclusion of communication links." DEFINED PHYSICAL BOUNDARY ("DPB") COMMENT: Do not adopt this definition. See comments on Physical Security Perimeter. ELECTRONIC ACCESS CONTROL OR MONITORING SYSTEMS COMMENT: The name for the term should be Electronic Access Control Systems and drop "monitoring" in the name to be consistent with Physical Access Control Systems. Drop the reference at the end of the definition to "or BES Cyber Systems." In this definition, does monitoring mean alerting and logging? If so, say so in the definition sentence. In other places, version 5 is using "alert" instead of "monitor," for example, in CIP-006 which says "control, alert or log." ELECTRONIC ACCESS POINT ("EAP") COMMENT: MidAmerican does not support the version 5 concept change away from the logical boundary or this definition as drafted. Also, as drafted, the definition lacks the concept of external connectivity and consequently could be applied to identify multiple access points between Cyber Assets within the ESP because some functionality on those Cyber Assets restricts communications between Cyber Assets. Retain the CIP-005-4 ESP logical border concept and electronic access point. If the existing definition is revised, it could be to specify the access point is an interface. It might also be revised to address CIP-005 interpretations. Changes were not, however, directed by 706. EXTERNAL CONNECTIVITY COMMENT: Revise to: "Routable or dial-up data communication through an Electronic Access Point between a Cyber Asset inside the Electronic Security Perimeter and a device external to the Electronic Security Perimeter." EXTERNAL ROUTABLE CONNECTIVITY COMMENT: Revise to: "Routable data communication through an Electronic Access Point between a Cyber Asset inside the Electronic Security Perimeter and a device external to the Electronic Security Perimeter." (Revised to be consistent with External Connectivity.) INTERACTIVE REMOTE ACCESS COMMENT: No comments. INTERMEDIATE DEVICE COMMENT: No comments. PHYSICAL ACCESS CONTROL SYSTEMS COMMENT: Drop Defined Physical Boundary and return to Physical Security Perimeter. PROTECTED CYBER ASSET COMMENT: In versions 1 through 4, these are noncritical. If a definition is created, it should use the existing term of noncritical. "Noncritical Cyber Asset - A Cyber Asset using routable protocol and connected within an Electronic Security Perimeter, excluding Critical Cyber Assets and Transient Cyber

Assets." REPORTABLE BES CYBER SECURITY INCIDENT COMMENT: Comments on this definition are not ready at this time, awaiting the next actions on the revisions to the EOP standard. TRANSIENT CYBER ASSET COMMENT: Refer to Critical Cyber Assets and Noncritical Cyber Assets. Might Transient Cyber Assets also be connected to Electronic Access Control Cyber Assets? "A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a Cyber Asset inside an Electronic Security Perimeter, 2) … and 3)…"
Yes
GENERAL CIP-002 COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC. Accomplish categorization in a separate standard for high impact Cyber Assets and in a separate standard for low impact Cyber Assets. The industry has met FERC Order 706 directives for CIP-002. GENERAL CIP-002-5 ATTACHMENT COMMENTS: The specific delta (or difference in outcome) of the proposed Attachment I changes has not been identified or supported in the version 5 materials.
No
R1 REQUIREMENT COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC. Accomplish categorization in a separate standard for high impact Cyber Assets and in a separate standard for low impact Cyber Assets. The industry has met FERC Order 706 directives for CIP-002.The specific delta (or difference in outcome) of the proposed framework changes has not been identified or supported in the version 5 materials. NERC's first annual report to FERC on TFEs was filed in September 2011 and noted that 241 entities had declared Critical Cyber Assets. These entities are complying with all of the CIP standards. Retaining the version 4 framework allows entities to preserve and leverage investments in versions 1 through 4 and evolve to version 5. There was significant industry opposition to the version 5 framework change in the 2009 concept paper. These concerns continue to be valid today: unclear where to start, too broad, abstract, too complex, does not provide any additional clarity or value versus the current process and does not provide detail as to why the proposed concept is an improvement or will improve reliability. It will increase implementation costs for entities with existing programs. It has the potential to impede timely progress in resolving remaining FERC directives and implementing security improvements in the other CIP standards.
No
R2 REQUIREMENT COMMENTS: Retain CIP-002-4 and Attachment I as approved by industry and NERC BOT and recommended to FERC.
No
This standard has a high VRF that applies to requirements for both high and medium impact asset categories. We recommend a medium VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with proposed revisions to CIP-002 and the VRFs.
No
GENERAL COMMENTS ON CIP-003-5 Most of the changes made to CIP-003 were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these also need revisions to be more in line with our proposed changes to the requirements. See also comments on CIP-010-1 and CIP-011-1. MidAmerican Energy does not support moving CIP-003-4 R6 to the a new CIP-010-1 separate standard. MidAmerican Energy does not support moving CIP-003-4 information protection requirements to the new CIP-011-1 separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within CIP-003-4 and preserve the numbering of the requirements within this standard. We propose the following requirements for CIP-003-5: R1: Cyber Security Policy R2: Leadership R3: Exceptions R4: Information protection The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. EXCEPTION COMMENTS: The V4 to V5 mapping document states that CIP-003-4 R3 Exceptions was deleted because "the FERC Order 706 made clear that you could not take exceptions to the policy." MidAmerican disagrees with this statement. In paragraph 376, FERC directed the ERO to "clarify that

the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards." Further, in paragraph 377, FERC stated "We do not believe that an entity's decision to not follow its cyber security policy in a particular situation should trigger a penalty, as long as no Reliability Standard Requirement (other than Requirement R1 in CIP-003-1) is violated as a result." Paragraphs 372 through 378 include discussion on documentation of exceptions and oversight by the ERO and Regional Entities. While the new term "CIP Exceptional Circumstance" has been introduced in Version 5, its use is limited to three standards (CIP-004, CIP-007 and CIP-010). There are situations outside of these three standards that may require an exception to the cyber security policy. Therefore, MidAmerican suggests going back to the Version 4 language for exceptions and modifying it to meet the FERC directive. R1 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to the language in CIP-003-4 R2 for leadership and making minor modifications to address FERC directives not already addressed.
No
R2 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to the language in CIP-003-4 R1 on the cyber security policy. FERC directed the ERO to provide additional guidance for topics and processes that the cyber security policy should address, but FERC did not direct any changes to the requirement itself. R2 REQUIREMENT PROPOSED REVISED TEXT: "Document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following: * The cyber security policy addresses the CIP standards, including provision for emergency situations; The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets; * Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2."
No
R3 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R1 language, which includes the annual review and approval by the senior manager.
No
R4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R1 language, which includes a requirement to make the policy readily available to personnel who have access to Critical Cyber Assets. There was no FERC directive to change this requirement.
No
R5 REQUIREMENT COMMENTS: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R2 language, which includes language on delegations. FERC Order 706 did not direct any changes to the requirement. The draft requirement would create an additional administrative burden that does not improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work.
No
R6 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be deleted, in conjunction with our suggestion to go back to the CIP-003-4 R2 language, which includes language on changes to the senior manager. FERC Order 706 did not direct any changes to CIP-003-4 R2.2. Proposed changes do not increase security over the current requirement but do increase implementation costs. The current requirement already covers changes to the senior manager that must be documented within thirty calendar days of the effective date.
No
This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the proposed revised VRFs and other revisions proposed to the requirements. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" We think some of the CIP-003-5 requirements could have gradated VSLs particularly as most of these requirements have lower Violation Risk Factors.
No
GENERAL COMMENTS ON CIP-004-5 Many of the changes made to CIP-004 were not directed by

FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. Further, CIP-004-4 states the entity will keep all documentation and records from the previous full calendar year unless directed by the Compliance Enforcement Authority to retain specific evidence for a longer period as part of an investigation. Version 5 expands this to three calendar years without justification. CIP-004 requirements generate a tremendous amount of detail records. The "canned" C.1.2 Evidence Retention section in this standard should be revised to correspond to the current obligation. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access R1 REQUIREMENT COMMENT: There were no FERC directives to change the language of this requirement. MidAmerican Energy proposes going back to the version 4 language. We would not be opposed to moving the mechanism examples to guidelines. R1 REQUIREMENT PROPOSED REVISED TEXT: "Establish, document, implement and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms, such as: direct communications (for example, e-mails, memos, computer-based training); indirect communications (for example, posters, intranet, brochures); management support and reinforcement (for example, presentations, meetings)." R1 APPLICABILITY COMMENTS: Revise to medium and high impact assets.

No

R2 REQUIREMENT COMMENTS: Many of the changes made to this requirement were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. MidAmerican Energy suggests the FERC directives be addressed within a structure and language that is more in line with version 4. MidAmerican has provided an example of how FERC directives could be incorporated into the version 4 structure. The draft version 5 did not address FERC Order 706, paragraph 435, which directed determination if modifications should be made to assure security trainers are adequately trained themselves. While we do not believe modifications are needed, we think the directive must be addressed somewhere in the draft standard so that FERC is aware of the determination on this directive. R2 REQUIREMENT PROPOSED REVISED TEXT: "R2.1 Establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets so that personnel understand how their actions or inactions could, even inadvertently, affect cyber security of all Cyber Assets within an Electronic Security Perimeter. R2.2 Review the cyber security training program annually, at a minimum, and update whenever necessary. R2.3. Ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency. R2.4. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-5, and include, at a minimum, the following core training elements appropriate to personnel roles and responsibilities: R2.5.1. The proper use of Critical Cyber Assets; R2.5.2. Physical and electronic access controls to Critical Cyber Assets; R2.5.3. The proper handling of Critical Cyber Asset information; R2.5.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. R2.5.5. Networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of Critical Cyber Assets. R2.6. Maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records."

No

MidAmerican Energy proposes deleting this requirement, in conjunction with the suggested restructuring of R2 back to the version 4 language, since it already is covered.

No

R4 REQUIREMENT COMMENT: FERC Order 706, paragraph 443, directed change to require completion of personnel risk assessments before granting access. This change was made in an earlier version of the standard. There were no other FERC directives for the personnel risk assessment program requirement. We recommend version 4 language and numbering for CIP-004, R3 be retained. This

would mean using one table rather than two. R4 REQUIREMENT PROPOSED REVISED TEXT: (Note: Numbering would become R3) “R3 Document a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. Conduct a personnel risk assessment pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include: R3.1. Ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position. R3.2. Update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause. R3.3. Document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-5.”

No

FERC Order 706, paragraph 446, states the ERO should consider the issue of reviewing results of personnel risk assessments (PRA). This was not a directive. MidAmerican Energy would support the addition of criteria or a process for reviewing results of PRAs, but we suggest it be incorporated into the requirement discussed in question #16 (that MidAmerican would renumber to the legacy R3).

No

R6 REQUIREMENT COMMENT: In FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the senior manager responsible for everything. We do not support requiring the CIP senior manager or delegate to authorize access as drafted in R6.1, R6.2 and R6.2 or the addition of ambiguity with the phrase “minimum necessary.” The version 5 draft is an additional administrative burden that does not commensurately improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work. As mentioned in our comments on CIP-003, we propose retaining the existing V4 language for the leadership requirement. We propose the FERC directive on revocation of access be incorporated into the structure and wording from CIP-004-4 R4. CIP-004-5 R4 REQUIREMENT PROPOSED REVISED TEXT: Note: Under our proposed structure, this would become R4. “R4: Maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets. R4.1. Review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. Ensure access list(s) for contractors and service vendors are properly maintained. R4.2. Revoke such access to Critical Cyber Assets: R4.2.1 at the time of termination for personnel terminated for cause R4.2.2 by the end of the next calendar day for personnel who no longer require such access to Critical Cyber Assets.” MidAmerican Energy does not support CIP-004-5 R6.4, R6.5 and R6.6, which change an annual requirement in CIP-007-4 and makes it a quarterly requirement in version 5. The additional administrative work created is not offset by a commensurate improvement in security.

No

R7 REQUIREMENT COMMENTS: MidAmerican Energy proposes deleting this requirement, in conjunction with the suggested restructuring back to the version CIP-004-4 R4 language, since revocation already is covered.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the proposed revised VRFs and revisions proposed to the requirements. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We believe most of the CIP-004-5 requirements could have gradated VSLs.

No

GENERAL COMMENTS ON CIP-005-5 The “canned” C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4.

See also comments on CIP-010-1. MidAmerican Energy does support combining the vulnerability assessment requirement from CIP-005-4 with CIP-007-4's vulnerability assessment requirement. GENERAL COMMENTS ON CIP-005-5 R1 While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. R1.1 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to low impact assets/systems, this requirement would be moved to the new low impact standard with the following suggested changes. R1.1 MEASURES COMMENTS: Change "…documented technical and procedural…" to "…documented technical or procedural…" to be consistent with the requirement. R1.2 APPLICABILITY COMMENTS: CIP-005-4 combined with CIP-006-4 R2.2 do not require ESPs for Cyber Assets that authorize and/or log access to the Physical Security Perimeter. MidAmerican Energy does not support expanding the scope to include Associated Physical Access Control Systems. Removing these from scope will also eliminate confusion over the applicability in R1.3-R1.5 R1.2 APPLICABILITY PROPOSED REVISED TEXT: Remove "Associated Physical Access Control Systems." R1.2 REQUIREMENT COMMENTS: As literally written, R1.2 would require traffic between two Cyber Assets inside the ESP to go through an Electronic Access Point. R1.2 does not distinguish that the traffic connecting into the ESP is to go through an Electronic Access Point. Version 5 introduces a concept change that focuses on discrete Electronic Access Points rather than the logical Electronic Security Perimeter in prior versions. This concept change adds confusion and is not an Order 706 directive. MidAmerican does not support the concept change. R1.2 REQUIREMENT PROPOSED REVISED TEXT Use version 4 CIP-005 concepts. Address R1 to ensure that every Critical Cyber Asset resides in an ESP and R1.4 to protect non-critical Cyber Assets in an ESP. R1.3 REQUIREMENT COMMENTS: This requirement appears to combine both R2.1 and R2.2 from legacy. This does not add clarity and is not a directive. Retain legacy concepts. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "Processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified." "At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services." R1.4 REQUIREMENT COMMENTS: Not a directive. May not be increasing security. More prescriptive. Use legacy language. R1.4 REQUIREMENT PROPOSED REVISED TEXT: "The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s)." R1.5 REQUIREMENT COMMENTS: The requirement should be to implement. "At" is not the best preposition, "through" is better. R1.5 REQUIREMENT PROPOSED REVISED TEXT: "Implement a method for detecting malicious communications through Electronic Access Points."

No

CIP-005 R2 GENERAL COMMENTS: Overall, MidAmerican Energy does not believe the proposed Intermediate Device and encryption sub requirements provide enough security benefit to offset the impact on operations. The Intermediate Device and encryption requirements also prescribe "how," not "what," is to be accomplished and do not allow room for alternate controls that could be equally or more effective. Narrow prescriptions in a rapidly changing technology environment obsolesce faster than the standards revision process can update. External routable connectivity is a different attack vector and warrants different treatment from dial up. MidAmerican Energy does not support requirements for dial up in this table. Our comment on CIP-005-5 R1 addresses securing dial up access. R2.1 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.1 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.1 REQUIREMENT COMMENTS: The draft definition of Intermediate Device refers to implementing the functions of an Intermediate Device and includes the very important concept of proxy systems. Revise the text of the requirement to "Implement the functions of an Intermediate Device."(Project 2010-15 CIP-005 also proposed the verb "implement.") This makes it clearer in the requirement that the desired results are the functions of an Intermediate Device, not a device itself. This also aligns with the definition better than "Require an Intermediate Device" since the definition recognizes the functions may be implemented on one or more devices. The Intermediate Device definition as posted excerpt follows for reference: "Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic

Access Point, or in a DMZ network." R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Implement the functions of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." R2.2 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.2 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.2 REQUIREMENT COMMENTS: R2.2 is ambiguous on where encryption is required to start and stop. The last version posted for Project 2010-15 CIP-005 R6.2 attempted to address this with the following language: "Implement interactive remote access such that communications between the Cyber Asset initiating interactive remote access and the intermediate device are encrypted … while using a network that is shared with users not associated with the Responsible Entity." Correct "Reference to prior version: CIP-007 R3.1" because that requirement is about ports, not encryption. R2.2 REQUIREMENT PROPOSED REVISED TEXT: "Implement encryption when interactive remote access uses a network that is not associated with the Responsible Entity. Encrypt communications between the Cyber Asset initiating interactive remote access and where the Intermediate Device functions are implemented." R2.3 APPLICABILITY COMMENTS: Add qualifier of External Routable Connectivity. Do not require for dialup. R2.3 APPLICABILITY PROPOSED REVISED TEXT: "High Impact BES Cyber Systems with External Routable Connectivity; Medium Impact BES Cyber Systems with External Routable Connectivity; Associated Protected Cyber Assets with External Routable Connectivity" R2.3 REQUIREMENT COMMENTS: Correct "Reference to prior version: CIP-007 R3.2" because that requirement is about ports. Multi-factor authentication correlates closer to CIP-005-4 R2.4 strong procedural or technical controls at access points to ensure authenticity for external interactive access. R2.3 REQUIREMENT PROPOSED REVISED TEXT: No changes.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with the revisions proposed for the VRFs and to the requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-005-5 requirements.

No

CIP-006-5 GENERAL COMMENTS: See also comments on Definitions where we recommend we retain the NERC glossary term Physical Security Perimeter. The change from Physical Security Perimeter to Defined Physical Boundaries creates the need to update numerous procedure documents and physical security drawings, etc. Changing the term does not improve security, but increases costs for 241 entities that have PSPs. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 APPLICABILITY COMMENTS: Add Medium Impact BES Cyber Systems with no External Routable Connectivity. R1.1 MEASURES COMMENTS: Change operational "and" procedural to operational "or" procedural to be consistent with the R1.1 requirement. R1.2 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.2 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. The proposed changes do not improve security. Delete "that restricts access to only those individuals that are authorized." Access is covered in CIP-004. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "All applicable Critical Cyber Assets shall reside within an identified Physical Security Perimeter. Each Physical Security Perimeter utilizes one or more different physical access control(s), where technically feasible." (Note: Use of the term CCA is recommended in CIP-002 comments.) R1.2 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Current standards do not include controlling egress. R1.2 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to, language in the physical security plan that describes how access is controlled." R1.3 APPLICABILITY COMMENTS: "Associated Electronic Access Control or Monitoring Systems" as well as "Associated Protected Cyber Assets" can be read to include devices used for electronic access to a

Medium Impact BES Cyber System or used within a Medium Impact BES Cyber System's Electronic Security Perimeter. This requirement only applies to High Impact BES Cyber Systems. R1.3 APPLICABILITY PROPOSED REVISED TEXT: “High Impact BES Cyber Systems; Electronic Access Control or Monitoring Systems associated with High Impact BES Cyber Systems; Protected Cyber Assets located within a High Impact BES Cyber System Electronic Security Perimeter” R1.3 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. The phrase "different and complementary" is not clear. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "All applicable Cyber Assets shall reside within an identified Physical Security Perimeter. Each Physical Security Perimeter must utilize two or more different physical access controls, where technically feasible. Physical access controls may be provided by single devices with multiple access control measures." R1.3 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Current standards do not require controlling egress. R1.3 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes how access is controlled, or * physical security perimeter drawings, or * list of physical security perimeters and access points into the PSPs” R1.4 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.4 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The proposed changes do not improve security. Change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. R1.4 MEASURES COMMENTS: Change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. Add human observation from CIP-006-3 R5 as other possible alert evidence. R1.4 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes the issuance of automated or human observation alerts in response to unauthorized physical access through any access point in a Physical Security Perimeter, or *additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that documents that these alerts were generated” R1.5 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.5 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. The proposed changes do not improve security. R 1.5 REQUIREMENT PROPOSED REVISED TEXT: "Immediately alert personnel responsible for a response to unauthorized physical access to Physical Access Control Systems." R1.5 MEASURES COMMENTS: Add human observation from CIP-006-3 R5 as other possible alert evidence. R1.6 APPLICABILITY COMMENTS: Change Medium Impact BES Cyber Systems to Medium Impact BES Cyber Systems with External Routable Connectivity. R1.6 REQUIREMENT COMMENTS: FERC Order did not direct any changes. It is redundant to restate the applicability information. Suggest going back to legacy language. R1.6 REQUIREMENT PROPOSED REVISED TEXT: "Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: computer logging, video recording or manual logging. Retain physical access logs for at least ninety days." R1.6 MEASURES COMMENTS: FERC Order did not direct any changes. R1.6 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in the physical security plan that describes logging and recording of physical entry into Physical Security Perimeters, or * additional evidence to demonstrate that this logging and recording has been implemented, such as logs of physical access into Physical Security Perimeters that show the date of entry into Physical Security Perimeters."

No

R2.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Require continuous escorted access of visitors (individuals not authorized for unescorted physical access) within any Physical Security Perimeter." R2.1 MEASURES COMMENTS: FERC Order 706 did not direct changes. The change from Physical Security Perimeter to Defined Physical Boundaries increases paperwork and related costs to update procedure documents with no security improvement.

R2.1 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters, or * additional evidence to demonstrate that the process was implemented"

No

R3.1 APPLICABILITY COMMENTS: Add language to clarify to which systems the physical access controls are referring. R3.1 APPLICABILITY PROPOSED REVISED TEXT: "Associated Physical Access Control Systems and locally mounted hardware or devices associated with Physical Security Perimeters for High Impact BES Cyber Systems; Medium Impact BES Cyber Systems; Associated Electronic Access Control and Monitoring Systems; and Associated Protected Cyber Assets" R3.1 MEASURES COMMENTS: Delete language that repeats the requirements. R3.1 MEASURES PROPOSED REVISED TEXT: "Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * dated maintenance records, or * other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months." R3.2 APPLICABILITY COMMENTS: Delete "or Monitoring" to match the defined term. R 3.2 APPLICABILITY PROPOSED REVISED TEXT: "Associated Physical Access Control Systems" R3.2 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes to this requirement. Suggest going back to legacy language. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Retain outage records for a minimum of one calendar year.”

No

The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: Lower – Part 1.7 should point to 1.6; High – Part 1.6 should point to 1.5. R1.4 VRF COMMENT: The VRF for R1 is "Medium." This is not appropriate with R1.5, which is Associated Physical Access Control Systems, or for R1.1, which is Low Impact and Associated Physical Access Control Systems. This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-006-5 requirements.

No

CIP-007-5 GENERAL COMMENTS: While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. See also comments on CIP-010-1 and CIP-011-1. MidAmerican Energy does not support moving CIP-007-4 requirements to the new CIP-010-1 separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within CIP-007-4 and preserve the numbering of the requirements within this standard. One exception is that we support combining the vulnerability assessment requirement from CIP-005-4 with CIP-007-4’s vulnerability assessment requirement. The “canned” C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 REQUIREMENT COMMENTS: FERC Order 706 didn't direct changes. Requiring documentation of the need for remaining logical network accessible ports is burdensome and does not improve security. "Services" is absent from this requirement. The table heading still shows "Ports and Services." R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Disable or restrict access to unnecessary logical network accessible ports. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed necessary." R1.1 MEASURES COMMENTS: FERC Order 706 didn't direct changes. Requirement revisions require Measures revisions. R1.1 MEASURES PROPOSED REVISED TEXT: Evidence may include, but is not limited to, documentation of how unnecessary logical network accessible ports for Critical Cyber Assets have been disabled. R1.2 REQUIREMENT PROPOSED REVISED TEXT: “Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media by disabling, restricting or labeling with a sign.” R1.2 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, documentation of how unnecessary

physical input/output ports have been disabled, restricted either logically through system configuration or physically using a port lock or labeled with a sign.”
No
R2.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct any changes. Clarify monitoring is for "security related" updates to software and firmware, which is comparable to security related patches. 2.1 REQUIREMENT PROPOSED REVISED TEXT: “Identify a source or sources that are monitored for the release of security related patches, or security related updates for all software and firmware associated with BES Cyber System or Critical Cyber Assets.” 2.1 MEASURES COMMENTS: Delete the last sentence regarding list sorting. 2.1 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, a list of sources that are monitored on an individual BES Cyber System or Critical Cyber Asset basis.” R2.2 REQUIREMENT COMMENTS: Recommend two separate requirements, one for identifying applicable security related updates within 30 days of release and one for creating a remediation plan within 60 days of release unless the security related update is installed within 60 days. If installed within 60 days, the remediation plan is not required. Also add “security-related” before “updates.” 2.2 REQUIREMENT PROPOSED REVISED TEXT: First New Requirement – “Identify applicable security-related patches or security-related updates within 30 days of release from the identified source.” Second New Requirement – “Create a remediation plan, or revise an existing remediation plan, within 60 days of release from the identified source for applicable security-related patches or security-related updates to address vulnerabilities. A remediation plan is not required for security patches or security upgrades installed within 60 days of release from the identified source.” R 2.2 MEASURES COMMENTS: Revised Requirements result in revised Measures. R2.2 MEASURES PROPOSED REVISED TEXT: First New Measure – “Evidence may include, but is not limited to, an assessment conducted by, referenced by, or on behalf of a Registered Entity of security-related patches or security-related updates released by the documented sources.” Second New Measure – “Evidence may include, but is not limited to, a dated remediation plan showing when the vulnerability will be addressed or documentation showing the security-related patches or security-related updates have been installed within 60 days.” R2.3 REQUIREMENT COMMENTS: Change rationale indicates this requirement is for implementation of the remediation plan, subject to exceptions. R2.3 REQUIREMENT PROPOSED REVISED TEXT: “Implement remediation plans, allowing for CIP Exceptional Circumstances.” R2.3 MEASURES COMMENTS: Although the "Background" section states bullets in Measures indicates any one of the bulleted items, not all of them, this needs to be clear in the Measures section to be enforceable. Replace semi-colons with "comma, or" at the end of each bullet.
No
R3.1 REQUIREMENT COMMENTS: The requirements need to be clear on the competency based approach. It is only in the summary of changes and application guidelines. It needs to be in the requirement that is enforceable. Methods do not have to be used on every single Cyber Asset. R3.1 REQUIREMENT PROPOSED REVISED TEXT: "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." R3.2 REQUIREMENT COMMENTS: Malicious code can be mitigated in various ways depending on many variables. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Mitigate identified malicious code.” R3.2 MEASURES COMMENTS: Each listed item should be separated by “or”. R3.3 REQUIREMENT COMMENTS: Include testing prior to updating. R3.3 REQUIREMENT PROPOSED REVISED TEXT: “Test and update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns).” R3.3 MEASURES COMMENTS: List of measures should be separated by “comma or.” Limit evidence retention period to 90 days because retaining it for three years becomes burdensome. R3.3 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, current signature or pattern updates, or screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls. Evidence to be retained for 90 days.” R3.4 APPLICABILITY COMMENTS: Remove the Associated Physical Access Control Systems and Associated Electronic Access and Control Monitoring items from the list. Protection is for Transient Cyber Assets and removable media when connected to Medium or High Impact BES Cyber Systems or Protected Cyber Assets according to the proposed version 5 requirements. R3.4 REQUIREMENT COMMENTS: Insert “known” prior to malicious code. It is reasonable to expect entities to protect against known malicious code, which also may protect for some unknown malicious code. However, it is not possible to protect against all unknown malicious

code. Revise the labels to use version 4 descriptions and NERC glossary terms for Critical and noncritical Cyber Assets. There is no security benefit to changing the labels. Changing the labels will be costly for the 241 entities that already have programs and documentation with these terms. R3.4 REQUIREMENT PROPOSED REVISED TEXT: “Deploy method(s) to deter, detect, or prevent known malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.” R3.4 MEASURES COMMENTS: Logs showing when Transient Cyber Assets were connected to Critical Cyber Assets or Noncritical Cyber Assets is in CIP-007-5 R3.5. Also, including it here creates double jeopardy. It should not be included here. R3.4 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent known malicious code on Transient Cyber Assets and removable media.” R3.5 APPLICABILITY COMMENTS: Delete Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems because they are not Transient Cyber Asset related. R3.5 REQUIREMENT PROPOSED REVISED TEXT: “Log each Transient Cyber Asset connection to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.” R3.5 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact Critical Cyber Assets or Associated Noncritical Cyber Assets.”

No

R4.1 REQUIREMENT COMMENTS: FERC Order 706 did not direct changes. The enumerated list is too prescriptive for the requirement. Add to guidelines. See more general requirement for R4.2. R4.1 REQUIREMENT PROPOSED REVISED TEXT: “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents. Devices that cannot log a particular event do not require a TFE to be generated.” R4.1 MEASURES PROPOSED REVISED TEXT “Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the Cyber Asset is configured to generate logs.” R4.2 REQUIREMENT COMMENTS: FERC Order 706 did not require a change; therefore the addition of “real time” is not required. Some assets can log, but cannot alert. R4.2 REQUIREMENT PROPOSED REVISED TEXT: “Generate alerts, where technically feasible, for events that the Responsible Entity determines necessary.” R4.2 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to paper or system generated listing of event classes and conditions that necessitate alerts; assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; screenshots showing how alerts are configured.” R4.3 APPLICABILITY COMMENTS: Delete “with External Routable Connectivity” from Medium Impact BES Cyber Systems. R4.3 REQUIREMENT COMMENTS: FERC Order did not direct a change. Add clarification to timing, “after identification.” R4.3 REQUIREMENT PROPOSED REVISED TEXT: “Activate a response to event logging or alerting failures before the end of the next calendar day after identification.” R4.3 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: dated event logging failures and screen-shots showing how alerts were configured, or dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures.” R4.4 APPLICABILITY COMMENTS: Delete "at Control Centers" from Medium Impact BES Cyber Systems. If this is not deleted, this requirement would not apply to substations, which would decrease security. R4.4 MEASURES COMMENTS: FERC Order 706 did not direct retaining records of disposition of security-related event logs. Retaining records of disposition of security-related event logs beyond 90 days up to the evidence retention period would be burdensome. R4.5 REQUIREMENT COMMENTS: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. Delete last portion of requirement to activate a response because it is already included in R4.3. Including it in this requirement too would result in double jeopardy. The term “unanticipated” is not needed. R4.5 REQUIREMENT PROPOSED REVISED TEXT: “Review a summarization or sampling of logged events every two weeks to identify Cyber Security Incidents and potential event logging failures.” R4.5 MEASURES COMMENTS: Delete last portion of measure to show personnel were dispatched or a work ticket was opened because it is already included in R4.3. R4.5 MEASURES PROPOSED REVISED TEXT: “Evidence may include, but is not limited to, documentation describing the review, findings from the review (if any), signed and dated documentation showing the review occurred.”

No

R5.1 REQUIREMENT COMMENTS: Need to allow for where technically supported and this is more

specifically addressing electronic user access. R5.1 REQUIREMENT PROPOSED REVISED TEXT: "Validate credentials before granting electronic user access to each BES Cyber System where technically supported." R5.2 REQUIREMENT COMMENTS: Delete because this replicates the CIP-004 access authorization requirements. 5.3 REQUIREMENT COMMENTS: Delete as this would already be included in the CIP-004 access authorization requirements. R5.4 APPLICABILITY COMMENTS: Move list of applicability from Requirements to Applicability. R5.4 APPLICABILITY PROPOSED REVISED TEXT: "High Impact Critical Cyber Assets, Medium Impact Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets." R5.4 REQUIREMENT COMMENTS: It is not necessary to list the applicability in the Requirements section. Provide additional options for controlling default accounts. R5.4 REQUIREMENT PROPOSED REVISED TEXT: "Control default accounts by initially changing default passwords, or removing or disabling the accounts, where technically feasible, unless the default password is unique to the device or instance of the application. For the purposes of this requirement an inventory of Cyber Assets is not required." R5.5 REQUIREMENT COMMENTS: 5.5.1. FERC did not direct a change in password length. Although eight characters increases security over six characters, 10 characters would increase security more than eight characters and so on. Where does one stop? Retain requirement for six character passwords. Passwords would be applied at the asset level instead of system level. R5.5 REQUIREMENT PROPOSED REVISED TEXT: "For password-based user authentication, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is the lesser of at least six characters or the maximum length supported by the Critical Cyber Asset; 5.5.2. Minimum password complexity of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non- alphanumeric) or the maximum complexity supported by the Critical Cyber Asset; 5.5.3. Password change or an obligation to change the password on an entity-specified time frame based on the impact level of the Critical Cyber Asset, the significance of passwords in the set of controls used to prevent unauthorized access to the Critical Cyber Asset and existing service agreements, warranties or licenses." R5.6 REQUIREMENT COMMENTS: This is a new requirement that is not directed by FERC Order 706 and would generate a lot of TFEs without commensurate improvements to security. It overlaps with the alerting requirement and should be deleted.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for many of the CIP-007-5 requirements.

No

GENERAL COMMENTS ON CIP-008-5: Most of the changes made to CIP-008 were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for entities with existing programs. We recommend returning to legacy language and structure for CIP-008-5. Suggested text is included below. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The proposed applicability of "All Responsible Entities" greatly expands the scope CIP-008, which was not directed by FERC. MidAmerican Energy recommends changing the Applicability for all of the CIP-008-5 requirements to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Develop, maintain and implement a Cyber Security Incident Response Plan that includes the following: 1.1.1 Procedures to characterize and classify events as Reportable Cyber Security Incidents. 1.1.2 Response actions 1.1.3 Roles and responsibilities of Cyber Security Incident response teams 1.1.4 Cyber Security Incident handling procedures 1.1.5 Communication plans" R1.1 REFERENCE: CIP-008-4 R1, R1.1, R1.2, R1.3 R1.1 RATIONALE: There were no FERC directives for revisions. Wording in version 4 is clear and does not need to be changed. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "Follow requirements in EOP-004 to report Reportable Cyber Security

Incidents." R1.2 REFERENCE: CIP-008-4 R1.3 R1.2 RATIONALE: FERC Order 706, paragraphs 673-677, addresses reporting of Cyber Security Incidents, including coordination between CIP-008 and other standards. Most of these FERC directives are being handled by the EOP-004/CIP-001 project. While the reporting requirement is being moved to EOP-004, a reference in this standard is needed. R1.3 REQUIREMENT PROPOSED REVISED TEXT: "Review the Cyber Security Incident response plan at least annually." R1.3 REFERENCE: CIP-008-4 R1.5 R1.3 RATIONALE: There were no FERC directives for revisions. Wording in version 4 is clear and does not need to be changed. R1.4 REQUIREMENT PROPOSED REVISED TEXT: "Update the Cyber Security Incident response plan within thirty calendar days of any organizational or technology changes that impact the plan." R1.4 REFERENCE: CIP-008-4 R1.4 R1.4 RATIONALE: There were no FERC directives for revisions. Additional words were inserted from version 4 language to clarify what changes are included in the requirement.
No
GENERAL COMMENTS ON CIP-008-5 R2: As mentioned in CIP-008-5 R1 comments, most of the changes made to CIP-008 were not directed by FERC Order 706 and do not result in improvements to security. MidAmerican Energy recommends returning to legacy language and structure for CIP-008-5. Suggested text is included below. The proposed applicability of "All Responsible Entities" greatly expands the scope CIP-008, which was not directed by FERC. MidAmerican Energy recommends changing the Applicability for all of the CIP-008-5 requirements to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Test the Cyber Security Incident response plan at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. The test should include verification of the list of entities that must be called pursuant to the plan and that the contact numbers are correct." R2.1 REFERENCE: CIP-008-4 R1.6 R2.1 RATIONALE: FERC Order 706, paragraph 687 states CIP-008 should include verification of the list of entities and contact numbers. R2.2 REQUIREMENT PROPOSED REVISED TEXT: "Review the results of the Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." R2.2 REFERENCE: New requirement R2.2 RATIONALE: FERC Order 706, paragraph 686 directs changes to the requirement to include revisions to the plan to address lessons learned. R2.3 REQUIREMENT PROPOSED REVISED TEXT: "Update the Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan." R2.3 REFERENCE: New requirement R2.3 RATIONALE: FERC Order 706, paragraph 686 directs changes to the requirement to include revisions to the plan to address lessons learned.
No
R3 REQUIREMENT COMMENTS: Most of the changes made to CIP-008 were not directed by FERC Order 706 and do not result in improvements to security. MidAmerican Energy proposes returning to the version 4 language and structure for CIP-008-5, which incorporates the R3 requirements into R1 and R2. Therefore, R3 would be deleted under our proposal.
No
The proposed VRFs and VSLs should be revised commensurate with revisions proposed to the requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" MidAmerican Energy believes it is possible to have gradated VSLs for CIP-008-5. As an example, the VSLs for R1 could include the following. Lower: The Cyber Security Incident response plan was updated more than 30 calendar days but less than 60 calendar days of organizational or technology changes that impacted the plan. Moderate: The Cyber Security Incident response plan was updated more than 60 calendar days but less than 90 calendar days of organizational or technology changes that impacted the plan. High: The Cyber Security Incident response plan was updated more than 90 calendar days but less than 120 calendar days of organizational or technology changes that impacted the plan. Severe: The Cyber Security Incident response plan was updated more 120 calendar days of organizational or technology changes that impacted the plan.
No
PURPOSE STATEMENT COMMENTS: MidAmerican suggests revising the purpose statement to the following: "Standard CIP-009-5 ensures recovery plan(s) are put in place for Critical Cyber Assets." GENERAL COMMENTS ON CIP-009-5: The revised version 5 structure splits backup media

requirements between R1 (recovery plan) and R2 (implementation and testing). We think the FERC directives for CIP-009 can be more effectively addressed within a structure that is closer to version 4. MidAmerican Energy proposes the following requirements: R1 recovery plan (which includes implement); R2 exercise of the recovery plan; R3 backup media; and R4 maintain the recovery plan. Our suggested text and structure are included below. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The current draft does not include any guidance. We think it is important to include guidance regarding possible ramifications to other NERC standards. For example, event analysis requirements and IRO-001 R3 must be considered if there is a potential delay of restoration to collect forensic data. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. Column headers above R1.4 and R3.4 are incorrect. The document currently shows "Part" for each column instead of only the first one. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Create and implement a recovery plan that addresses at a minimum: R1.1.1. Conditions for activation of the recovery plan, and R1.1.2 Roles and responsibilities of responders" R1.1 RATIONALE: There were no FERC directives for this requirement, except for adding implementation. We suggest V4 legacy language, and incorporate implementation as directed. R1.2 REQUIREMENT COMMENT: Delete since this has been incorporated into R1.1. R1.3 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R3 backup media, under the revised structure mentioned above. R1.4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R3 backup media, under the revised structure mentioned above. R1.5 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be moved to R2 exercise of the recovery plan, under the revised structure mentioned above. See comments under R2.

No

R2 REQUIREMENT COMMENTS: This requirement is about exercises and actual incidents. The use of the term "implement" in this requirement is confusing. We suggest implementation be incorporated into R1 to meet the FERC directive, and change this requirement to be more in line with version 4. R2 REQUIREMENT PROPOSED REVISED TEXT: "Each Responsible Entity shall exercise its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Exercise [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]" R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Exercise the recovery plan(s) annually. An exercise can range from a paper drill, to a full operational exercise, to recovery from an actual incident." R2.1 RATIONALE: Maintain the version 3 language. R2.2 REQUIREMENT COMMENT: We suggest moving the requirement for testing backup media to R3. R2.3 REQUIREMENT COMMENT This requirement would become R2.2 under our proposed structure. R2.3 REQUIREMENT PROPOSED REVISED TEXT: "Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual response may substitute for an operational exercise." R2.3 (which becomes R2.2) RATIONALE: We removed text on "initially upon the effective date." This should be incorporated in the implementation plan. R2.3 (which becomes R2.2) APPLICABILITY: This requirement should apply to High Impact BES Cyber Systems only. Associated assets should not be included. PROPOSED R2.3 REQUIREMENT COMMENT: MidAmerican Energy proposes R1.5 be moved to R2.3, since it is associated with events that trigger the recovery plan. PROPOSED R2.3 PROPOSED REVISED TEXT: Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. PROPOSED R2.3 RATIONALE: We removed "technically feasible" because the TFE concept does not work with this requirement due to the 60 day safe harbor in the rules of procedure. We revised the requirement to eliminate any conflicts with other reliability standards and event analysis requirements. The focus should be getting the system back up and operational. See paragraph 708 of FERC Order 706, which states: "should not impede or restrict system restoration." We also incorporated the concept "necessary to determine the cause," which is based on FERC's directive, paragraph 710. In some situations, data preservation may not be needed to determine the cause of an event that triggers the recovery plan. PROPOSED R2.3 APPLICABILITY: This is a burdensome new requirement. Therefore, MidAmerican Energy proposes the applicability be limited to High Impact BES Cyber Systems. PROPOSED R2.3 MEASURES: Measures should be bulleted with "ors" and commas.

No

R3 AND R4 GENERAL COMMENTS: Under our proposed structure, all of the requirements in the draft R3 would be moved to a new requirement, R4. Please see R4 below for comments regarding the draft R3.1 to R3.5. R3 REQUIREMENT COMMENT: MidAmerican Energy proposes R3 be a separate requirement for backup storage. Version 3 had two requirements related to backup storage. These had been incorporated into other requirements in the draft V5. R3 REQUIREMENT PROPOSED TEXT: “Each Responsible Entity shall have one or more documented processes that collectively include each of the applicable items in CIP-009-5 R3 - Recovery Plan Backup Media.” R3.1 REQUIREMENT COMMENT: We have moved R1.3 to be R3.1. R3.1 REQUIREMENT PROPOSED REVISED TEXT: “Back up and store information required to successfully restore BES Cyber System functionality. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.” R3.1 RATIONALE: The revised text is based on V3 language. This removes the word "protection" since this is not a FERC directive. The sentence "For example…" from V3 could be moved to measures. R3.2 REQUIREMENT COMMENT: We have moved R2.2 to be R3.2. R3.2 REQUIREMENT PROPOSED REVISED TEXT: “Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.” R3.2 RATIONALE: We propose the version 4 language, since there were no FERC directives to change it. R3.3 REQUIREMENT COMMENT: We have moved R1.4 to be R3.3. R3.3 REQUIREMENT PROPOSED REVISED TEXT: “Verify after significant changes that the backup process for software, data and information required to successfully restore CCAs completed successfully.” R3.3 RATIONALE: Refer to FERC Order 706, paragraph 740, which refers to "significant changes." R3.3 APPLICABILITY COMMENTS: Limit to High Impact BES Cyber Systems due to the burdensome nature of this new requirement. R4 REQUIREMENT COMMENT: Under our proposed structure, R4 would be Recovery Plan Review, Update and Communication. We propose deleting the draft R3.2, since there were no FERC directives to add this as a requirement. We propose deleting the draft R3.4. This is covered in the suggested text from version 4 for R4.2. R4.1 REQUIREMENT COMMENT: We have moved R3.1 to be R4.1. R4.1 REQUIREMENT PROPOSED REVISED TEXT: “Review the recovery plan annually.” R4.1 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language. R4.2 REQUIREMENT COMMENT: We have moved R3.3 to be R4.2 R4.2 REQUIREMENT PROPOSED REVISED TEXT: “Update the recovery plan(s) to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.” R4.2 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language. R4.3 REQUIREMENT COMMENT: We have moved R3.5 to be R4.3. R4.3 REQUIREMENT PROPOSED REVISED TEXT: “Communicate updates to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.” R4.3 RATIONALE: There were no FERC directives to change the requirement. Revert to version 4 language.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We think some of the CIP-009-5 requirements could have gradated VSLs for CIP-009-5. As an example, the VSLs for R2 as proposed by MidAmerican Energy could include the following. Lower: The recovery plan was exercised more than 39 calendar months but less than 40 calendar months since the previous exercise. Moderate: The recovery plan was exercised more than 40 calendar months but less than 41 calendar months since the previous exercise. High: The recovery plan was exercised more than 41 calendar months but less than 42 calendar months since the previous exercise. Severe: The recovery plan was exercised more than 42 calendar months since the previous exercise.

No

GENERAL COMMENTS ON CIP-0010-5: CIP-010-5 R1 and R2 greatly expand the scope of change control and configuration management beyond what was directed in FERC Order 706. MidAmerican does not support this scope expansion. MidAmerican Energy does not support organizing these requirements into a separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements

could remain within their version 4 standard and preserve the numbering of the requirements within those standards. One exception is that we support removing the vulnerability assessment requirement from CIP-005-4 and combining it with CIP-007-4's vulnerability assessment requirement. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1 RATIONALE COMMENTS: The rationale does not address paragraph 399 of FERC Order 706 – having processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. R1.1 REQUIREMENT COMMENT: The draft requirement is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Establish and document a process of change control and configuration management for adding, modifying, replacing or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process." If industry consensus can be achieved, MidAmerican will support requiring authorization of changes, but without the additional bureaucracy as drafted of authorization by the senior manager or delegate. Entities should be able to use their existing corporate change control authorization processes without having to create a CIP-only variation on their standard processes. R1.1 MEASURES COMMENTS: Change the measure to match the revised requirement, such as documentation of the change control process. R1.2 REQUIREMENT COMMENT: FERC Order 706 did not direct authorization by the senior manager or delegate. It directed "express acknowledgement of the need for the change control," which we believe is achieved with the proposed text below. R1.2 REQUIREMENT PROPOSED REVISED TEXT: "Authorize changes to hardware and software components of Critical Cyber Assets." R1.3 REQUIREMENT COMMENT: This requirement should be deleted with our proposal to remove the burdensome requirement for baseline configurations in R1.1. R1.4 REQUIREMENT COMMENT: MidAmerican Energy proposes this requirement be replaced with CIP-007-4 R1. R1.4 REQUIREMENT PROPOSED REVISED TEXT: Ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of this standard, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware. R1.4.1 Implement and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation. R1.4.2 Document that testing is performed in a manner that reflects the production environment. R1.4.3 Document test results. R1.5 REQUIREMENT COMMENT: With our proposal to create a standard for controls that are only applicable to high impact assets/systems, this requirement would be moved to the new high impact standard with the following suggested changes. Delete "results of the testing" from R1.5.2 because it overlaps with R1.4 for highs. Delete and put in guidance: "including a description of the measures used to account for any differences in operation between the test and production environments." R1.5.2 REQUIREMENT PROPOSED REVISED TEXT: "Document the differences between the test environment and the production environment."

No

R2.1 REQUIREMENT COMMENT: MidAmerican Energy is concerned that this requirement creates the possibility of "double jeopardy" for violations with multiple other requirements. As currently written, if an auditor finds a violation for CIP-010-5 R1, the same situation likely would result in a violation of CIP-010-5 R2. The current draft also overlaps with the alerting that is required in CIP-007-5 R4.2 and the investigation that is required by CIP-008. We have provided proposed revised text that addresses the possibility of double jeopardy. We also deleted the words "and document" since documentation is

not providing any improvements to reliability, but increases implementation costs for entities. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. R2.1 REQUIREMENT PROPOSED REVISED TEXT: "Where technically feasible, detect unauthorized changes to the configuration that have not been alerted under other CIP standards."

No

CIP-010-5 R3 GENERAL COMMENTS: MidAmerican Energy proposes the draft R3 be replaced with combined legacy language from CIP-005-4 R4 and CIP-007 -4 R8, with the following FERC directed additions: • The addition of an entity imposed timeline for completing the already required action plan. • Active vulnerability assessments every three years. MidAmerican generally supports the inclusion of details in guidelines. However, in this case, the current draft of CIP-010-5 R3 has removed too many details from the standard, thus making it a vague standard that introduces the possibility of significant scope expansion that was not directed by FERC. MidAmerican agrees the FERC directed requirement for active vulnerability assessments should be limited to High Impact Critical Cyber Assets. With our proposal to create a standard for controls that are only applicable to high impact assets/systems, R3.2 would be moved to the new high impact standard. MidAmerican would suggest deleting R3.3 since this is covered by the implementation plan.

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that "as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…" We think some of the CIP-0010-5 requirements could have gradated VSLs.

No

CIP-011 GENERAL COMMENTS: MidAmerican Energy does not support organizing these requirements into a separate standard. This was not directed by FERC, does not improve security and increases implementation costs for entities with fully implemented CIP programs. These requirements could remain within their version 4 standard and preserve the numbering of the requirements within those standards. While we have not provided comments on applicability and measures for every requirement due to the large scale of this project, these would also need revisions to be more in line with our proposed changes to the requirements. The "canned" C.1.2 Evidence Retention section in this standard should be reviewed and revised, as necessary to correspond to the current obligation in version 4. R1 GENERAL COMMENTS: The only FERC directive for information protection was prompt revocation of access to protected information (paragraph 386), which is addressed in CIP-004. There was no FERC directive to move the information protection requirement to a separate standard or to make other changes that increase implementation costs for entities with implemented programs, without any improvements to security. MidAmerican proposes going back to version 4 language and structure for information protection, with two parts instead of three. Proposed text is listed below. R1 REQUIREMENT PROPOSED REVISED TEXT: "Each Responsible Entity shall have one or more documented processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]" R1.1 APPLICABILITY COMMENTS: Remove Associated Protected Cyber Assets. This was not directed by FERC and is an expansion of scope that does not improve security. R1.1 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to text that is more in line with version 4 language. The SDT is proposing to remove the explicit requirement for classification. The SDT states this does not prevent having multiple levels of classification. However, the legacy language does not require multiple levels of classification. R1.1 REQUIREMENT PROPOSED REVISED TEXT: "Implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets. R1.1.1 The information to be protected shall include the following: Critical Cyber Information operational procedures; lists as required in Standard CIP-002-5; Critical Cyber Information network topology or similar diagrams; floor plans of computing centers that contain Critical Cyber Assets; equipment layouts of Critical Cyber Assets; disaster recovery and incident response plans for Critical Cyber Assets; and Critical Cyber Asset security configuration information. R1.1.2 Information shall be classified based on the sensitivity of the Critical Cyber Asset information." R1.1 MEASURES

PROPOSED REVISED TEXT: “Evidence may include, but is not limited to: (following should be bullets, separated by commas and “ors”) * evidence that physical media is stored in secured locations to prevent unauthorized access, or * evidence that technical measures are in place to prevent unauthorized access to electronic information, or *records of training on information handling procedures” R1.2 APPLICABILITY COMMENTS: Remove Associated Protected Cyber Assets. This was not directed by FERC and is an expansion of scope that does not improve security. R1.2 REQUIREMENT COMMENT: MidAmerican Energy proposes going back to text that is more in line with version 4 language for assessment of the program. R1.2 REQUIREMENT PROPOSED REVISED TEXT: “At least annually assess adherence to the Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.”

No

R2.1 REQUIREMENT COMMENTS: We suggest some minor wording changes to begin the requirement with a verb and clarify that information is being retrieved from the asset. R2.1 REQUIREMENT PROPOSED REVISED TEXT: “Prevent the unauthorized retrieval of Critical Cyber System Information from Critical Cyber Asset media prior to the release of Critical Cyber Asset media for reuse.” R2.2 REQUIREMENT COMMENTS: We suggest some minor wording changes to begin the requirement with a verb and clarify that information is being retrieved from the asset. We suggest incorporating footnote #2 into the requirement or a definition, since a footnote can easily get overlooked. R2.2 REQUIREMENT PROPOSED REVISED TEXT: “Destroy the Critical Cyber Asset media prior to disposal or prevent the unauthorized retrieval of Critical Cyber System Information from Critical Cyber Asset media prior to disposal.”

No

This standard has a medium VRF that applies to requirements for both high and medium impact asset categories. We recommend a lower VRF for the medium impact assets to recognize the difference between asset impact categories. The proposed VSLs should be revised commensurate with revisions proposed to the VRFs and requirements. As recommended in the NERC document VSL_Guidelines_20090817, references should include the Part number. FERC Order RR08-4-000, paragraph 27, states that “as a general rule, gradated VSLs, wherever possible, would be preferable to binary VSLs…” We think some of the CIP-0011-5 requirements could have gradated VSLs.

No

MidAmerican Energy does not believe it is possible to complete the implementation plan in 18 months given the scope and depth of changes contained in the current draft version 5. MidAmerican Energy, like many other entities, has found it complicated and confusing to apply the changes proposed in CIP-002-5. It is not possible to commit to an implementation plan when not sure of the entire scope of proposed changes. The number of changes required for CIP-003 through CIP-011 also makes it difficult to achieve the proposed implementation timeline. About 80 percent of the changes are not directed by FERC Order 706. Several of these changes are administratively burdensome with limited, if any, security improvement. The proposed changes for existing definition terms, such as Physical Security Perimeter and Critical Cyber Assets, also extends the time it takes to implement the number of changes needed in procedure documents, training materials, facility diagrams, etc. MidAmerican Energy suggests an alternative approach to create the opportunity to achieve a quicker implementation, particularly for high and medium impact Critical Cyber Assets. The approach builds on the work completed by the drafting team and on the CIP-002-4 standard already approved by the industry. MidAmerican Energy recommends retaining CIP-002-4 as approved by the industry in 2010. This version is filed with FERC. Industry and NERC comments on the FERC NOPR recommend FERC approval. This will eliminate the confusing and complicated process to identify BES Cyber Systems proposed in version 5. Retaining CIP-002-4 will meet FERC Order 706 directives regarding CIP-002. FERC 706 directives for CIP-002 are met by using industry approved guidance documents for identifying Critical Assets and Critical Cyber Assets, see paragraphs 253-258 and 270-273. CIP-002-4 aligns with FERC’s affirmation that the applicable responsible entities are responsible for identifying Critical Assets, see paragraphs 319-321. Also, CIP-002-2 added senior manager approval of risk-based methodology, see paragraphs 294-297. Excerpts from paragraphs 284 and 285 indicate FERC is not looking for changes to CIP-002. Paragraph 284 states, “…there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time.” Paragraph 285 says, “CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find

sufficient justification to remove this provision at this time." Building on the categorization concept, we recommend development of two new standards, one for those requirements applicable only to high impact assets and one for those requirements applicable only to low impact assets. The new standards would use CIP-002-4 to categorize Critical Assets and Critical Cyber Assets into the high and low impact levels. The new "high only" standard would group the eight extra protections for only high impact assets (not medium or low) identified in the current draft of version 5. This separate standard on requirements applicable only to high impact assets provides an opportunity for a separate implementation timeline for the additional controls that apply only to high impact assets. This new standard provides flexibility in adjusting controls on high impact assets. In the future, only one standard has to be modified for these extra requirements on high impact assets. Also, entities that do not have high impact assets will not have to sort through this new standard and reliability standard audit worksheet to assure compliance and security. CIP version 5 introduces several new controls for low impact assets not directed by FERC Order 706 or included in the standard authorization request. The resulting scope expansion is not supported by many in the industry and will likely slow down the process to approve the new CIP 5 standards. A new "low only" standard would group those requirements applicable only to low impact assets (not high or medium.) This new separate standard can be commented and voted on in parallel with the efforts listed above without impacting the schedule to meet FERC Order 706. The new standard provides full transparency in the stakeholder process. It allows separate discussion on the cost and compliance concerns with low impact assets. Also the standard allows for a separate implementation schedule for low impact assets so changes for high and medium impact assets can be completed first. The vast majority of the drafted requirements in CIP-003 through CIP-011 remain in place. However, they should be adjusted to meet the changes described in the requirements comments to: 1 - include any changes necessary to address all of the applicable FERC directives and 2 - include security improvements not directed by FERC that are known to have significant industry support. Retain version 4 language for requirements that do not meet one of these two criteria (not a directive or not an industry established security improvement). Additional implementation notes: When the time comes, MidAmerican would propose an implementation date different than Jan. 1 due to resource issues at year-end. There are 36 references to "initially upon the effective date of the standard and at least once each calendar year" (or similar language) throughout the draft standards. All of these references should be eliminated from within the standard and incorporated into the implementation plan. This ensures the effective dates of the requirements are clearly spelled out for the initial implementation of the standard, as well as for newly identified assets. The industry (not this drafting team) should consider a standard authorization request to create a NERC Glossary term for the definition of annual and retire CAN-010. There could be another opportunity to positively impact the timeframe. Any improvements to TFEs prior to implementing version 4 and version 5 would lessen the impact of these transitions. NERC's first annual TFE report to FERC was filed in September 2011. It identified 3,998 approved TFEs of which 2,814 or 71 percent were approved on the basis of "not technically possible." Industry (not an expectation for this drafting team) working with NERC and FERC should determine if a NERC Rules of Procedures revision for TFEs can be supported. Could a rules of procedure change be achieved in time to alleviate some implementation burden for both registered entities and regional entities for version 4? For example, could some administrative overhead be reduced for the 71 percent that are not technically possible?
Individual
Dan Roethemeyer
Dynegy
No
Yes
On an 11/15/2100 NERC webinar regarding V5, a presenter indicated Large Control Centers were those owned by an RC, BA, or TOP but not by a GO or GOP. Slides 18 and 29 seem to support this. However, Attachment 1, Section 1.4 seemingly contradicts the webinar information by indicating a GOP's Control Center can be a High Rating. Suggest deleting Section 1.4 and let GOP Control Centers get picked up in Section 2.13. Also, please clarify in Attachment 1, Section 1.4 (if not deleted) and 2.13 that a generating station's Control Room is not considered a Control Center in accordance with Version 5.

No
Recommend consistency with R2 and do it annually not-to-exceed 15 months.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
Recommend selecting either V4 or V5 as the next step. This issue is complicated enough without having to implement two different versions over time as well as show compliance and get audited (or do the auditing).
Individual
J. S, Stonecipher, PE
City of Jacksonville Beach dba/Beaches Energy Services
No
BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. BES Reliability Operating Services – under Dynamic Response to BES Conditions, suggest adding Excitation Response. Under Balancing Load and Generation – suggest removing unit commitment since it will not meet the 15 minute window and it is an operations planning function and not a real-time operating service. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01 Control Center – (1) We assume that a Control Center is only a Control Center as used by a BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. I suggest: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. Defined Physical Border is ambiguous. Specifically, are all spacial dimensions, horizontal and vertical, to be established as part of the boundary? In other words, it seems like the “roof” may no longer be required, e.g., 5 walls instead of 6 walls, but, vertical dimension requirements of walls / fences are ambiguous.
No
I believe that a fourth category of risk impact be developed, a “De Minimus Impact” category that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. I understand that there is concern about Low Impact BES Cyber Assets due to the risk of a coordinated attack. A coordinated attack is much more likely to BES Cyber Assets that have routable protocol or dial-up access than to those BES Cyber Assets with no connectivity. It is much more difficult and impractical to attempt a coordinated attack on BES Cyber Assets without connectivity. Recognizing this difference in both difficulty level and Low Impact (in other words, it wouldn’t be worth the effort because other attack vectors with similar levels of difficulty would have more impact), we propose adding a fourth impact category, De Minimus Impact. I would propose that these De Minimus Risk BES Cyber Assets would not need to comply with the CIP standards because the costs would be unjustified. Bullet 1.2, a Control Center for any BA, even very small ones, being High risk is inappropriate. For instance, the entire load or supply of a small BA would fit into the “noise” of a large BA for supply and demand mismatch. Suggest changing 1.2 to parallel 1.3, e.g., a BA Control Center that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4 and 2.12. Bullet 2.13 could then be used to accommodate smaller BAs Bullet 1.3, Transmission

Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Bullet 2.5, “Facilities” should be changed to “Elements”. The cranking path is not necessarily part of the BES. Bullet 2.6, is an autotransformer of 500 kV to 230 kV included? Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. I suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3,000.” Bullets 2.8 and 2.9, the phrase “at a single station or substation location” does not seem to add any value and can be a source of ambiguity. I suggest striking the phrase. Bullet 2.12, the 300 MW bright-line seems arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with 2.1 of 1500 MW. The reasoning applied in the Application Guideline is flawed. UVLS and UFLS are only last ditch efforts if other events have already caused the system to be on the edge. So, how is that different from 2.1 if the system is already on the edge? The focus should be on how a malicious user can cause an Adverse Reliability Impact; hence, I suggest 1500 MW instead of 300 MW. Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet.
Yes
I agree with the requirement but question whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
The Evidence Retention section of the standard should not refer to Rules of Procedure language that is subject to change. The sentence that states: “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit” should instead reference the Rules of Procedure, Attachment 4C on the CMEP, Paragraph 3.1.4.2, e.g., “also refer to the Rules of Procedure, Attachment 4C … Paragraph 3.1.4.2”. In this way, it is possible to accommodate changes to the ROP language without needing the change to the standard.

Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. I suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
The grammar of the sentence is a bit off and it is not clear whether the CIP Senior Manager needs to approve each of the policies or not. Suggest moving the phrase “each of its cyber security policies” to after the word “Manager”, e.g., “Each Responsible Entity shall review and obtain the approval from its CIP Senior Manager for each of its cyber security policies …”
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
There is an extra “2” at the end of the sentence within the standard.
Yes
See the discussion of Evidence Retention in response to Question 3 VSL to R5, should there be a time frame applied, e.g., failed to document … two delegations within the audit period, within a year? If three failures are spread over 30 years, e.g., one failure each 10 years, is that a severe violation?
Yes
“Implement” is ambiguous. If a process in “in force” but in one instance is not followed, is that a violation? The process has been implemented. Merriam-Webster’s has two definitions of “implement”, one of which is probably intended: 1: carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures 2: to provide instruments or means of expression for A process can meet both of these definitions. If enforced, a process can meet the first definition; if not enforced, the process can meet the second definition. I assume the SDT intends the first definition. I suggest adding a footnote to specifically identify which definition of “implement” is intended.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? I suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable but are instead examples of evidence.

No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. I suggest the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. I propose we create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. I suggest end of the next calendar week.
No
See the discussion of Evidence Retention in response to Question 3 The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs,, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. I suggest rewording bullet

1.2 to require identification of EAPs and not “secure and control”.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See the discussion of Evidence Retention in response to Question 3 The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? I encourage the SDT to develop non-binary VSLs.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirements, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes access points, FMPA encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences, non-electronic door locks that control access to substation control houses that contain Low Impact digital relays, etc. Such an interpretation would

then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. I suggest adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
See the discussion of Evidence Retention in response to Question 3 R1 has both a Long Term Planning and a Same Day Operations time frame listed because the separate bullets are different time frames. If a non-compliance occurs, wouldn’t Same Day Operations always trump Long Term Planning? If that is not the desired outcome, consider separating the bullets into separate requirements or apply the time frame on a bullet by bullet basis.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”. On bullet 2.3, “A process for” is redundant with the parent Requirement and should be deleted and just start the sentence with “Remediate as identified in the plans of 2.2 …”
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 4.2 allows the entity to establish its own threshold criteria for what unauthorized electronic access or malware activity results in a real-time alert, is that a desired state? Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low. Bullet 5.5.3 allows the entity to specify the amount of time between password changes, is this appropriate or should a bright-line be developed? For instance, High – 3 months, Medium – 6 months, Low – 12 months Bullet 5.6 allows the entity to specify the number of unsuccessful login attempts before an alert is issued, is this appropriate or should a bright-line be developed?
No
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures

described in Question 15. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to "identify, classify and respond to BES Cyber Security Incidents" on Low Impact systems? This "hidden" requirement is inappropriate. I recommend making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know "when a BES Cyber Se4curity Incident occurs". This "hidden" requirement is inappropriate. I recommend making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, "implement" is not the correct term and is duplicative with the parent requirement. How would one "implement" the entire response for a table top drill since no IT systems would be involved? "Exercise" or equivalent term is more appropriate, e.g., "R2 … implement a process for … 2.2 an Exercise …" Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
First, the question does not match the posted Requirement. The Requirement actually states: "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication". See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. See comments to Questions 34 and 35. I believe that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this "hidden" requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. Bullet 1.4, what does the word "verified" mean, than the data is "retrievable", or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
No
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in response to Question 13. Bullet 2.1, "implement" is not the correct term and is duplicative with the parent requirement. How would one "implement" the entire recovery for a table top drill since no IT systems would be involved? "Exercise" or equivalent term is more appropriate, e.g., "R2 … implement a process for … 2.1 an Exercise …" Bullet 2.2 "current configuration" is not accurate. The back-up will not reflect the "current configuration" but the configuration at the time of the back-up.
Yes
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15.
Yes
See the discussion of Evidence Retention in response to Question 3.
Yes
See comment on ambiguous reference to tables and improper use of the word "must" in Measures described in Question 15. See discussion of the ambiguity of the word "implement" discussed in

response to Question 13. The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3). Bullet 1.3, the phrase “as necessary” does not seem to add anything and creates ambiguity. Suggest deleting the phrase.
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. I suggest that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
Yes
See the discussion of Evidence Retention in response to Question 3.
No
(No comment at this time.)
Group
Pacific Northwest Small Public Power Utility Comment Group
Steve Alexanderson P.E.
Yes
We continue to see problems with the definitions. We note that the definition of Control Center now applies to “facilities” with a lower case f and with five widely differing definitions in the online dictionary we consulted. Consider a System Operator’s smart phone. It is programmable, so it is a Cyber Asset per the definition. If set up to receive automatically generated emails or texts regarding BES status or alarms from two BES locations, it “facilitates” the System Operator in doing his job, meeting one of the five definitions of “facility”. If misused, the operator might act on the false information within the fifteen minute window causing a negative impact to the BES (using the list of BES Reliability Operating Services). Therefore it is a both a BES Cyber Asset and a Control Center per the proposed definitions. This phone will carry either a Medium or High Impact rating from CIP-002 making it subject to most of the CIP standard requirements. We continue to believe the SDT did not mean to capture tools such as a smart phone in the definitions, since they do not very easily fit into

the CIP requirements. But they do get caught as we have demonstrated, so the unintended consequence is these tools will be abandoned resulting in possible negative effects to the reliability of the BES. As a start, we suggest that “Control Center” should be limited to rooms or buildings dedicated to controlling BES assets. We also note that the definition of Control Center depends on the NERC term System Operator, the definition of which uses the phrase “control center”; creating a circular definition. The definition of Cyber Asset hinges on whether or not the electronic device in question is “programmable.” Again consulting our online dictionary we see that programmable means capable of receiving working instructions for automatic operation. Therefore a simple static electronic UF relay set only by way of dials and switches and with no communication of any kind will be considered a Cyber Asset and also a BES Cyber Asset because of the function it performs. A Q&A during the webinar confirmed this assessment. Even if low impact, numerous CIP requirements now apply to the device and the entity that owns it. The entity owning this device will need to: 1. document and implement cyber security policies including the 10 sub-requirement subjects, 2. annually review the cyber security policies, 3. ensure employee awareness of the cyber security policies, 4. implement a Security Awareness Program conveying security awareness concepts with quarterly reinforcement of the concepts for the relay in question, 5. define operational or procedural controls to restrict physical access to the relay in question, 6. go through the TFE process for CIP-007 R5 since the relay in question has no password capability, 7. create a Cyber Security Response Plan for the relay in question, 8. implement and perform drills of the Cyber Security Response Plan for the relay in question, 9. and annually review the Cyber Security Plan for the relay in question. All of the above is in addition to the five CIP-002 and CIP-003 requirements that would apply whether the relay was electronic or electro-mechanical. The nine additional requirements represent a huge burden on UFLS owning DP/LSEs with no corresponding improvement in reliability. We suggest that Cyber Asset be limited to electronic devices that are programmable via a communication medium such as RS232, USB, Ethernet, Bluetooth, removable media, etc. BES Cyber System uses Maintenance Cyber Asset in its definition, although this term remains undefined. We believe the SDT intended to use the defined term Transient Cyber Asset here.
No
Yes
Thank you for taking our recommendation to exclude temporary changes.
Yes
We agree with the changes.
No
We note that most of the subject topics align with other CIP standard titles. In particular, sub-requirements 1.7, 1.8, and 1.9 align with CIP-009, 010, and 011. These three standards have no requirements for Low Impact BES Cyber Assets. Likewise CIP-003 R1.7 through R1.9 should not apply to entities that have no Medium or High Impact BES Cyber Assets. All of the sub-requirements should be renumbered to 2.1, 2.2... etc. This would match the mapping document and the Guideline section of CIP-003.
No
We believe this training program would more properly be included in CIP-004. Since security awareness and policy should be closely related, we believe the two subjects should both be addressed by CIP-004 R1.1.
No
“...at least a quarterly basis” may be stated contrary to the SDT’s intent. Since a quarter (1/4) is the smallest interval allowed, more frequent reinforcement would be considered a violation while less frequent would not be, since no upper interval limit was established. And like other intervals, quarter

is subject to interpretation as to whether a calendar quarter is intended, or any random three month period measured to the day. We suggest: "… at least once every calendar quarter." Also, please see our comment under Question 9 above.
Yes
Thank you for removing low impact from this requirement.
No
5.4 contains the magic words "where technically feasible", which will require TFEs for items that cannot meet strict compliance. Contrary to the statement regarding inventory, the TFE process will require a detailed inventory of those items an entity is requesting an exception for. We suggest substituting "possible" for "technically feasible."
The comment form provided no room for comments not addressing particular requirements, so we are listing our more general comments here. From the webinar we understand that where the requirements refer to tables where none of the table entries applies to an entity, the requirement itself is not applicable. Since this is not the general case for the relationship between requirements and sub-requirements in NERC standards, we suggest explicitly stating that this is how it works in the CIP standards. We find the Applicability-Facilities Section (4.2) in CIP-003 to be confusing, since all the requirements of this standard appear to apply to the applicable entities and not to facilities.

Suggest removing the 4.2.1 through 4.2.3, or stating more clearly how the facilities affect the requirements. The background section of CIP-003 goes into great detail regarding the table format while CIP-003 itself does not follow this format. Please remove or rewrite this section. The very last statement of the guideline section of CIP-005 references a document we are not familiar with. Please provide a complete reference or link to its location.
Individual
Thomas Lyons
Owensboro Municipal Utilities
Yes
The definition of “Control Center” needs to be very clear. It should be explicitly stated that a Control Center must have control functions over 2 or more BES facilities and that these BES facilities must be located in 2 or more separate geographic locations. If this definition is not clear, smaller entities that might otherwise be considered low impact may be labeled inappropriately as medium impact. The SDT should consider the addition of voltage criteria so that Control Centers are more easily identified. For example, a Control Center could be defined as supporting the real time operation of 2 or more BES facilities operated at 200kv & above or 3 or more BES facilities operated at 100kv & above. In addition, wording should include the following: Control rooms located at generation facilities should be excluded unless they perform the functions of a System Operator as a TOP, BA, or RC and perform control for the above mentioned BES Facilities.
Yes
“Control Center” in section 2.13 should be capitalized.
No
The wording of R1.1 is confusing. It may be more effective if this is divided into two separate requirements. For example: R1.1. Responsible Entities shall update the identification and categorization within 30 calendar days of a modification to BES Elements or Facilities if the modification is intended to be in effect for more than 6 calendar months and causes a change in the identification or categorization of the associated BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. R1.2. Responsible Entities shall update the identification and categorization within 30 calendar days of a BES Element or Facility being placed into operation if it is intended that the BES Element or Facility will be in operation for more than 6 calendar months and causes a change in the identification or categorization of the associated BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.
Yes
No
“And” needs to be struck from moderate and high VSL in the phrase “High and Medium Impact and BES Cyber Assets”.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No

Quarterly reinforcement of security awareness concepts will be difficult to implement and burdensome to document in order to sufficiently demonstrate compliance. The periodicity of on-going reinforcement should be at the discretion of the responsible entities. Annual training on security awareness concepts may be more practically implemented and more easily documented.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Responsible Entities need to be allowed some discretion in evaluating the effectiveness of security-related patches or updates and in determining the potential threat posed by an identified vulnerability. There may be circumstances when unintended effects of a patch or update are more debilitating to a Responsible Entity's Cyber System than the vulnerability being addressed. This may be implied within the requirement since the remediation plan is to be created by the Responsible Entity, but probably needs to be more explicitly defined if the requirement is going to be similarly applied by Compliance Enforcement Authorities throughout the various regions.
Yes
Yes
Yes
Yes

No
If not read in conjunction with the rationale, it may not be understood that an incident is reportable per the terms established by the DOE and by NERC in EOP-004. Perhaps R1.2 should state: A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident as defined in NERC Reliability Standard EOP-004 Attachment 2-EOP-004.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Randy Hahn
Ocala Utility Services
Yes
Control Center – (1) We assume that a Control Center is only a Control Center is used by an BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity (RC, BA, TOP, and GOP entities only) to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. We suggest: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. (3) "support" needs to be better clarified, and limited to only control centers that provide electronic support (specifically exclude any control center that does not provide

continuos electronic data to System Operators, otherwise any control center that receives any verbal instructions or inquiries from a System Operator could be drawn into the Medium impact, as supporting operations by System Operators) BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01
Yes
Attachment I - Bullet 1.3, Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Attachment I - Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet. Attachment I - Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. We suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000.”
Yes
OUS agrees with the requirement but questions whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented.

Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. OUS suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
Yes
Yes
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? We suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable but are instead examples of evidence.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
No
The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. FMPA suggests the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No

Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. OUS proposes to create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. OUS suggest end of the next calendar week.
No
The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. OUS suggests rewording bullet 1.2 to require identification of EAPs and not “secure and control”.
Yes
No
The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? OUS encourages the SDT to develop non-binary VSLs.
No
Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Does video surveillance suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirement, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes physical access points, OUS encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall

material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences, non-electronic door locks that control access to substation control houses that contain Low Impact digital relays, etc. Such an interpretation would then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. OUS suggests adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
Yes
No
On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”.
Yes
No
Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low.
No
No
This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect

and respond to cyber security incidents. Otherwise, how is one to “identify, classify and respond to BES Cyber Security Incidents” on Low Impact systems? This “hidden” requirement is inappropriate. OUS recommends making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know “(w)hen a BES Cyber Se4curity Incident occurs”. This “hidden” requirement is inappropriate. OUS recommends making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire response for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.2 (an) Exercise …” Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
See comments to Questions 34 and 35. OUS believes that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this “hidden” requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
No
Bullet 1.4, what does the word “verified” mean, that the data is “retrievable”, or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
No
Bullet 2.1, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire recovery for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.1 (an) Exercise …” Bullet 2.2 “current configuration” is not accurate. The back-up will not reflect the “current configuration” but the configuration at the time of the back-up.
Yes
Yes
Yes
The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3).
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. OUS suggests that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities.
No
Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.

Yes
No
There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
Yes
Yes
Individual
Tracy Richardson
Springfield Utility Board
Yes
SUB suggests the addition of a definition for the term “BES Cyber System Impact”. SUB assumes that it is in reference to CIP-002—5 Attachment 1 “Impact Categorization of BES Cyber Assets and BES Cyber Systems,” but other entities may not have the same assumption(s). Based on information received during NERC’s November 11, 2011 Electronic Security Perimeter (ESP) webinar, SUB would recommend adding clarification similar to the following language to “BES Cyber Systems”: “If an entity has determined that it has no Critical Cyber Assets, then it is not possible to have an Electronic Security Perimeter, and no BES Cyber Systems.”
Yes
SUB is concerned with the inclusion of Distribution Providers (DPs) in the Version 5 CIP Standards, as well as with the qualifiers proposed for Load-Serving Entities in the Applicability section of CIP-002-5. This inclusion will draw in small entities with no operational capabilities and cause them to go through an administrative burden of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. SUB recommends that a bright line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from CIP-003-5 through CIP-011-5.
No
CIP-002-5 Attachment 1 – Impact Categorization of BES Cyber Assets and Cyber Systems addresses Impact Categorization, but there appears to be no guidance in the actual identification of BES Cyber Assets and BES Cyber Systems. In the Background statement of each of the Version 5 CIP Standards, it is noted that, “Standard CIP-00X-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.” However, CIP-002-5 is titled BES Cyber Asset and BES Cyber System Categorization, with no mention of identification. Measure 1 for Requirement 1 of CIP-002-5 requires physical lists for High and Medium categorization; however there is no list requirement for Low Impact. The following Version 5 CIP (CIP-003 through CIP-011) Standard Requirements imply or assume that all Responsible Entities (regardless of impact) have created a list identifying BES Cyber Assets and BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Assets and BES Cyber Systems list requirement, or altogether removing the Requirement for those with a Low-Impact (or no impact) categorization. SUB believes more guidance and clarity should be provided for the actual identification of BES Cyber Assets and BES Cyber Systems, and suggests general guidelines be provided on how Registered Entities would identify demarcation points where a BES Cyber Asset and/or BES Cyber System begin and end. It is also SUB’s recommendation that a bright-line criteria method for Registered Entities to demonstrate “no impact” and be given an outright exemption from Standards CIP-003-5 through CIP-011-5.

Yes
SUB agrees with Requirement 2, believing this is not a change from previous versions of the CIP Cyber Security Standards, and understands this to already be a part of an entity's annual Self-Certification process.
No
SUB is concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB does not see this as a new requirement, based on previous versions of CIP-003.
Yes
SUB does not see CIP-003-5 R2 as a new requirement(s), but just as a consolidation of requirements spelled out in previous versions of the CIP-002 through CIP-009 Standards.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
SUB does not view this as a new requirement, based on previous versions of the CIP-003 Standard.
Yes
No comment.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
SUB agrees with this programmatic approach to a culture of cyber security by requiring entities to have a Security Awareness Program. However, SUB sees a quarterly requirement as too severe, particularly for entities with Low Impact BES Cyber Systems. SUB proposes separating the applicability based on impact and providing different time basis for each.
Yes
SUB agrees with CIP-004-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R4 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R5 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-004-5 R6 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
In Part 7.2 Requirements for reassignments or transfers, "by the end of the next calendar day" does not take into consideration weekend days. SUB would recommend "by the end of the next business day" for High and Medium Impact. SUB agrees with CIP-004-5 R7 not being applicable to Low Impact BES Cyber Assets and Cyber Systems.

No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
Based on information received during NERC's November 11, 2011 Electronic Security Perimeter (ESP) webinar, SUB would see value in adding clarification similar to the following language: "If an entity has determined that it has no Critical Cyber Assets, or BES Cyber Systems, then it is not possible to have an Electronic Security Perimeter." Requirement 1 of CIP-005-5 again implies that a listing of BES Cyber Systems, including those for Low Impact BES Cyber Systems, has been or would need to be created. Many of the Requirements of the Version 5 CIP Standards can be interpreted to require a listing of BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement in CIP-002-5, or removing the Low Impact BES Cyber Systems Electronic Security Perimeter requirement from CIP-005-5. SUB believes this requirement or non-requirement for a listing should be addressed in CIP-002-5, and SUB's preference is the removal of the requirement.
Yes
SUB agrees with CIP-005-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
There's a typo in M1. "Evidence must includes…" SUB suggests, "Evidence must include each of the documented physical security plan(s)…" SUB does not disagree with requiring operational and procedural controls to restrict physical access to be defined. However, as previously commented in CIP-002-5, SUB is concerned that an entity will need to produce a list of Low-Impact BES Cyber Assets to demonstrate that they have correctly (or incorrectly) categorized BES Cyber Assets in the "Low-Impact" category. As also noted in CIP-005-5 comments, the CIP-006-5, Part 1.1 Requirements apply to Low Impact BES Cyber Systems, which assumes that a list of these systems has been created. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement to CIP-002-5, or removing the Low Impact BES Cyber Systems Physical Security Plan requirement from CIP-006-5. SUB's preference is the removal of the requirement.
Yes
SUB agrees with CIP-006-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees CIP-006-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB agrees with CIP-007-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB appreciates the extended time period to allow for documentation of implementation.
Yes
SUB agrees with CIP-007-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes

SUB agrees with CIP-007-5 R4 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with APPA's comments that point out that when requirements are applicable to All Responsible Entities including Low Impact BES Cyber Systems, these requirements must address "programmatic protection controls". SUB agrees that this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by programmatic plans or procedures will improve cyber security. However, Table R5, Part 5.4 calls for "Procedural controls for initially changing default passwords," in the Requirements, but in the Measures the first bullet says; "Demonstration showing default vendor passwords have been changed, sampled on a locational basis." SUB agrees with APPA's recommended language changes. Requirement 5 of CIP-007-5 again implies that a listing of BES Cyber Systems, including those for Low Impact BES Cyber Systems, has been or would need to be created. Many of the Requirements of the Version 5 CIP Standards can be interpreted to require a listing of BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Systems Identification List requirement in CIP-002-5, or removing the Low Impact BES Cyber Systems Electronic Security Perimeter requirement from CIP-005-5. SUB believes this requirement or non-requirement for a listing should be addressed in CIP-002-5.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
SUB is concerned that the Requirements of CIP-008-5 create potential conflict with the Requirements of EOP-004-2. The development of the two Standards appears to be in parallel with one another, rather than working together. SUB recommends more coordination between the Version 5 CIP SDT and the EOP-004-2 SDT. SUB understands CIP-008-5 to be the "Incident Response Plan" and EOP-004-2 requires the development of an "Operating Plan for Event Reporting." However, CIP-008-5 Table R1, Part 1.1 requires a process to "identify, classify, and respond to BES Cyber Security Incidents" while EOP-004-2 R1.1 requires; "A process for identifying events listed in Attachment 1." SUB recommends the SDT revise the CIP-008-5 Requirement and Measure in Table R1, Part 1.1 to remove the terms "identify" and "classify." Table R1, Part 1.2 requirement of a process to determine if an incident is a "Reportable BES Cyber Security Incident" is in direct conflict with Event Reporting Reliability Standard EOP-004-2. SUB suggests Part 1.2 be removed and coordinated with the EOP-004-2 SDT. Table R1, Part 1.3.3 requires definition of "Internal staff and external organizations that should receive communications of the incident." EOP-004-2 R1.3 requires "A process for communicating events in Attachment 1 to the ERO, the RC… and other appropriate entities." APPA suggests Part 1.3.3 be removed and coordinated with the EOP-004-2 SDT.
Yes
No comment.
No
Table R3, Part 3.2, 3.3, and 3.4 requires different times for updates, both 30 and 60 calendar days. For consistency and clarity, SUB again recommends coordinating with the EOP-004-2 SDT, which allows 90 calendar days for update of the plan.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
SUB agrees with CIP-009-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes
SUB agrees with CIP-009-5 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
Yes

SUB agrees with CIP-009-5 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
The definition of the term “configuration” is unclear. Configuration is not clearly defined in the Glossary of Terms Used in NERC Reliability Standards, Definitions of Terms Used in Version 5 CIP Cyber Security Standards, nor in the CIP-010-1 Cyber Security – Configuration Management and Vulnerability Assessments Standard. Are “configuration management”, “configuration change management”, and “asset management” intended to be synonymous in the way they are used in the CIP-010-1 Standard? Configuration is only mentioned in terms of “security configurations”. SUB recommends that a specific definition be provided for Configuration, Configuration Management, Configuration Change Management, and/or Asset Management. Perhaps, based on the extensive changes to definitions in Version 5 of the CIP Standards, it would be appropriate to create a CIP-specific glossary of terms used in the CIP Standards. SUB agrees CIP-010-5 R1 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
SUB agrees with CIP-010-1 R2 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
SUB agrees with CIP-010-1 R3 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
Yes
No comment.
Yes
No comment.
No
This overall proposal is not substantive enough to objectively assess VSRs and VSLs. SUB recommends that VSRs and VSLs be proposed after Standard Requirements are better clarified, perhaps in a separate, next-phase process.
No
As previously stated, SUB believes that an entity must identify all BES Cyber Systems and Cyber Assets, push systems through the Medium / High impact filter, and come out at the end of the process with a “Low Impact” (or No Impact) list of systems and assets (which may be a “null” list). While there are no requirements to specifically identify Low Impact systems, this does not remove applicability for the Low Impact BES Cyber Systems from the Version 5 CIP Standards. In the Background statement of each of the Version 5 CIP Standards, it is noted that, “Standard CIP-00X-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the Version 5 CIP Cyber Security Standards.” However, CIP-002-5 is titled BES Cyber Asset and BES Cyber System Categorization, with no mention of identification. Measure 1 for Requirement 1 of CIP-002-5 requires physical lists for High and Medium categorization; however, there is no list requirement for Low Impact. The following Version 5 CIP (CIP-003 through CIP-011) Standard Requirements imply or assume that all Responsible Entities (regardless of impact) have created a list identifying BES Cyber Assets and BES Cyber Systems. SUB recommends either adding a Low Impact BES Cyber Assets and BES Cyber Systems list requirement, or altogether

removing the Requirement for those with a Low-Impact (or no impact) categorization. SUB would also recommend that a simple method for DPs and LSEs to demonstrate “no impact” and be given an outright exemption from Standards CIP-002-5 through CIP-011-5.
Individual
Kirit Shah
Ameren
Yes
Definition of BES Cyber Asset – The second line where it states “, when required,” is out of place and as used does not make sense; please remove, or remove the comma. Definition of BES Cyber System – The proposed definition of BES Cyber System contains a reference to a “Maintenance Cyber Asset.” This should be replaced with the term “Transient Cyber Asset.” Definition of BES Reliability Operating Services – Inclusion of Dynamic Response to BES Conditions, the inclusion of Governor response provides for a wide array of systems. Consider listing the systems that should be included. Definition of BES Reliability Operating Services – Inclusion of Controlling Voltage, the inclusion of AVR does not define if it is for voltage control from the generator terminals or from the high side of the GSU. This service can create some jurisdictional problems where part of the system is owned by transmission, and the other part is owned by generation. Definition of BES Reliability Operating Services – Inclusion of Restoration of BES in the list of BES Reliability Operating Services is too broad without clarifying language that only those systems absolutely necessary for the restoration of the BES must be considered as BES Cyber Systems. Definition of BES Reliability Operating Services – Inclusion of Situational Awareness in the list of BES Reliability Operating Services is too broad without clarifying language that only those systems absolutely necessary for the continuing operation of the BES must be included as BES Cyber Systems. For example, there are visualization tools used purely for market participation purposes which serve a situational awareness function but which do not enhance reliability operations in any way and which do not pose any threat to the BES if compromised; those should not be included as BES Cyber Systems. Definition of Control Center – As constructed, the inclusion of the bullet beginning with “Providing information” would cause a facility containing a communications processing node which received information from multiple BES facilities to be classified incorrectly as a control center. For example, a substation containing a MUX which received RTU readings from multiple other substations or a satellite data node in a distributed EMS system located in an unattended communications hub would qualify their locations as control centers. This would have a chilling effect; removing from consideration some otherwise preferable communication systems designs. This clause does not bring in any facilities which would not be covered by the other items in the bullet list; it should be removed. Definition of Cyber Assets - Need to retain "and communication networks". We believe that without keeping the communications as part of the definition, any programmable device at a location, for example, within a substation, is a cyber asset regardless of whether we communicate to it or is used for communications. Our understanding is that this does not follow the original intended purpose of the CIP standards which is to secure remote communications to devices used to control the system. Definition of Electronic Access Control or Monitoring Systems – Remove the words "or BES Cyber Systems" at the end of the sentence. This is related to our comments above. Unless the BES Cyber Systems is not removed, the existing definition of Cyber Assets may require a need to put physical security around each location, for example substation, depending on interpretation. Definition of Electronic Access Point – While the need for a broad definition which allows for the wide range of real-world situations is appreciated, this definition does not properly capture the nature of an access point. The use of “Cyber Assets”, rather than any inclusion of “BES Cyber Assets”, implies that any barrier device anywhere within an Entity is in scope. The use of “restricts” rather than “allows but restricts” logically implies that even an Asset which is not connected to a BES network could be considered as an access point. The use of “interface” adds nothing to the definition and will lead to unnecessary confusion. Proposed replacement definition: “A Cyber Asset which allows but restricts routable or dial-up communication between a BES Cyber Asset and another Cyber Asset.” Definition of Interactive Remote Access – The second sentence adds nothing to the definition and could leave some unintended gaps; it should be removed or it should be clarified that the three items are examples.
Yes
In the application guidelines on page 18 of 30, the table at the bottom of the page needs to include the LSE Function Registration type and LSE needs to be referenced throughout the application guidelines. In the first bullet under Overall Application, the verb tense for “support” and “supports”

switches back and forth. “Supports” is correct. Under High Impact in the 5th line, a word is missing from “it must be noted that there may "be" agreements”.
No
Requirement 1.1 as stated is confusing. Suggested replacement: “Update the identification and categorization within 30 calendar days of the date when a change to BES Elements and Facilities is placed into operation, if the change is intended to be in service for more than 6 calendar months and causes a change in the identification or categorization of any related BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.” M1: It is impossible to create a categorized list of High and Medium impact assets without a resultant Low Impact list. For version 3, auditors have pointed out that you cannot have a CCA list unless you have a list of all Cyber Assets at a location. A similar situation exists in version 5 here as the last sentence to R1 and M1 are in conflict with each other. In R1, the phrase "do not require discrete identification" implies that Low impact BES Cyber Systems do not require categorization at all; but, in M1 it asks for evidence of categorizing of Low Impact BES Cyber Assets and BES Cyber Systems. Thus, R1 and M1 are contradictory and we suggest the last line of M1 should be removed.
No
M2 – Need to change the words after CIP Senior Manager to "or delegate approve" after CIP Senior Manager on the 3rd line of the paragraph for M2 and remove the words "review and update".
Yes
No
R1 Requirement – Change R1 to R2 to match legacy numbering in previous CIP versions.
No
R2 Requirement – Change R2 to R1 to match legacy numbering in previous CIP versions. Also, update numbering of sub-requirements to match requirement number.
Yes
No
R4 Requirement – Add the words "Medium or High Impact" in front of the words "BES Cyber Systems" on the first line.
Yes
Yes
R6 Requirement - The description of this requirement [on page 14 of 22] appears to have a typo, in that a "2" is included at the end of the first sentence.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
R6.6 Requirement - This requirement contains a grammatical error in the form of an extraneous “of” at the end of line 3.
No

R7 Applicability – This section needs to be revised to: Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets, and Associated Physical Access Control Systems of: High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. R7 Rationale - The third paragraph could be interpreted to mean that all authentication credentials must be revoked for personnel to be considered as having their access revoked, rather than revocation being accomplished by revoking only the credentials which can allow the terminated individual to gain access to the Asset in question. If revoking "all" is the intended interpretation, it should be clarified; but, we believe that it would require a substantial amount of resources for no additional security gain and would cause unnecessary enforcement actions. If "all" is not the intended interpretation, the paragraph should be re-drafted to better clarify the intent. Suggested replacement text: Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services), although revocation can be accomplished by revoking all permissions which could allow the terminated individual to gain access to a given Cyber Asset. R7.1 Requirement – The words “at the time of” is poorly-defined, and many possible interpretations of it cannot be technically enforced as there is no threshold. R7.2 and R7.3 Requirements – There is no security benefit to using a one-day requirement for revocation as opposed to a seven-day revocation. In the entire span of UA 1200 and CIP versions 1 through 3, there have been no known incidents where a shorter revocation requirement would have prevented an incident. Consider stating “by the end of the next business day” in circumstances where a transfer may take place on a weekend or holiday. Consider changing all “calendar day” statements to “business day” statements to account for weekends and holidays. Application Guideline - We hesitate to call for more stringent wording, but In the Application Guidelines it seems to indicate that no action is required to revoke access in the case of the death of an employee. Given that unused accounts represent a small but real security risk with no corresponding benefit, the table should be changed to require removal of access in a reasonable timeframe.
No
The VSLs for R1, R2, and R3 should be should be progressive instead of binary. Also, the VSL for R6 has too many “or” clauses. Consider labeling VSLs for sub requirements to eliminate the multiple or statements.
No
R1.1 Requirement - In the requirement “define” should be replaced with “define and implement” for clarity. R1.1 Measure - The requirement states “technical or procedural controls” while the measure states “documented technical and procedural controls.” Please match language of the Requirement and Measure to their intended purpose. R1.2 Requirement - In cases where only one connectivity method exists, please state in the requirement “routable and/or dial-up” R1.3 Applicability - Change applicability for High Impact BES Cyber systems by adding the wording "with External Routable Connectivity." R1.4 Applicability - Why are these controls in place for “non-Interactive” or read only remote access? Would suggest removing this language out of the Applicability section.
No
Application Guideline - Requirement R2, If the Secure Remote Access Reference Document is going to be referenced in the Application Guidelines, then it needs to be included in the ballot packet and voted on along with the rest of the package because auditors may use content of this referenced document for the audit which is not the intended purpose of the referenced document. R2.3 Requirement - Need to define "multi-factor authentication" by adding this term to the definitions document.
No
(1) All the VSLs should be progressive instead of binary. (2) VSL for R1 should be split out into sub-requirements because they do not match the BES Cyber System classification. For example, if a Responsible Entity did not define any technical or procedural controls to restrict unauthorized electronic access for a Low Impact BES Cyber System this should not be a Severe VSL.
No
The Application Guidelines do not sufficiently allow for the development of new types of technology which could provide improved controls. R1.4 and R1.5 Requirements – We have concerned about the term "real-time" as it is not defined. Irrespective of the definition, these requirements should have

the possibility of a Technical Feasibility Exception; to preclude that possibility may hinder mitigating an emergency to issue an alert. We further suggest that, the alert language should be changed from issuing real-time alerts to issuing alerts within 15 minutes along with an option for TFE. R1.6 Requirement - Remove “of” after “entry” on the second line of the paragraph.
No
R2.2 Requirement – Need to remove the words "on a 24-hour basis". This could become an issue if the visitor crosses the midnight time-line. Suggest inserting words to allow a visitor turnover process in cases where the visitor begins work on shift 1 but continues through shift 2. This way the escorts can change without the visitor having to log in and out of the system.
No
R3.1 Requirement – Wording needs to be added to this requirement to prevent systems that are in place prior to version 5 to be forced to perform pre-commissioning testing for version 5. We suggest adding clarification to the Application Guideline on the reasons for a 24 calendar month M&T period and also provide some examples of M&T programs used in the industry.
No
VSL for R1 should be split out into sub-requirements because they do not match the BES Cyber System classification. For example, if a Responsible Entity did not document operational and procedural controls to restrict physical access for a Low Impact BES Cyber System this should not be a Severe VSL.
No
R1 Applicability – This section needs to be revised to: Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets, and Associated Physical Access Control Systems of: High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. Other tables should include similar clarity.
No
R2.1 Requirement – Add the words "security related" in front of the words "software and firmware". R2.1 Measure – Remove the last sentence of the measure as we do not see a reason for it in reference to meeting the requirement.
No
R3.1 Requirement – This requirement should allow for the possibility of an Asset which requires no action, such as a vendor-hardened security appliance. R3.3 Applicability – This requirement should be limited to High Impact BES Cyber Systems and to Medium Impact BES Cyber Systems with External Routable Connectivity. R3.4 and R3.5 Applicability – This requirement should be limited to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, and Associated Protected Cyber Assets. Transient Cyber Assets (stated in the Measure) do not include Physical Access Control Systems or Electronic Access Control or Monitoring Systems per the definition of a Transient Cyber Asset.
No
R4.1 Requirement – As a clarification, at the end of the requirement, add the words "Devices that cannot log a particular event do not require a TFE to be generated" to cover devices that cannot produce logs. R4.2 Requirement – Remove the words "necessitate a real-time alert" at the end of the requirement and replace with "be necessary". R4.2 Measure – Remove the end of the sentence starting with "necessitate a real-time alert" and replace with the word "necessary". R4.3 Requirement – Replace the words "calendar day" with "business day after notification". Suggest making High Impact the next business day and the remaining categories 7 calendar days. R4.4 Requirement – Remove the word "consecutive". R4.4 Measures – Remove the last part of the sentence starting with the words "and records of disposition". R4.5 Requirement – We do not see a reason to rectify deficiency before the end of the next calendar day in every case. We suggest to remove the last sentence or change rectification period to certain number of business days.
No
R5.4 Requirement - would require a massive effort to change passwords for devices already in place in Low Impact locations (for an average mid-sized utility, for example, 200 Low Impact substations with an average of 25 Assets per substation would represent at least 5000 password changes during the implementation phase) with no noticeable benefit to security, given the required physical protections and the unimportance of the Facilities involved. This represents the single point currently

at which the v5 standards treat Low Impact BES Cyber Systems on an individual basis rather than on a programmatic basis, and that substantially changes the nature of the work required to comply with the standards, that is removing resources from the much more important work of securing the High Impact Assets. Also, suggest restating the requirement to simply "Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purpose of this requirement an inventory of Cyber Assets is not required". R5.5 Requirement – Since the passwords are changed at the Asset level not the System level, add the word "Assets" after the words BES Cyber System" in the requirement.
No
(1) VSL R1 through R5 – For Medium Impact Assets, the VSL level should be changed to Medium and High from High and Severe. For Low Impact Assets the VRF should be changed to Low and the VSL should be changed to Low. (2) The VSL for R1 and R2 should be progressive opposed to binary.
No
R1.1, R1.2, and R1.3 Applicability – Include removal of Low Impact BES Cyber Systems from the Applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have.
No
R2.1 Requirement – Remove the words "or test" from the end of the sentence. R2.2 Requirement – The initial timing required by 2.2 is confusing. A literal interpretation would require that the Entity be conducting the test implementation of the plan on the day that the standard goes into effect. The boilerplate wording used here should be replaced with a statement that the plan be tested before the implementation date of the standard and then repeated within 15 months of the pre-implementation test. R2.3 Requirement – Propose deletion of this sub requirement as this sub requirement is only a documentation issue that is already stated in the compliance section (1.2) of the standard. R2.1, R2.2, and R2.3 Applicability – Include removal of Low Impact BES Cyber Systems from the applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have.
No
R3.1 Applicability – Include removal of Low Impact BES Cyber Systems from the applicability section because security incidents have to do with incidents to the Electronic Security Perimeters and the Defined Physical Boundaries that Low Impact BES Cyber Systems would not have. R3.4 Requirement – Need to remove the comma in the requirement section of 3.4.
No
VSL - Make the VSL for R2 progressive opposed to binary.
No
The column headings above 1.4 are incorrect. Suggest adding an Application Guideline for all of CIP-009 as a guideline would be very helpful. R1.3 Requirement – This requirement needs to be reworded to "One of more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality". R1.4 Requirement – This requirement needs to be reworded to "Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery".
No
R2.1 Requirement - The initial timing required by R2.1 is confusing. A literal interpretation would require that the Entity be conducting the test implementation of the plan on the day that the standard goes into effect. The boilerplate wording used here should be replaced with a statement that the plan be tested before the implementation date of the standard and then repeated within 15 months of the pre-implementation test. R2.2 Requirement – On lines 3 and 4, remove the words "initially and". R2.3 Requirement – Change the words "39 months" to "3 years not to exceed 39 months" to match other requirements on a 39 month schedule.
No
R3.1 Requirement and Measure – Remove the phrase "when BES Cyber Systems are replaced". R3.2 Requirement and Measure – Add the words "or incident" after the word "exercise". R3.4 Requirement – Suggest the deletion of Requirement 3.4 as is a new requirement for the CIP standards with no security benefit and it does not align with FERC Order 706.

Yes
No
R1.1.4 Requirement – Add the words "installed on the BES Cyber Asset" to the end of the sentence. R1.1.5 Requirement – Reword requirement to "Any network accessible ports and services; and". R1.2 Requirement – Reword requirement to "Document approved changes to the BES Cyber System that deviate from the existing baseline configuration". R1.5.2 Requirement – Remove the end of the sentence after the words "production environment" as it is too burdensome and unnecessary to document all the insignificant differences between test and production environments.
Yes
No
Application Guideline – The Application Guidelines for R3 needs an editorial correction, “not” rather than “note”. Also, the phrase “Strongly encouraged” is vague and subject to different interpretations, so suggest removing it.
Yes
No
R1.1 Requirement– Add the word "implement" at the beginning of the requirement. R1.2 Requirement – Correct the column header labels. Add the word "Establish" at the beginning of the requirement.
Yes
Yes
No
The implementation schedule needs to be modified to allow different time frames for Low, Medium, and High BES Cyber Systems. Recommend an implementation schedule of 36 months for High and Medium Impact BES Cyber Systems and 48 months for Low Impact BES Cyber Systems.
Individual
Aliza Dewji P.Eng
ATCO Power Canada Ltd.
Yes
Section 2.13 of Attachment 1 contains a 300 MW threshold for generation control centers. The application guideline suggests that the 300 MW value was used because the same value is used for UVLS and UFLS. The rationale for this threshold is flawed as generation control centers have no control over load-shedding. In addition there is a significant difference between a loss in generation and the loss of load. If the intention is that shedding load and loss of generation are to be treated the same, then the 300 MW threshold should apply to all generating units over 300 MW. The 300 MW threshold for generation control centers is far below the 1500 MW threshold for generating units with common mode vulnerabilities set out in section 2.1. In addition, the 1500 MW was approved by industry in the Version 4 consultation. As 1500 MW was derived from the single largest contingency criteria, the principle behind that value is acceptable. ATCO Power suggests that the SDT consider removing generating control centers from section 2.13. If this is done, generation control centers that control 1500 MW or more of generation will be covered under section 2.1, and all generation will be handled consistently.

Individual
Alice Ireland
Xcel Energy
Yes
1) Control Center: We recommend the definition be modified as follows, in order to add clarity: A facility hosting BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for more than one BES generation facility or transmission facility, at more than one location; 2) Routable Protocol: We recommend that

a Routable Protocol definition be created and added using criteria in the "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets" version 1.0, dated June 17, 2010. For example, this would maintain the listing of example non-routable protocols shown on page 27 of this NERC guidance document. 3) Electronic Security Perimeter (“ESP”): Please clarify what is meant by the phrase “collection of Electronic Access Points”. Discussions within a NERC webinar on 11/18/11, “Establishing an Electronic Security Perimeter”, indicated that the general meaning of network based controls would not be impacted.
Yes
1) There appears to be an error in category 1.4 where it references 2.12 (which is UFLS and UVLS). To match version 4 the cross-reference should be to 2.11 (Special Protection Systems). 2) The meaning of 'adversely impact' is unclear. We recommend that the preambles in Appendix I, for high and medium control level facilities, be modified to read: “Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes, cause one or more of the following BES Reliability Operating Services to malfunction, preventing operation within prescribed reliability limits.” It is well understood that 'prescribed reliability limits' are those routine or situational operating requirements for the listed services, and ‘malfunction’ means the inability to respond to reliability needs as expected.
Yes
Yes
Yes
Yes
Yes
No
1) We feel that the requirement should reference cyber security policies created to satisfy CIP-003-5 R2. The wording could be modified as follows: “Each Responsible Entity shall review each of its cyber security policies created to satisfy CIP-003-5 R2 and obtain the approval of its CIP Senior Manager . . . “
Yes
Yes
Yes
Yes
No
1) Table R1, Part 1.1: The quarterly awareness is too frequent, considering many other critical aspects of reliability task execution are successfully and consistently implemented with a longer reinforcement period. A suggested change: Table R1, Part 1.1: "A security awareness program that conveys security awareness concepts and provides on-going reinforcement of such concepts on an established interval, not to exceed a calendar year." 2) Table R1, Part 6.4: The quarterly verification of accurate access provisioning requires more effort than needed if the initial provisioning event is properly executed. A too frequent interval allows for complacency and potential 'process escapes' between quarters. A better process would require continuous verification (lists updated at the time access is granted). This ensures day to day control. The periodic verification should be used to confirm proper execution of this process. Recommended change: "Verify at least once each calendar year that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access."

Yes
Yes
Yes
Yes
No
1) The requirement parts 6.1-6.3 states “Access permission shall be the minimum necessary for performing assigned work functions.” We would like to ask for clarification on the meaning of “the minimum necessary” and how this is to be measured. While someone may not access a CIP facility or BES Cyber System on a regular basis, their job description or the location of an asset/system may require access only infrequently. If access, electronic or physical, is only used occasionally will a violation be considered under the minimal verbiage? 2) We believe the approach of quarterly verification of physical or virtual access to listed BES Cyber assets is too frequent. It assumes the ongoing, as needed verification process for a personnel status change (requires access, now does not require access) may not be executed properly. We believe that a process that requires quarterly reconciliation to ensure secure physical and virtual access is broken. We propose instead that the process for day to day management of personnel status changes for access be reviewed at least annually, and then, based on the results of that review, the frequency modified commensurate with conditions found. For example, a good on-going process should show no 'process escapes' for the previous period, and not require quarterly reviews. A process that shows errors should then be reviewed quarterly until two consecutive error-free verification reviews are performed.
No
CIP-004 R7.1 states, “For resignations or terminations, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.” R7.2 states, “For reassignments or transfers, revoke the individual’s unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.” Finally, R7.3 states, “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the next calendar day following the resignation or termination.” The “same day” and “next calendar day” requirements do not allow for normal business flow especially in the case of holidays, vacations or weekends. Most databases update nightly (or on a 24 hour schedule) so the notification to revoke access, unless done manually every time, would be behind the requirement. If done manually, this would require an unprecedented amount of labor from management, Human Resources and in the case of access, Security. Additionally, for transfers, “the next calendar day” does not allow for the review of new role descriptions and required access reviews. It is recommended that the verbiage for the revocation within 24 hours for “for cause” situations and 7 days for those who no longer require access be re-established for requirements R7.1, R7.2 and R7.3. If not 7 days, a period of time that would allow for notification to management and the necessary databases to be updated.
Yes
Yes
No

1) Part 2.2 from Table R2 requires encryption for all Interactive Remote Access sessions. Some entities still use dial-up access, for any number of reasons such as cost, lack of infrastructure, etc. and encryption is not an option with dial-up access. This section should be modified so as not to require entities to redesign their entire system. The modification could read something like “Require encryption for all Interactive Remote Access sessions, where supported by available technology, to protect the confidentiality and integrity of each Interactive Remote Access session.” 2) In addition, Part 2.3 from Table R2 requires multi-factor authentication, with the additional note that a UserID is not considered an authentication factor. Under many instances, this multi-factor authentication will be difficult to achieve, and by removing a UserID as an authentication factor, it becomes even more difficult. We recommend this be modified to allow for UserID as an authentication factor.
Yes
Yes
1) CIP-006 R1.4 states, “Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.” Please clarify if the standard of “real-time” allows for any system delay? While the time between the alarm and the notification is minimal, there may be a short delay. 2) In regards to the Application Guidelines for CIP-006-5 R1 which state, “Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Xcel Energy provided comments related to protective measures in CAN-0031. Our comments are, “While we appreciate NERC providing some flexibility in how compliance with the six-wall border requirement is met, we feel this is going beyond the scope of what can be discerned from the standard. Furthermore, the source documents seem to introduce even more ambiguity as to what type of materials might be acceptable for construction of your PSP. Instead, we propose that NERC provide clarification on what threat(s) an entity should be protecting against. Then an entity's chosen protective measures/materials could be tested against those threats. This method would be more effective in ensuring a secure environment, and would allow for the introduction of new materials and defense strategies as the industry and vendor products develop/mature.” While the language has been changed from PSP to Defined Physical Boundary the need for clarification on what the threat we are trying to protect from is still needed.
Yes
Yes
Yes
The Table of Compliance Elements, R1 under High VSL states, “The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary.” Please clarify what constitutes an appropriate level of “initiation” of a response. For example, if a response is in motion, such as personnel on their way to the site, does that meet the intent of “initiation” of a response? Additionally, the lower VSL for R1 states, “The Responsible Entity has documented and implemented physical access controls, but logging of authorized physical entry through any Defined Physical Boundary does not provide sufficient information to uniquely identify the individual and date of entry”, while the secondary, Severe VSL (as indicated by the OR) states, “The Responsible Entity has documented and implemented physical access controls, but two or more different and complementary methods do not exist to restrict access to High Impact BES Cyber Systems.” These two VSLs seem to be reversed. Would it not be a greater risk to the BES to have unidentified individuals accessing an area at unknown times than to have a documented and functioning access control system without a secondary measure?
No
Part 1.1 of Table R1 requires that the entity disable or restrict access to unnecessary logical network accessible ports. From the wording of the proposed requirement, it is unclear what a necessary port would include; is it only ports used during normal operations, does it include ports used to access the asset during maintenance, etc. In addition, it is unclear what is meant by “disable or restrict access”. One could argue that location within a PSP and ESP would “restrict access”. This requirement should

be clarified to address this ambiguity.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Request clarification on R1.4; “Information essential . . . that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully.” Does this mean that every time a backup is performed a verification needs to occur, or that when a backup system is initially configured and the first backup is performed, that the verification needs to occur?
Yes
No
Request clarification of what “Review the recovery plan(s) initially upon the effective date of the standard . . . “means in this context.
Yes
Yes
Yes
There will be significant impacts to available resources with this requirement.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Thomas M. Haire, P.E.

Rutherford EMC
No
No
No
CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be modified by one of the following: 1) plainly state those entities with no Bulk Electric System (BES) assets per the definition included in the NERC Project 2010-17, Definition of Bulk Electric System, are not required to comply with this standard or, alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no BES Cyber Assets/Systems or; 2) create a fourth category of “No Impact”, thus no further action required which can be certified annually by the Senior Manager. As the standard is currently stated, smaller entities with non-critical assets of the BES appear not to be involved with this standard, but that is dependent on the interpretation of “Transmission Protection System”. Concurring with the thoughts implied in comment 27.b by PNGC (et al) and considering the recent interpretation of PRC-004 and PRC-005 regarding the interruption of electric current fed from the BES, electronic relays with no communication to the “world” could be considered a Cyber Asset even though the relay has no impact on the BES if it were to fail or was lost or compromised. But regardless, the relay would be forced into the Low category because a “No Impact” or “Non-Critical” category does not exist. The Standard, as written, tends to assume that an entity does have Cyber Assets that can impose a risk to the BES. This assumption should be removed. Furthermore, in the context of protective relays, a small entity may be required by their Transmission Provider to own and maintain Under Frequency Load Shedding (UFLS) relays or a relay system. In the standard, the UFLS threshold is established at 300MW. The small entity may not have 300 MW of total load on their electric system, but their relaying is included in an UFLS system that is much greater than 300 MW. Thus the Standard needs to clarify how the 300MW threshold applies. For example, this small entity’s relay may not be critical to the BES and if degraded or destroyed would not compromise the total capability of the Transmission Provider’s UFLS system as this system is sufficiently small to be encapsulated by the window of design of the parent system. In many cases, the two systems are not integrated and do not have communications across a wide are network. The breaker controlled from the relay in this example may be monitored by SCADA through the use of a dry contact, but the relay itself does not have any other connections to the “world” other than the leads to sense frequency, provide relay power, and to control breaker operation.. Therefore, does the small entity own a Cyber Asset due to the 300 MW level, or is it still exempt? The Standard Drafting Team should work to clearly identify the entities not included by the BES definition. As the standard is currently written, an assumption is implied that all entities own Cyber Assets and all entities’ assets impact the BES. Left to the determination of what would or would not degrade the BES, the Standard Drafting Team has created a series of interpretations and clarifications that will be required from NERC regarding smaller DPs and LSEs. The assumptions and resultant ambiguity of interpretations and clarifications should be removed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Tommy Drea
Dairyland Power Cooperative
Yes
Make certain all terms are formally and clearly defined so that it does not rely on any interpretation outside the version 5 documents. Also, where definitions have been altered, there should be a clear statement as to what former interpretation is no longer valid.
Yes
It is not directly clear if equipment providing operational communications between BES facilities is now in scope as being classified as subject to categorization under the standards. The previous standard clearly excluded this specifically. The version 5 standard does not directly state this positively or negatively. Does this lack of mention mean communications (whether private or commercial) between facilities are in scope if it can effect BES Reliability Operating Services? The standard should be clear on this point as it previously excluded such communications from the scope of the standards. It is common for regional entities to place communications equipment at member entity facilities and mandate connection terms and 3rd party management of equipment. This is typical for Inter-Entity Coordination and Control applications such as ICCP. This practice puts the member in the position of being physically responsible for infrastructure it cannot control. Is it valid for the member to exclude the regional infrastructure from its compliance program? Is it acceptable

for a region to place such potentially critical infrastructure beyond the bounds of their physical control (and CIP program)? If the regional WAN infrastructure is not treated as critical, how can a member/entity's Inter-Entity Coordination and Control system be presumed to be critical (as it is in Attachment 1)?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The Summary of Changes for R1 states in reference to in reference to R1.2 "The non-routable protocol exclusion no longer exists; therefore there is no need for this requirement." It appears that "no longer exists" means that routable/non-routable/dial-up is no longer a criteria for CIP-002 classification. It is presumed that this reference to R1.2 means CIP-005-3:R1.2 has been removed. It is confusing that CIP-005-5 also has a requirement R1.2 that specifically addresses routable and dial-up electronic access points, which excludes non-routable. In the Applicability section on page 8, Electronic Access Point has a description that excludes non-routable from its scope. Also, the "Definition of Terms used in Version5 CIP Security Standards" document defines Electronic Access Points are either routable or dial-up. In the Guidelines and Technical basis section on page 20, in

discussing applicability of trust zones and deny by default, it states “Direct serial, non-routable connections are not included.” Is the Summary of Changes in conflict with other sections of this standard? Does the standard intend that non-routable electronic access points will not be allowed? Does it intend that externally connected non-routable (serial, hard-wired I/O, etc) devices are allowed as cyber assets, but not classified as Electronic Access Points? This should be defined clearly in the standard.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Requirement 1.5 categorically requires all changes to be implemented first in a test environment. There should be a requirement to have a test system, but there should also be allowance that not all implemented changes can be effectively performed on a test system. Further, those entities with Legacy systems may have no practical means of providing test equipment to meet this requirement.

Does this make these entities non-compliant?
No
The idea of monitoring for unauthorized baseline changes is good. The implementation for many systems may be very difficult. Common modern operating systems put up a multitude of ephemeral logical ports—how to automate finding the difference between ephemeral and unauthorized? “Where technically feasible” keeps this from being a compliance issue, but seems to reduce this from a “requirement” to a “guideline”.
No
This requirement needs to me specific as to what controls are required to be tested. Does this mean all controls related to CIP-005 and CIP-007? Does it mean all standards (including personnel security or information protection)? This requirement should be clear.
Yes
Yes
Yes
No
A “Medium” VRF for R1 seems very high, when the details for this requirement seem so general/non-specific. If this item is this important, there should be more specificity as to what is required for information protection.
Yes
The implementation plan should also allow for entities who would like to transition their CIP program to version 5 at an earlier date.
Individual
Saurabh Saksena
National Grid
Yes
General comment: There has been a significant change in the framework from version 4 to version 5 regarding definitions and core concepts such as Critical Assets, Critical Cyber Assets, etc. These proposed changes are not a requirement of FERC Order 706, do not enhance cyber security controls and create administrative burdens when migrating to version 5. There should be a correlation between BES Cyber Systems and the facilities that these systems serve. The current version of the CIP standards provides the correlation and recognize that systems (CCAs) do not operate independently of facilities (CAs). Therefore, applying physical and electronic controls is more transparent. We propose maintaining the current Critical Asset and Critical Cyber Asset definitions and concepts. High, Medium and Low categorizations can still be utilized with the legacy CA and CCA concepts. Regarding the use of the term “annual” throughout the standards, we suggest that the registered entity be allowed to maintain it’s own definition of “annual” based on CAN-0010 guidelines. 1) For all definitions please include the old term that the new term is replacing, as applicable 2) The time periods included in the first and second sentence of the definition of “BES Cyber Asset” are confusing. The 15 minutes discussed in the first sentence and the “delay” discussed in the second sentence are unclear. Suggest re-wording as follows: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The 15-minute period begins to run when the asset is operated, mis-operated, or fails to operate when necessary, regardless of the time period between the asset was degraded or misused and the time the asset is then operated, mis-operated or fails to operate when necessary. 3) BES Cyber System Definition - Maintenance Cyber Asset needs to be defined or if appropriate changed to Transient Cyber Asset
No
Yes

Yes
Yes
Yes
Yes
Yes
No
We recommend eliminating this requirement and moving it into CIP-004 R2 and include policy as part of the training required. This way, all awareness and training would be in CIP-004.
No
We propose retaining the current language in CIP-003-3 R2.
Yes
There should not be a foot note in the standard – make this part of the requirement.
No
R.2 – we suggest a "Lower" VSL for "The Responsible Entity has implemented the required cyber security policy or policies but has failed to adequately document the policy or policies." R.4 – We suggest Lower to Severe VSLs be based on a failure to take action, rather than a specific number of employees who are aware. As drafted, it would be a "high" violation to miss one single employee. That seems overly strict and does not match well with the requirement and measures, particularly when measures suggested includes making an internet posting. We suggest the following: "Lower" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but has not adequately documented the measures"; "Moderate" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 30% -50% of individuals who have access"; "High" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 50% -70% of individuals who have access"; and "Severe" VSL = "Registered entity has taken no measures to make any individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function OR Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 70% or more of individuals who have access" R.5 - Why do the VSLs begin at medium for the failure of one delegation? We recommend "Lower" VSL = failure of one delegation; Moderate = failure of two delegations; High = failure of three, and Severe = failure of "four or more". R.6 – We suggest VSLs structured similarly to CIP-002 - Lower = Change to one delegation was not documented within 30 days, but was documented within 31-41 calendar days of the effect vive date ; Moderate = Change to two-three delegations was not documented within 30 days OR change to one delegation was not documented within 30 days, but was documented within 42-52 days of the effective date; High = Change to three-four delegations was not documented within 30 days OR Change to one delegation was not documented within 30 days, but was documented within 53-63 days of the effective date; Severe = Change to more than four delegations was documented within 30 days of the effective date OR Change to one delegation was not documented within 74 days of the effective date.
Yes
No
We do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training on CIP, as required under current version, is all that should be required.

Yes
Yes
Yes
No
There is no added security by requiring the CIP Senior Manager or delegate to authorize access. We suggest using legacy wording that only requires access to be authorized.
Yes
No
R.1: It seems harsh to include the failure to document a security awareness program as a severe VSL. We recommend the following as a "Lower" VSL "The Responsible Entity implemented, but failed to document a security awareness program" and change the Severe VSL to "The Responsible Entity failed to implement and document a security awareness program." Additional comments around adding “Missed a quarter and/or target audience (authorized physical or authorized electronic)?” R.2: No comments. R.3: The annual training requirement assumes that the initial training was completed before access was granted, therefore, missing a small number of employees with the subsequent annual training does not necessarily indicate high risk to the bulk electric system because these employees presumably had received prior training when their access was granted. We recommend a tiered approach to the VSLs for missing the annual training requirement so that failing to meet the annual requirement for a low percentage of employees (like 10% or less) is a lower VSL, failing annual requirement for between 11-20% is moderate, failing the annual requirement for 21-30% is high, and failing to meet the annual requirement for over 30% OR failing to do the initial training is severe. R.4: No comment R.5: A documentation error should not be a "severe" VSL. Delete the "OR/documentation" part from the Severe VSL and make a Lower VSL that reads "The Responsible Entity implemented, but failed to document a process for personnel risk assessments." R.6: For most utilities, there could be 100s of employees with access, and it seems unrealistic to base the VSLs on one failure with regard to one or two employees. We recommend changing the values in the Moderate - Severe to percentages of employees 10%, 20%, 30%or more. R.7: Same comment as R.6 - change values of one to three employees to percentages.
Yes
No
Requirement 2.2 specifies encryption for all Interactive Remote Access sessions, but does not specify where the encryption is required. If the intent is to require encryption from the user to the Intermediate Device the requirement should specify that clearly. Not all assets currently support encryption, so requiring encryption from the Intermediate Device to the Asset is not practical nor necessary if encryption is being employed outside of the ESP.
No
R.1 and R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
Yes
No
R.1: There should be lower VSL where the processes listed on the tables are implemented but not documented. Add to the Lower VSL: "OR the Registered entity has implemented but failed to document the required physical access controls" R.2: There should be lower VSL where the processes

listed on the table are implemented but not documented.
Yes
Yes
No
Requirement 3.5 requires logging of each Transient Cyber Asset connection. This is not practical as many assets do not have the capability of logging when someone makes a direct physical connection to the asset. Many assets are not capable of logging to centralized logging systems. Also, in a typical day, and engineer in the field may connect a Transient Cyber Asset to many different assets and it would be impractical for one to log each connection.
No
4.1 - The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement. 4.3 - The activity level of some devices is such that they may not generate a logged event every day. Therefore, responding to an event failure with a day may not be possible. 4.3 & 4.5 – there is a conflict between these two. 4.3 requires a response to logging failures before the end of the next day. But, 4.5 requires bi-weekly sampling of logged events which would uncover logging failures. If the logs are being reviewed bi-weekly then logging failures may not be detected and responded to within the next day.
No
Items 5.4 & 5.6 in Table R5 includes the phrase “where technically feasible”. Does that mean a TFE will be allowed? If so, we believe that phrase should be removed and replaced with “as supported by the BES Cyber System” to eliminate need for TFE.
No
R.1 We have the same comment here about percentages for open ports (similar theme from above). What is written in high should be in moderate. What’s in severe should be broken down by percentages/numbers. R.2 Consider severity of patch as recommended by the vendor and the percentage of assets that may not have had a remediation plan associated with that patch. R.3 Consider putting some wording in here around the percentage.
No
There is some concern that multiple plans would prevent one single entry point into the Cyber Security Incident Response Process. We’d like to make the argument that only one plan is necessary and supporting documentation can be created as necessary that supports that plan.
No
The Applicability section of the tables refers to “All responsible entities”. We suggest using the same wording that all the other standards use (High Impacts, Medium Impact, Associated, etc) In R 2.2 In the first sentence, we recommend replacing the word “implement” with “exercise.” This is really about exercising the plan on a regular basis as the plan is already implemented. In 2.3, the "measure" for "relevant documents" does not give adequate guidance to the industry regarding what documents may be acceptable to demonstrate compliance. The "measure" indicates any "dated documentation related to" the reportable incident may be accepted. Please give some additional examples of the specific types of dated materials could be considered acceptable.
No
3.1 The terms “accuracy” and “completeness” are referenced but in terms of completeness there’s not a specific benchmark to compare the document again what should be quantified as complete. The suggestion is again to define a minimum set of information that would be expected in an Incident Response Plan. 3.2 - We recommend that clarity be added to ensure that language represents that review occurs 30 days after closure of the incident rather than invocation; rationale is that you might still be remediating and won't have learnt all lessons. We recognize the importance of the requirements to review the lessons learned, update the Incidence Response plan, and communicate the updates. However under the current structure it creates a rolling compliance effort following each incident. That is, an auditor will require that after each incident one has recorded lessons learned

review, changes to the response plan or that none were necessary and updated communications or that none were necessary. It would be easier to update the plan on a quarterly basis based on the previous quarter's incidents and not have so many auditable events to track.
Yes
No
1.5 – The requirement to preserve data for analysis or diagnosis may slow down the recovery process. There are times when recovery is urgent and must be done in a timely fashion. Is your intent to include this when you say "where technically feasible"? If so, language should be added spelling it out.
No
2.2 – We recommend removal of the phrase "and reflects current configurations" from the requirement. It is acceptable to have backup information that is less than current configuration and still perform a successful recovery. If this phrase is not removed, it will require a backup to be taken and tested for even the most minor configuration changes which is unnecessary.
Yes
No
We recommend the following VSLs for number of days until plan is reviewed in R3: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating plan. We also recommend the following VSLs for number of responsible personnel that the plan updates have not been communicated to: 1 person missed = Moderate, 2-4 = high and 5 or more is severe. We like the VSLs in CIP-010 R3. These recommendations attempt to make CIP-009 R3 consistent to CIP-010 R3.
Yes
Yes
No
We recommend considering emergency equipment replacement (partial outage) as "Exceptional Circumstances" . Based on the nature of our typical outages we would consider this practice to hinder the restoration efforts and bringing systems back on-line in a timely manner. We would certainly be good with language that allowed us to bring systems back on-line, ensure they are stable and then run a scan.
No
We recommend the following VSLs for number of days until documentation is updated in R1: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating documentation. R3 We like this structure. We've suggested this approach a number of times We aren't talking about whether or not this is violation, but rather about the severity of the violation and then rating the severity. We think this is a really good approach.
Yes
No
The footnote here should be part of the requirement.
No
We recommend the following VSLs on R 2: If the process to prevent unauthorized retrieval wasn't done on 1 device that would be low 2-5 moderate, more than 5 is high.
No
Due to the current status of version 4 (not FERC approved), there is potential for overlap of implementation with version 5 that could create extensive rework in a short period of time. This will cause an unnecessary expense to entities while not providing any additional cyber security benefit.
Individual
MIchael Johnson

APX Power Markets
No
Comments: Page 3 – under the Balancing Load and Generation section, “Unit commitment” section the word “know” should be “known”. Page 5 – Monitoring & Control – recommend that you include “situational awareness” into the definition. There is a separate definition for it, but including it here ties the two together better. Example: “… provide monitoring, situational awareness, and control of….” Page 6 – Control Center – include “situational awareness” in the fourth item. Example: “Alarm monitoring, situational awareness and processing specific…” Page 8 – Transient Cyber Asset – I believe it would be good to have examples on what these can be. There will be too much guessing and possible CEA leeway here to make in-consistent application of the definition. This is my major issue with this document.
No
Page 9 – M1. The last sentence that starts with “Evidence of categorization of Low Impact BES…”. What does this mean – it did not may a sense to me. Examples would be a help here. Attachment I – for items 1.4 and 2.1 it would be good to include some reference or example that relates to a Registered Entity that does not own generation, but provides services to those who do. Our business model is a SCADA SaaS provider – we connect generators to the ISO, so the loss of our systems could have significant impact on a regions capability to see what their generation is (situation awareness) and impact the BES if conditions change and the ISO could not see those changes in sufficient time to react to them. I have asked the SDT about our situation and it is felt that 1.4 and 2.1 would cover us, but it would be helpful if it was clearer. For 1.4 suggested modification could be “that includes control or situational awareness of one or more….” For 2.1 suggested modification could be “Generation or Control Center with an ….” I believe the above ties together independent references to Control Centers and Situation Awareness to make it clearer on their importance and impact to the BES .
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
This will be very difficult to implement for Service Vendor where the individual executing the service will not necessarily be the same person. This happens with hardware issues and the dispatch of the first Technician who can respond to the ticket. Getting vendors to agree to training would be almost

impossible for large service vendors like DELL, HP, IBM. I would like to suggest that the Guidelines include examples for exceptions to having this type of training that does not include an “emergency”. We can get around this by declaring everything an “emergency”, but that is not the spirit of the requirement. If we have hardware in a remote data center a service Tech may be brought into the facility and then left with the hardware while the work is being performed. The personnel bring the person into the facility are not employees of our company and we are charged for each 25 minutes they can not do other tasks. Would like to see provisions for exceptions that are documented with some type of mitigation. I do not have a suggestion on what they could be, but would be will to help the SDT define what the mitigations are.
Yes
Yes
Yes
Yes
Yes
Yes
No
Encryption and multi-factor of internal communications to some type of devices could be a problem. Encryption can be expensive for devices to implement and vendors may not be willing to provide that. Agree with the External communications that are coming in-bound. Need to allow for exceptions related to internal communications.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Real-time alerting is error prone – daily log review should be allowed as an alternative for those items that can generate a high number of false-positives.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Need to allow the Registered Entity (RE) to define what the baseline configuration items are and will be monitored. This is not specifically spelled out that I can see. If the baseline configuration is not cleared defined (or allowed to be defined by the RE), I can see the CEA defining their own set of items that the RE may not being watching for.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Scott Bos
Muscatine Power and Water
Yes
MPW is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls (CIP-003 through CIP-011). This approach also appropriately maintains an ultimate focus on protecting the BES elements, which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the BES from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. If the SDT does not take this recommendation,

then the following comments are submitted concerning Version 5 CIP Standards. Significant work needs to be performed on the definitions. Many times new definitions are proposed in version 5 that aren't an absolute necessity. This would require entities to unnecessarily revise documentation and drawings just to meet new wording in a definition when the old definition or a change to the definition itself, rather than the term/phrase, would suffice. For example, instead of changing Critical Cyber Asset to BES Cyber Asset, retain the term Critical Cyber Asset and change the definition of Critical Cyber Asset to include "within 15 minutes". Definitions may also confuse and unnecessarily expand the scope of compliance. This will likely generate the need for Compliance Application Notices and Standard Interpretations. The CIP Rev 5 definitions and requirements are confusing in that they require entities to carefully align separate definitions and requirements to understand the full impact. They also unnecessarily expand the compliance scope into assets not currently covered by CIP Rev 4. This expansion will increase the burden on almost all entities. One example is, a BES Cyber Asset is defined as a "Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact one or more BES Reliability Operating Services". The use of "adversely impact " is ambiguous and will lead to people applying their own interpretation to what "adversely impact" means. An entity may have generation connected at the distribution level that when unavailable may adversely impact any one of a number of items listed in the definition of BES Reliability Operating Services. MPW recommends the SDT update BES Cyber Asset to be: "A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, would impact the reliable operation of the BES within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance". This recommend definition is based on and is aligned with Section 215, Electric Reliability, (a), (4) of the Federal Powers Act. The above recommended definition would also allow for the definition of BES Reliability Operating Services to be deleted, since BES Cyber Asset is clearly identified. The definition of BES Reliability Operating Services includes several items that a non-BES user or owner does in real-time. Other examples and opportunities for improvement: 1) BES Cyber Asset: Contains multiple references to other definitions. It is unclear as to the "within 15 minutes of its operation" inclusion. The redundancy of devices should be taken into consideration if there is a totally isolated redundant system providing the same functions or in a supervisory role. In protection schemes, there are primary and secondary relays which protect the same lines and a good practice recommends the relays have different logic/hardware to avoid common mode failures (totally independent of each other). 2) BES Cyber System: Need to correct reference to Maintenance Cyber Asset 3) BES Cyber System Information: This begs a definition of "BES Cyber System Impact" (is this based on section 215 of the Federal powers Act?). 4) Situational Awareness: Definition includes the term "Situation Awareness Operating Service" that is not defined. The Current day and Next Day Planning functions can normally be performed on a corporate PC. Does this bring the entire corporate network into scope? 5) Control Center: Based on this definition, a Control Center could be a building at a substation with 2 RTU's that monitor a 345 KV substation with multiple transmission facilities (lines) and a 115 KV substation with multiple transmission facilities (lines) in two different yards (locations) but geographically adjacent. Need to clarify that the two or more locations refers to some type of geographical separation. If not, the control building could meet the bulleted items under the Control Center definition. 6) Transient Cyber Asset: Break up the 3rd qualifier based on the intention of the SDT as such: "3) capable of altering the configuration, or (and) 4) capable of introducing malicious code to the BES Cyber System." A second example of where definitions may also confuse and unnecessarily expand the scope of compliance is shown just below: 1) CIP-002-4 requires cyber controls on: Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. (Emphasis added) Whereas: 2) CIP-002-5 requires cyber controls on: Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES

restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. 3) Medium Impact Rating (M) Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: 4) 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation (emphasis added) The concern here is that every Distributed Control System (DCS) that controls two or more generators or substations with a total output of more than 300 MW will now be subject to the CIP Standards. Even if the DCS is not externally connected by serial or routable protocols it will be subject to the CIP standards.

Yes

MPW is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. Issue: As currently drafted Version 5 of the CIP standards: • Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. • Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. • Does not consider that smaller Entities have a much lower impact on the BES • Greatly exceeds FERC's 706 order without justification. Proposed Solution: 1) Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: • Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed by the drafting team in Rev 5 • Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. ¶253-258, 270-273 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. ¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. ¶294-297 • Not exceed FERC Order 706: • ¶284: "… there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." • ¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find sufficient justification to remove this provision at this time." 2) Develop a new standard for High Impact Assets: • That identifies which assets in CIP-004-2 are High Impact and • Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3) Develop a separate standard for the Low Impact assets or abandon this concept. • Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4) Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described in this paper and meet FERC Directives in order 706 If the SDT does not take this recommendation of maintain CIP-002-4, then MPW submits the following comments. Keep the "bright-line" criteria thresholds defined in CIP-002-4 in the CIP-002-5 standard. There was much industry input into developing these thresholds and it does not seem appropriate to modify them

again. It is difficult for utilities to keep up with the changing thresholds in the changing CIP versions and associated implementation plans, with no BES reliability improvement Issue - 1 high Impact, bullet 1.2, states: Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority. MPW does not understand how this can be applied to every BA, regardless of size. Upon review bullet 1.2 has qualifiers for a TOP in order to be a High Impact category (notwithstanding that a TO should not be included since TO's are not required to have primary or backup control centers). We can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of lines, Blackstart Resources, etc, for being considered High Impact or Medium Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, we want to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA in North America, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the same High Impact Rating? Issue - Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. There is no guidance given for transformers. Many entities may treat a facility that has multiple voltages as separate substations, with separate control houses, and may be assessing the independent Impact Level of each voltage as separate facilities. Therefore, there must be some guidance on how to deal with transformers. Furthermore, it is suggested that the weight value given a transformer (if transformers are to be included in the calculation) be the weight value of the secondary, not primary side. For example, a 345kV substation may have a single 345kV transmission line out of it, weighted at 1300. That same substation may then have two 345kV/230kV transformers. It is not obvious from criterion 2.7 what the total weight of the substation would be. It is suggested that the secondary voltage be used (if transformers are to receive a weighting value) making each of these transformers valued at 700, for a total of 2700 at this substation, making it Low Impact. However, if the primary voltage level was used to determine the weight, the transformers would each count for 1300, making the total weight value of this substation 3900, and a Medium Impact facility. It is suggested, if transformers are to be included, that the secondary voltage be used because, from the 345kV bus in this example, its two additional outlets (the transformers) are only capable of 230kV outlet flows, even though they are connected to the 345kV bus. Issue - Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Issue - Criterion 2.11 in Attachment I states "Each SPS, RAS or automated switching scheme that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations." It is unclear whether the phrase "that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations" refers to the SPS itself or the BES elements that the SPS operates. It is possible (and likely) for an SPS to be a higher Impact Level than the BES elements that it operates. Assuming the phrase is meant to apply to the SPS, a suggested re-wording of this phrase is the following. "Each SPS, RAS or automated switching scheme that operates BES Elements and is capable of causing one or more IROL violations if the SPS is destroyed, degraded, misused or otherwise rendered unavailable. MPW proposes the following: Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency

No

Issue - What is the NERC basis for 30 days? Many Utility reviews are performed annually. NERC has not provided any technical justification for a 30 day update. An annual update is sufficient based upon the low probability of a serious cyber or physical attack. Issue - The text "all other BES Cyber Assets and BES Cyber Systems … shall be deemed to be Low Impact." This text appears to include all BES Cyber Assets in CIP scope. This has NOT been directed by FERC Order 706.

No
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”.
No
Issue – MPW believes the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.
Issue - Most of the changes made to CIP-003, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, but do result in increased bureaucracy and implementation costs for 241 entities in North America with existing programs. MPW suggests the FERC directives be addressed within the structure and language of CIP version 4. MPW proposes the following requirements for CIP003-5: R1: Cyber Security R2: Leadership R3: Exceptions R4: Information Protection
No
Issue - This is an administrative task and once implemented does not add to BES security.
No
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”. Issue – MPW suggests changing to annual “review” and NOT approval. Entities need not “approve” the same security policy if there are no changes or updates.
Yes
Yes
No
Issue: What is the justification for documentation within 30 days?
Yes
No
Issue - Many of the changes made to CIP-004, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for the 241 entities in North America with existing programs. MPW suggests the FERC directives be addressed within a structure and language that is more in line with CIP version 4. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access
Yes
Yes
No
Issue – MPW recommends adding clarification to R4.4 in terms of vendor support from foreign companies. Also, please clarify when an Entity or contractor is initially in the CIP Standards then they are removed (for some reason) then they are brought back into CIP compliance responsibility. Is the risk assessment previously obtained still valid if obtained within 7 year period?
Yes
No
Issue – MPW wants to point out that in FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the Senior Manager authorize every individual change down to the account level. The version 5 draft is an additional administrative burden that does not commensurately improve security of the BES and

creates a disproportionate amount of administrative bureaucratic work.
No
Issue - For reassignments requiring a different level of access, there may be the need for a large amount of work in setting up new user accounts, modifying user accounts, changing firewall and router rules, etc, that cannot be accomplished by the end of the next calendar day without jeopardizing reliability. This is also an issue for BES Cyber System information for entities which are using document management systems with individual accounts to restrict access to information. It is typically easier for most Entities to “remove” an account than it is to “modify” an account, yet the modification of these accounts is subject to a single calendar day while the removal of these accounts is allowed for 30 calendar days. Due to the amount of reconfiguration needed for these types of changes, MPW suggests to allow at least 7 calendar days for modifications in access levels. Issue - FERC Order 706 did not direct a change. MPW recommends retaining CIP-004-4 where revocation already is covered. Issue - The time requirements are exceedingly restrictive for Medium Impact BES Cyber Systems. Allowing 7 calendar days for R7.1 and R7.2 would be more acceptable and practical for systems that may not be controlled centrally. Issue - MPW values how the SDT tried to give treatment to the “immediate revocation” requirement of the FERC order in Part 7.1. However, MPW feels the current language is broad, vague and considerably open for interpretation. Even with the footnote qualification, an auditor could still interpret “at the time” to mean literally “to the minute”. Complicating matters is the fact that there is often no way to determine specifically when a person resigned or is terminated. MPW suggests for Part 7.1 to restate as: “Develop and implement a program to revoke an individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination”. This way, the Entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that Entities use shared accounts for remote access. Suggest adding “...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1”.
Yes
No
Issue - R1.1. To MPW, this appears to require that Entities document Low Impact Cyber Systems. This requirement should not be required for Low Impact BES Cyber Systems; otherwise, Entities would have to prove to auditors that external routable connectivity is not used at EVERY Low Impact BES Cyber System.
No
Issue - This Requirement disregards the fact that some Entities have their own (unique) communication network from the Control Centers to the Substations. Adding encryption devices and additional devices adds additional points of failure without increasing security. Exceptions should be made for interactive remote access across company-owned and operated communication links.
Yes
No
Issue - In the “Measures” column of Table R1, Part 1.1, it states the need for documented “operational and procedures controls”, while the Requirement states “operational or procedural controls.” MPW highly recommends to correct the Measures column to be consistent. If the error was in the Requirements column, MPW disagrees that operational physical access control systems should be required for Low Impact BES Cyber Systems. Issue - The Requirement in Table R1, Part 1.2 and Part 1.3, should define whether or not these physical access controls are to be operational, procedural, either, or both for Medium Impact and high Impact Cyber Systems as was done in Part 1.1 for Low Impact Cyber Systems. If operational controls are required, is a separate operational physical access control system needed to monitor the primary physical access control system or is it allowed for a system to monitor access to itself? Issue - For CIP-006, in general, MPW disagrees with changing the definition name from Physical Security Perimeter to Defined Physical Boundaries because it unnecessarily creates the need to update numerous procedure documents and physical security drawings, etc. MPW wants to be clear that changing the term does not, in any way, improve security, but increases confusion and adds costs for the 241 entities in North America that have Physical Security Perimeters.

No
Issue - R2.2 does not seem applicable to Medium Impact Substations. The logging of entry and exit of visitors will be tedious without bringing much value. R2.2. should only be applicable to Medium Impact Control Centers.
No
Issue - R3.1 and R3.2 will be exceedingly troublesome for Low Impact Facilities that use procedural controls for Physical Access Control. MPW wants to know what hardware or devices would be included? R3.1 and R3.2 should only be for applicable electronic physical access control systems.
Yes
Yes
No
Issue – MPW suggests changing the term “remediation” to “mitigation.” R2.3 appears to require the installation of the patches, where some Entities may mitigate the vulnerability through procedural controls.
No
Issue - R3.1. Allows the Responsible Entity to choose which approach they want to take to “deter, detect, or prevent.” If a Responsible Entity chooses to deter or prevent malicious code by procedural controls on isolated control systems (i.e. non-routable serial links), MPW wants to point out that requirement R3.2 and R3.3 are impossible to achieve compliance. Furthermore, R3.3 requires modifying a tested and working control system at a substation with the possibility of inadvertently introducing malicious software with manual updates (e.g. using thumb drives to install signature updates on non-networked systems). MPW recommends excluding Medium Impact BES Cyber Systems that do not have external routable connectivity. (Most AV or malicious code software cannot recognize new malicious code such as Stuxnet until the signatures are discovered anyway.)
No
Issue - FERC Order 706 does NOT direct these changes. CIP-007-5 R4.1 - The enumerated list is too prescriptive for the requirement. Add to guidelines. CIP-007-5 R4.2 – Some assets can log, but not alert. Remove “real-time”. CIP-007-5 R4.3 – MPW requests a clarification on timing. MPW proposes revised text, “Activate a response to event logging or alerting failures before the end of the next calendar day after identification.” MPW appreciates that the SDT allowed entities to develop their own system events related to cyber security, but this leaves an open door for auditors to apply their own approach (and interpretations) to what the THEY believe is acceptable. MPW believes R4.1. will be troublesome for Entities to prove compliance with Medium Impact BES Cyber Systems with no external routable connectivity, unless the auditors accept the configuration files and not the actual logs. Issue - R4.2. This Requirement also leaves a large audit hole for the Entity determining what events necessitate a real-time alert and the auditors having differing opinions of what they feel the entity should include.
No
Issue – MPW recommends to delete R5.2 because it replicates the CIP-004 access authorization requirements and could create a double jeopardy situation. Issue - R5.5.1 – FERC Order 706 did NOT direct a change to password length. Although an increase in password length from six to eight characters improves security, an increase to ten would improve it more and so on. This begs the question “Where does one stop?” Not all assets have capability for longer passwords. MPW recommends retaining the six-character password. Issue – MPW recommends that R5.4. be limited to Entities having a policy in place that all default passwords should be changed. Proving compliance at a sampled location opens up the door in an audit to have Entities having to prove compliance on all their BES cyber systems if there is 1 finding. That 1 finding would require the Entity to have to inventory all Low Impact Cyber Systems and show that every system had the default password changed. The requirement also leaves open the auditor’s interpretation of what is considered a Low Impact Cyber System at a sampled location, since there is not an inventory required by the Standard.
Yes

No
Issue – MPW recommends the SDT to coordinate more closely with EOP-004-2, SDT
Yes
Yes
Yes
No
Issue - R1.5 states, “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.” As FERC Order 706, paragraph 708 states, “should not impede or restrict system restoration”, MPW recommends this proposed revised text: “Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required by Requirement R1.
No
Issue - The wording in the Requirement Column of Table R2, Part 2.2, implies that all backup media must be tested annually. If an Entity, for example, has 25 Windows Servers – that entity should be able to annually test a Windows backup without having to test the backup for each system, especially if the same backup system is being used for all Servers. This is even more extreme in the case of substation cyber assets, such as protective relays. MPW recommends changing the language from “Test any information used in the recovery …” to “Test information, for each type of Cyber Asset, used in the recovery …”
No
Issue - In Table R3, Part 3.4, the language “Update recovery plan(s) to address any organization or technology changes…” is exceedingly vague with regards to technology changes. MPW recommends wording as “Update recovery plan(s) to address any organization or implemented technology changes…” Issue - R3.1. Is not clear on how soon the recovery plan has to be updated “when BES Cyber Systems are replaced”. MPW suggests to include “or within 30 days of when BES Cyber Systems are replaced.” Additionally, MPW recommends that “Update recovery plan(s) to address any organization or implemented technology changes that would prevent a successful implementation of the recovery plan”
Yes
No
Issue - The draft requirement is excessively prescriptive, which was not directed by FERC. Move these details to guidelines. MPW recommends limiting the applicability to High Impact Critical Cyber Assets, which will allow Entities to focus security improvement efforts on the highest priorities. Issue - R1.1. Will be tedious and extremely time-consuming for Medium Impact BES Cyber Systems at substations/plants. The number of IED’s and programmable devices is quite large and some of these devices may have multiple modules or add-on boards with different software versions. Issue - R1.2. and R1.4. will create many problems when making emergency repairs in the field that require replacing a “card” or “module” with different software versions and obtaining CIP Senior Manager approval without any security benefits for the BES. MPW suggestion: Provide a separate requirement for Medium Impact Control Centers and Medium Impact Systems excluding Control Centers which allow more flexibility for the type of environments and equipment. For Medium Impact BES Cyber Systems excluding Control Centers could require documenting baseline configurations on only a subset of the cyber assets (e.g. HMI’s, EAP’s, etc.) not including meters, gauges, battery chargers, electronic programmable thermostats, relays, modules, PLC’s, etc
No
Issue - MPW recommends that the applicability of Table R2, Part 2.1 include only “Medium Impact BES Cyber Systems with Routable Connectivity."
No
Issue - Annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very

costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed. MPW recommends allowing Medium Impact Cyber Systems to have 2 years between vulnerability assessments. Issue - Though FERC directed guidance for Vulnerability Assessments, the rewritten Standard's general reference to "security controls" could result in varying interpretations and likely expansion of assessment scope. Issue - R3.1. Needs to be reworded to more clearly define if the assessment is a vulnerability assessment or only an "assessment of the security controls", such as the EAP and Physical Access Controls. Issue - R3.2. Should allow entities to perform an active vulnerability assessment on either the production system or the test environment to meet the requirement. This will allow entities to make the choice on which environment to use and not require the documentation of differences between the test environments and production environments that leave entities open for interpretation of differences by auditors. Issue - For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where "test" systems just aren't economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. Issue - For Part 3.3, please clarify whether "new Cyber Asset" means literally that or, more reasonably, could mean "new Cyber Asset category" or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn't make sense.
Yes
No
Issue - R2.1. Needs to include additional clarification of devices that are included. Where do protective relays or devices that have flash memory or other on-board memory media fall? Does this apply when reusing the device from a Medium Impact BES Cyber System to a Low Impact BES Cyber System? The application guideline does not distinguish if there is a difference between impact levels and only refers to reuse outside of a BES Cyber System (e.g. could go from High-Medium-Low without being erased.)
Yes
No
Issue - It is imperative for the industry to know whether or not Version 5 will supersede Version 4 well in advance of any implementation plan. If Version 4 has a short implementation period before Version 5 is in effect, entities will view their efforts to comply with Version 4 as "wasted" in many cases because the infrastructure required for a Version 4 Critical Asset is more than that of a Version 5 Medium Impact facility. It would be irresponsible to ask entities to "over-protect" facilities that will not be High Impact with Version 5 right around the corner. In addition, this could also have a drastic impact on decreasing reliability as many entities may elect to remove all routable protocols and dialup access to cyber assets within Version 4 "Critical Assets", to bide them time until Version 5 becomes effective. During this time, engineers would not have access to troubleshoot protection systems, retrieve fault data, and perform multiple other duties without having to travel to a remote site – this could result in prolonged customer outages, and possible instability with known defects in design taking longer to correct. Entities realize that NERC has made an effort to do this, however, there is still risk associated with version 5 not passing in time to supersede version 4. This could be catastrophic to the standards development process.
Individual
Robin W. Blanton
Piedmont EMC
No
Yes
CIP-002-5 makes great strides to remove ambiguity and categorize the potential impacts of Cyber Assets. However, the standard should be changed in one of the following: 1) plainly state those entities with no BES assets per the definition are not required to adhere to this standard or,

alternatively, the Senior Manager must annually certify that the entity has no BES assets per the definition thus no Cyber Assets; or, 2) create a fourth category stating No Impact, thus no further action required which can be certified annually by the Senior Manager. As the standard is currently stated, smaller entities with non-critical assets of the BES appear not to be involved with this standard, but that is dependent on the interpretation of “Transmission Protection System”. Concurring with thought implied in comment 27.b by PNGC (et al) and considering the recent interpretation of PRC-004 and PRC-005 regarding the interruption of current fed from the BES, electronic relays with no communication to the “world” could be considered as a Cyber Asset even though the relay has no impact on the BES if lost, but the relay would be forced into the Low category because a “No Impact” or “Non-Critical” category does not exist. The Standard, as written, tends to assume that an entity does have Cyber Assets that can impose a risk to the BES. This assumption should be removed. Furthermore, in the context of relays, a small entity may be required to own and maintain UFLS relay or relay system by the Transmission Provider. In the standard, the UFLS threshold is at 300MW. The small entity may not have 300 MW of load, but their relaying is part of the design of an UFLS system that is much greater than 300 MW. This small entity’s relay is not critical to the BES and if degraded or destroyed would not compromise the capability of the Transmission Provider’s UFLS system as the two systems are not integrated and do not communicate. Therefore, does the small entity own a Cyber Asset due to the 300 MW level, or is it still exempt? The Standard Drafting Team should work to clearly define the entities not included by the definition. As the standard is currently written, an assumption is implied that all entities own Cyber Assets and all entities assets impact the BES. Left to the determination of what would or would not degrade the BES, the Standard Drafting Team has created a series of interpretations and clarifications that will be required from NERC regarding smaller DPs and LSEs. The assumptions and then the created ambiguity for interpretations and clarifications should be removed.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R1 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, R2 will not apply to those utilities.
Yes
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R2 will not apply to those utilities.
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R3 will not apply to those utilities.
Yes
No
The assumtion is that CIP-002-5 will be changed so that utilities that do not have any BES will not have any Critical Cyber Assets or Systems and therefore, CIP-003-5 R5 will not apply to those utilities.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Marc Child
Great River Energy
Yes
The word “any” in the definition of “External Routable Connectivity” can be a bit misleading, and could be mis-interpreted as being similar to the “any” rule commonly found on a firewall. Recommend the SDT change “any” to “a”. The definition of “Interactive Remote Access” seems to refer to a person having interactive access to the operating system of the cyber system, but what about at the application layer? How does an entity give CIP-005 treatment to an EMS/DMS system in a control center that is accessed via a fat-client application via “remote” employees? The SDT should strongly consider adding a definition for the word “Access” (from a cyber perspective), or specifically state that an entity can make their own definition of access such that different treatment can be given to high-risk access versus low-risk access. High-risk meaning the ability to interact with, operate, modify, or cause availability issues with a BES Reliability Operating Service. Other examples where “access”, if left undefined, could cause problems for an entity are: VMWare hypervisors, Oracle database clusters, or NAS systems that contain both BES and non-BES data/systems. Is the entity required to give CIP-004 treatment to an accounting clerk who has “access” to a receivables data table on an Oracle cluster that also hosts the backend database to a (BES) load control or EMS system? The definitions of “Physical Access Control System” and “Locally Mounted Hardware of Devices Associated with Defined Physical Boundaries” (the latter defined within the CIP-006-5 standard) do not specifically define workstations used by guards to monitor Defined Physical Boundaries, nor do they define physical security panels which control (usually many) door readers and alarms. Are these two types of assets in scope for CIP-006-5 or not? The definition of Electronic Access Control or Monitoring Systems is still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting (“AAA”) of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument,

the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA process, and therefore an Electronic Access Control cyber asset. Likewise, a PC in the Security Operations Center that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or "bright-line" set of criteria for Electronic Access Control or Monitoring Systems. (The same concern applies to Physical Access Control Systems as well). Lastly, the definition of "Transient Cyber Asset" leads one to believe that this only applies to devices directly plugged into other Cyber Assets, as opposed to those temporarily plugged into the ESP network. We ask that the SDT review this definition against CIP-007-5-R3.5 to ensure this was the intention.
Yes
Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. Suggest criteria 2.4 be modified to read "Each Blackstart Resource identified in its Transmission Operator's restoration plan used to provide power for remote start of another generation unit(s)". Criteria 2.11 contains the words "…if destroyed, degraded, misused". (Twice). This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the "15 minutes" qualification as defined at the top of the Medium Impact Rating section. Criteria 2.12 refers to a "system" – as in "Each system or Facility…" – that implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. This seems like an odd exception. Recommend removing "Each system or". Lastly, page 30 of the draft standard contains an example methodology or process flow for categorizing BES Cyber Assets and BES Cyber Systems. We realize that this graphically illustrates the overall intent of the SDT for CIP-002-5, but in reality we still have a standard that an entity will interpret as: Step One – list all my High and Medium facilities ("critical assets"). Step Two – list all my High and Medium cyber assets ("critical cyber assets"). This point of view is further supported by the fact that when you boil down all the security controls in CIP-003-5 through CIP-011-5, there really isn't any appreciable difference between High and Medium requirements. Therefore, the additional paperwork burden of stratifying High and Medium facilities and High and Medium cyber assets doesn't seem to be worth the effort. We understand that there is pressure to expand the scope of CIP to more hard assets, but let's not hide behind this High/Medium smokescreen and instead be honest with industry. Modify items 1.1 through 2.13 on Attachment I to be "All these assets have a Critical Impact Rating". Requirement 1 should therefore be "For all cyber assets including associated physical and electronic access control and/or monitoring systems and associated protected cyber assets, that support one or more BES reliability operating services at a Critical facility, apply the controls as specified in CIP-003 through CIP-011". If there are cases (like CIP-010-5-R3.2) where specific "High Impact" systems are intended, then say so in the requirement: "For Control Centers, perform an active vulnerability assessment every 39 months…".
No
What constitutes a "change to BES Elements…" per part 1.1? Suggest modifying this language to simply state that new or retired assets be added or removed from the list within 30 days of commission or decommission. For M1, we believe the intention is that entities are not specifically required to list their Low Impact systems, therefore we would recommend the last sentence be changed to "Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems is not required, but instead may be demonstrated by the application of the required controls". (New words are "is not required, but").
No
Recommend that this requirement and all others that use the words "…initially upon the effective date of the standard…" have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It's not reasonable to assume that every entity is capable of executing all procedures "upon the effective date". Minor point, but this is the first time "CIP Senior Manager" is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5. In section "B. Compliance", under sub-section "1.2 Evidence Retention", there is a typo in the second to last line. Please change "complaint" to "compliant". I'm sure this was unintentional, even though it sort of fits either way.
Yes

Yes
Yes
Yes
Yes
No
Are the measures listed under M5 actually examples of compliance, meant to be prescriptive? These are very specific and imply requirements. On this point, throughout the standards, measurements are now tightly tied to requirements and are much more prominent. We feel this is rightly so. However, we need to be very (very) careful that examples are stated as examples, lest “measures” become “requirements” themselves. Please state (somewhere) the compliance applicability of Measures. In the second bullet under M5, CIP-002-5 R3 is mentioned. There is no R3 in CIP-002-5. In the last sentence in the last bullet under M5, the words “…of the plant managers…” is mentioned. I don’t think it was the intention of the SDT to be this specific. In fact, this entire bullet is one huge run-on sentence, confusing, and should be redrafted for clarity.
Yes
Yes
Yes
No
Parts 2.2 and 2.4 seem somewhat redundant. If there was a specific distinction intended by the SDT, please rewrite to make this more clear. Part 2.10 needs a bit more clarity to understand what was intended. Was this meant to be technical training on how systems talk to each other over a network? Or is it for general knowledge on risks and controls of routable networks? Please add more clarity here.
No
One potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for “transient” workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. We request that the drafting team add some words to R3 (or Part 3.2) to make clear the requirements for this category of worker.
No
One potential oversight in all versions of the CIP-004 standard is guidance on the PRA requirements for “transient” workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. We request that the drafting team add some words to R4 to make clear the requirements for this category of worker. The Applicability sections of R4 and R5 are different. This appears to be an oversight by the SDT, as it doesn’t make sense to design a PRA process for one set of assets, but implement it for a different set.
No
The Applicability sections of R4 and R5 are different. This appears to be an oversight by the SDT, as it doesn’t make sense to design a PRA process for one set of assets, but implement it for a different set.
No
Parts 6.1, 6.2, and 6.3 seem to imply that the CIP Senior Manager must specifically delegate persons who have the authority to authorize electronic/physical access. If it was the intention of the SDT that a signed list of authorizers is required, then please make this a specific requirement – either in CIP-004-5 or CIP-003-5. Parts 6.1, 6.2, and 6.3 state that “access permissions shall be the minimum necessary…” We feel this to be an aspirational statement that entities will be hard-pressed to prove at audit time. Recommend this sentence be moved to the Rationale or Guidelines section. Part 6.3

should include a cross-reference to CIP-011-1-R1.2, as in "…as documented in the entities information protection access control procedures in CIP-011-1-R1.2." Parts 6.1, 6.2, and 6.3 include the qualifier "…except for CIP Exceptional Circumstances". For consistency, we feel this language should either be stricken, or amended to include a reference back to the entities CIP Exceptional Circumstances policy per CIP-003-5-R2. Please clarify whether Part 6.5 applies to cyber access or physical access, or both. The notion of "groups" can theoretically apply to physical access control systems as well as cyber. Part 6.6 appears to be redundant to the annual information protection review performed per CIP-011-1-R1.3. Per earlier comment, the "minimum necessary" language throughout R6 will be difficult for entities to prove to an auditor and should be moved to the Rationale or Guidelines section.
No
We appreciate how the SDT tried to give treatment to the "immediate revocation" requirement of the FERC order in Part 7.1. However, we feel the current language is too open for interpretation. Even with the footnote qualification, an auditor could still interpret "at the time" to mean literally "to the minute". Complicating matters is the fact that there is often no way to measure specifically when a person resigned or is terminated. Our suggestion for Part 7.1 is to restate as: "Develop and implement a program to revoke an individual's unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination". This way, the entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that entities use shared accounts for remote access. Suggest adding "...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1".
No
In the Guidelines section of CIP-004-5, the last sentence under Requirements R3 (and again under R4) states "…by the single senior management official identified in Requirement R1". This should be re-written to say "…by the CIP Senior Manager or delegate identified in CIP-003-5-R1". In the Requirement R4 section of the Guidelines the reference to CIP-011 is a typo and should state CIP-004 instead. In the Requirement R6 section of the Guidelines, the last sentence of the first paragraph should be modified to state "Best practice recommends that access authorization and provisioning should not be performed by the same individual". Some entities are too small for strict separation of duties to be feasible.
No
How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please revise the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Please provide a technical basis for the requirement that outbound access permissions are necessary per Part 1.3. If no technical basis can be defined that can be uniformly applicable to all BES entities, then please qualify "outbound" to be "…inbound and, where implemented by the entity, outbound access permissions". In Part 1.5, the term "malicious communications" is too vague. Recommend changing 1.5 to say "A documented method for malicious traffic inspection at each EAP". The Guidelines section provides good information and a technical basis for R1, and the SDT should be complimented on their well-reasoned analysis, but we have concerns about Guidelines and Technical Basis language being included within the Standards themselves. The third paragraph, for example, states "This requirement applies only to communications for which 'deny by default' type requirements can by universally applied…". This sort of language, while useful, should more properly be included in the requirements. The SDT should make very (very) clear the intent of the Guidelines and Technical Basis section of the standards, and the expectations of the entity - and of the compliance enforcement authority – on how this information should be used.
No
We recommend that "where technically feasible" qualifiers be added to Parts 2.1, 2.2, and 2.3.
Yes
No
How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please revise the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Retention requirements for Part 1.6 are not made clear. Perhaps it was intentionally left

undefined by the SDT? If this is true, should the entity therefore assume they will need to retain three years of Logs per the Evidence Retention portion of the standard?
No
Retention requirements for Part 2.2 are not made clear. Perhaps it was intentionally left undefined by the SDT? If this is true, should the entity therefore assume they will need to retain three years of Logs per the Evidence Retention portion of the standard?
Yes
Yes
No
For Part 1.1, SDT should acknowledge the use of dynamic ports/ranges used by a wide variety of cyber systems. The documentation requirement seems a bit redundant to the configuration management documentation requirements of CIP-010-1-R1.1.
No
For Part 2.1, suggest the language be rewritten as “Identify and implement a process to monitor for the release of security patches…” As it’s currently written, “identifying sources” might be interpreted as writing down a bunch of third-party URL’s that may change without warning. Recommend revising Part 2.2 to say “Identify applicable security-related patches or security-related updates…” As written, a person could interpret “updates” to mean security-related or not. The words “…that addresses the vulnerabilities within a defined timeframe” should be separated from the end of the sentence and rewritten as its own sentence for clarity. Part 2.3 is not clear on what is actually required. The requirement talks about a process, yet the Measures suggest evidence that the remediation took place. Should Part 2.3 say “Execute the remediation plan documented in Part 2.2”?
No
For Part 3.5, need to add “where technically feasible” qualifier here. If we serial-connect a laptop into a router or a relay, the device may not be capable of detecting and logging that connection. The Change Rationale for Parts 3.4 and 3.5 mention the term “ESP”. Beyond just that typo, the definition of Transient Cyber Asset implies that this requirement only applies when such devices are directly connected to other BES Cyber Assets, not the “ESP” itself. In the Guidelines section under Requirement R3, the second paragraph states “…the entity must specify how those updates are tested”. Yet, there is no specific requirement for malware signature testing in R3 of the standard.
No
Parts 4.1, 4.2, and 4.3 are concerning in that no accommodation for “where technically feasible” is mentioned. Yet, the last paragraph on Page 41 – the Guidelines section – states that the SDT does not intend for TFE’s to be required. Does the Guidelines section carry any weight when an entity is being held to the letter of the standard? Or are the Guidelines to be read as part of the Standard? For Part 4.4, please clarify the contradictory requirements for 90-day log retention versus the three-year evidence retention specified in Part C Section 1.2 of the Standard (page 32). The Measures for Part 4.4 are a good start, but “records of disposition” is too vague.
No
This is a bit nit-picky, but Part 5.1 could be wrongly interpreted as “Show me your driver’s license before I provision an account for you on the BES Cyber System”. Recommend using language similar to CIP-006-5-R1.2 “Utilize at least one electronic access control that restricts access to only those individuals that are authorized”. Part 5.2 implies, but does not state, that a signed and approved list of delegates is required. Please clarify. Also, this requirement talks about the “use of” shared accounts. This could be interpreted as either the initial creation of, or day to day use of, those ID’s. We believe the SDT meant the former, but we request that you please clarify. Parts 5.2 and 5.3 imply, but do not explicitly state, that there must be a procedure to authorize individuals having access to shared/administrative accounts. Please clarify. For Part 5.4, please simplify by stating “Procedural controls for initially changing default passwords, where technically feasible”. All the rest can be stricken, and the asset types moved to the Applicability column.
Yes

No
For Part 1.2, need to have a cross-reference to the applicable EOP standard and requirement.
No
Part 2.1 the words "…when incidents occur" is redundant. The requirement is a bit contradictory in that the incident response plans MUST be used, yet deviations allowed. (emphasis mine). Recommend rewording this requirement to say "When a suspected BES Cyber Security Incident occurs, the incident response plans shall be executed. Should deviations from the plan be necessary, those shall be documented for later review". Part 2.2 should state simply "Test the BES Cyber Security Incident Response Plan at least once every calendar year", and include the three bullets.
No
The Change Description field mentions "DHS Controls". What are these? Also, due to the complexity of the testing and review of the BES Cyber Security incident response plans, recommend including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan.
Yes
No
General question about the scope of CIP-009 that has never been addressed – is the intent of the standard the recovery of the function of an asset or system, or the recovery of the actual asset itself? This would be a good opportunity to clarify. For Part 1.4, what does "verified initially" mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets.
No
Part 2.1 should state simply "Test the Recovery Plans at least once every calendar year", and include the three bullets. It also needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Need to also allow for the fact that not all cyber assets can be "backed up" in a traditional IT sense. For Part 2.3, it was commented earlier, but an operational exercise "initially upon the effective date of the standard" will make for an exciting day on the North American bulk power system. Please remove all instances of such language from all the standards, and make this part of the implementation plan and allow for staggered and entity defined rollouts.
Yes
Yes
No
For Part 1.1.4, the word "scripts" is too generic and thereby problematic. Scripts that are used for key functionality of the system would make sense to include in the baseline, but scripts for administration, backups, maintenance or troubleshooting, for instance, may be too dynamic by nature to be included in the baseline. Please either clarify, or strike, the words "and scripts". For Parts 1.1 and 1.2 there is a potential problem with dynamic port ranges. Perhaps sub-Part 1.1.5 could be written as "Any static logical network accessible ports". Part 1.2 seems to imply that the CIP Senior Manager must approve a list of delegates who have the authority to authorize changes. If this was the intent, please add a specific requirement.
No
Requirement R2 needs a lot of work and justification. Perhaps unintentionally, this requirement as written will result in another massive filing of TFE's, since I can't install Tripwire on my Router. While the purpose of the requirement is well-intentioned, with good reference to best practices, the application doesn't work outside traditional IT server-based cyber assets. This is a net-new requirement within CIP that, if retained, will require major initial and ongoing investment by entities for little reliability benefit. We recommend striking R2, or vastly limiting its scope (Server-type assets at Control Centers, for instance).
No

For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where “test” systems just aren’t economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. For Part 3.3, please clarify whether “new Cyber Asset” means literally that or, more reasonably, could mean “new Cyber Asset category” or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn’t make sense.
Yes
Yes
No
For Part 2.1, please add language that allows for re-use or redeployment within a similar BES Cyber System.
Yes
No
The SDT should modify the Implementation plan to identify requirements that are net-new (like CIP-010-1-R2) and might require capital investment, and provide an additional 12 months to implement. The justification being the reality of capital/budgeting cycles within an organization. Depending on the timing of the regulatory approval, it may be twelve months before capital can be obtained, thus leaving three calendar quarters to design, test, and implement these technologies to meet the “seven calendar quarters” implementation date. Secondly, every instance in the standards where “initially upon the effective date of the standard” is written needs to be removed from the standard and added to the Implementation Plan. For each of those specific requirements, a staggered table should be developed that allows entities the flexibility to perform their first iterations of cyclical events in a phased manner.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
We are concerned with the exclusion of the “Intermediate Device” from the definition of “Interactive Remote Access”. As specified in the definition of “Intermediate Device”, this “Intermediate Device” can be located outside the ESP, and by excluding the this device from the interactive remote access rules defined in CIP-005-5, part 2.1 through 2.3, we feel that this may be a weakness that may opens up the danger of opening up potential, unprotected path to BES Cyber Assets.
Yes
1. IROLs may be based on dynamic system phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response. We suggest an additional criterion that captures this important impact: ‘Generation Facilities at a single station that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies’ 2. Currently our risk-based methodology includes a criterion to protect transmission stations that act as data hubs critical for monitoring and control of the BES. There appears to be no criterion in CIP-002-5 that recognizes this critical role. We suggest an additional criterion (similar to CIP-002-3 R1.2.7) in the Medium category to capture these self-identified impacts: ‘Any additional facilities that support BES Reliability Operating Services that the Responsible Entity deems appropriate.’
Yes
Yes

Yes
Yes
We are agreeing with this proposal; however, we feel that defining NERC senior manager to a role rather than to an individual may be more practical, especially when personnel changes are more frequent.
Yes
We agree that organizations shall have security policies to cover all of those elements described from 1.1 to 1.10 under R2 of this standard. However, we want clarification on the term “policy” that does not necessarily have to be represented or tied up with a “policy” documents, but should also includes other type of governing documents, such as “security standard” type of enforcement document that an organization already accustomed to.
Yes
Yes
Yes
Yes
Yes
We agree to all VRFs, except for the “medium” VRF proposal for R2. We suggest this should be a “high” VRF, because the security policy is the main driver from and the means from top level authority of the organization to enforce overall security and without one the overall security posture will not follow through, including the NERC standard requirements outlined.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Part 2.2 specifies that “Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session”. We feel that for clarity, the encryption termination point must be specified with this rule. We suggest the following language for the rule: “Require encryption for all Interactive Remote Access sessions, terminated at the intermediary device, to protect the confidentiality and integrity of each Interactive Remote Access session”.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
"Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1." This could require TFEs in a very ad-hoq manner. For example if data could not be preserved due to the nature of the technical damage (level or nature of coruption) of the media, this requirement would force the entity to file for a TFE because it was not techincally feasable to preserve the data. We suggest that this would not be a practical or effective use of TFEs. We suggest that the wording "where technically feasible" be replaced with "to the extent possible". We believe this would allow for situations where it is not possible to preserve the data without having to invoke a TFE for every instance that this occurs.
Yes
R2.3 states in part: "Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard,". We suggest that this would be impossible to test each plan on the recovery date. We suggest that the wording be revised: "Test each of the recovery plans referenced in Requirement R1, initially within 12 calendar months of the effective date of the standard,"
Yes
Yes
Yes
Yes

We suggest that the wording of “technically feasible” should not be included in R2, part 2.1 as this term is contradicting with R1, part 1.1 as the baseline configuration should already been created as required by this requirement.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Rodney Luck
Los Angeles Department of Water and Power
Yes
In Section "1. High Impact Rating (H)" of Attachment 1, the phrase in the first paragraph "within 15 minutes adversly impact..." is vague. More guidance and clarity are needed on how to determine adverse impacts.
No
R3.2 defines "annual" training as being completed within 15 months. This is a change from the NERC current definition as described in CAN-0010. Entities need more leeway in being able to define "annual" training and other "annual" requirements. It is extremely difficult to track and manage training of thousands of employees based on a 15 month time frame. Entities need to be allowed to complete training over an entire calendar year.
No
The time limits for revoking access upon terminations and transfers being proposed for the next calendar day present extreme challenges. More time needs to be given - the next calendar day for terminations and 72 hours for transfers to make these processes manageable.

No
R1.1 defines operational or procedures controls to restrict physical access to Low Impact BES Cyber Systems. Need to remove applicability of this requirement for Low Impact BES Cyber Systems. Existing Standard Operating Procedures address and restrict physical access to Low Impact BES Cyber Systems. Demonstration of existing procedures should be sufficient to meet the intent of this requirement. R1.3 requires utilization of two or more different and complementary physical access controls. This presents technical challenges and may not create additional security. One control is preferred. Depth of defense already exits through gates, security personnel and card reader systems. The current requirement of one or more physical access methods has been implemented with little or no problems encountered. The increase to two or more physical access controls may bring about unintended consequences and complexity. NERC should provide compliance feedback to the industry demonstrating that the one or more physical access methods have been ineffective. Additionally, High Impact Control Center typically emply stringent physical security controls and monitoring. In addition, the language under Measures in R1.3 describes how ingress and egress are controlled by one or more different methods. The requirement for egress has not been explicitly defined as a requirement. Preference is for ingress only. Egress requirement has been alluded to in the language stated in the Measure. Access controls for egress present a number of safety issues and concerns. R1.6 does not address access log retention. Preferenece is to maintain a log retention of ninety calendar days. A log retention of ninety calendar days maintains status status quo as far as log retention.
No
R3.1 requires maintenance and testing every 24 months. We prefer a maintenance and testing cycle to be no longer than three years. Equipment failure rates do not support the need for maintenance and testing every two years. Manufacturer Mean time before failure rates are in excess of three years. We believe maintaining the three year cycle is reasonable and effective. Additionally, equipment is monitored and malfunctions are reported immediately thus negating the need for a two year maintenance and test cycle.
No
R1.2 requires to "disable" unused physical ports. Given the age of some equipment, this may not be technically feasible and there are no provisions for exceptions. There is a designation for "signage" being acceptable. What is meant by "signage"? There needs some exception for physical ports that can not be disabled.
No
R4.5 The requirement that the time frame of documenting a response to rectify before the end of the next calendar day presents a very short time frame to come up with a way to rectify an issue that may require extended investigation. 30 days is preferred.
No
In R5.1, it is not clear if alternatives to password authentication can be used. There are many new forms of technology for validating credentials before granting electronic access such as biometrics, IRS scans, finger print scans, etc.
No
R2.3 states "test each of the recovery plans... through an operational exercise." The requirement

needs to allow for recovery plans which are representative of similar or like Applicable Cyber Assets which would achieve the same goal as individually testing each recovery plan. Excessive operational exercises when numerious recovery plans are available may potentially disrupt operations.
No
R3.3 states that prior to adding a new Cyber Asset to a BES Cyber System, the entity is to perform an active vulnerability assessment of the cyber asset. It is problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. "Active vulnerability assessment" is not defined. There are sufficient controls in place that any "active vulnerability assessment" would be unnecessary.
Individual
Jack Stamper
Public Utility District No. 1 of Clark County
Yes
The SDT should consider the following changes to the defined terms. BES Cyber System - One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. BES Cyber System Impact – Need definition. CIP Senior Manager - A single senior management official with overall authority and responsibility for leading and managing implementation of the requirements within the NERC CIP-002 – CIP-011 Standards.
Yes
The impact rating of control centers needs to be tied in with the facilities controlled by the control center. CIP-002-5 -Attachment I attempts to classify all Transmission Owner, Transmission Operator, and Generator Operator control centers as either High Impact or Medium Impact. There is a slight exception offered for Generator Operator control centers only. The SDT has for the most part adopted the Version 4 criteria; however, Version 4 was intended to identify an entity's facilities as either "critical or not critical." It is unreasonable that a control center determined to be "not critical" under Version 4 is then determined to have a Medium Impact Rating in Version 5. Yet this is exactly what criteria 2.13 will do. The SDT has attempted to lessen the harshness for generator control centers by adding a limit of 300 MW but has not provided any such "ceiling" for transmission control centers. The STD needs to be made aware that there are some Transmission Operators and Transmission Owners that operate small systems that have no practical impact on the reliability of the BES. Some of these utilities operate systems from dispatch centers that meet the definition of Control Center in CIP-002-5. Many of these entities have no real-time balancing capabilities and no frequency or voltage control (other than notifying the Balancing Authority in the event of an alarm). Also with no blackstart generation or cranking paths, system restoration consists of clearing of loads from distribution busses and then the re-establishment of load upon the restoration of the transmission system voltage by the Balancing Authority. If a utility has only electric facilities that have a Low Impact Rating, it is reasonable to expect that the center used to control these facilities would also have a Low Impact Rating. A similar argument can be made for control centers that control Medium Impact Rating electric facilities and High Impact Rating electric facilities. The SDT should further develop the criterion so that a reasonable boundary exists between the High and Medium Impact Rating and between the Medium and Low Impact Rating. Control centers should be rated based on the facilities controlled.
No
The SDT uses a number of different calendar days for reporting throughout the CIP standards. Clark recommends one consistent time of 90 calendar days.

No
The SDT uses a number of different calendar days for reporting throughout the CIP standards. Clark recommends one consistent time of 90 calendar days.

Individual
Paul Crosby
Platte River Power Authority
No
Yes
Attachment I, Criterion 2.13 – It's not clear if the term "generation control centers" is referring to: • control centers local to generation, • centralized control centers controlling multiple geographically disparate generation resources, • or both
No
Please consider revising Requirement 1 as follows: R1. Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its BES Cyber Assets and BES Cyber Systems as High or Medium Impact according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems not categorized as High or Medium Impact shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning]
Yes
Yes
Yes
Yes
No
We feel that Requirement 4 is training and should be moved to CIP-004-5 Requirement 3.
Yes
Yes
Yes
No
We feel that the term "security controls" in R2, Part 2.2 is broad and overlaps with R2, Part 2.4 "electronic access controls". We suggest either combining Part 2.2 and 2.4 or separating them into specific types of access controls, such as: • Electronic access controls • Physical access controls • Remote electronic access controls • Etc.
No
Since R3, Part 3.1 and 3.2 both reference and are related to R2 we suggest combining Requirements 3 and 2. The way they're written it's odd that the role-based program does not address completing training prior to access authorization nor requiring training updates once a year.
No
As written the Requirements don't require that the personnel risk assessment include a seven year criminal history check. The Measures do but not the Requirement. Should it?
No
As written the Requirements don't require that the personnel risk assessment include a seven year criminal history check. The Measures do but not the Requirement. Should it? R5 references and relates to R4 we suggest combining Requirements 4 and 5. The way they're written it's odd that the personnel risk assessment (PRA) program does not address completing the PRA prior to access

authorization nor requiring updates every seven years.
Yes
Yes
No
Part 1.2 states “Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs)”. The Measures for 1.2 do not address the demonstration of “control and secure”, only the identification of EAPs. Perhaps 1.2 should only address the use and identification of EAPs while Parts 1.3 addresses “control and secure”. Additionally, the requirement doesn’t specifically require the protection of a BES Cyber System. “Control and secure all routable and dial-up connectivity” to…? We suggest revising the language for Part 1.1 as followings, “Identify Electronic Access Points (EAPs) used to control and secure all routable and dial-up connectivity to applicable BES Cyber Systems.” Part 1.3, the term “access permissions” is unclear. We suggest revising the term to match the language in Part 1.2 using “access controls” instead. Part 1.4 still uses the term “where technically feasible.” We were under the impression that the drafting team was going to do away with TFEs.
No
CIP-005-2 Table R2 is labeled “Remote Access Management”. All the Parts contained within deal specifically with “interactive” access. We suggest renaming the table to “Remote Interactive Access Management”.
No
Part 1.4 states “Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary.” We don’t believe it’s possible to issue real-time alerts for successful but unauthorized physical access. The system cannot distinguish between an unauthorized person using valid credentials and an authorized person using valid credentials. We suggest revising the requirement as follows, “Issue real-time alerts (to individuals responsible for response) in response to failed physical access attempts at any access point in a Defined Physical Boundary or to physical access control system alarms. Part 1.5 - Please see previous comment.
Yes
Yes
No
Part 1.1 – We are assuming this applies to the Asset level although it’s not clear. The applicability is defined per “BES Cyber System”, “Access Control System”, or “Associated Protected Cyber Asset”. We suggest revising as follows: “Disable or restrict access to unnecessary BES Cyber Asset logical network accessible ports and document the need for any remaining logical network accessible ports.”
No
Part 2.2 – The requirement isn’t written clearly. We suggest revising as follows “Assess security-related patches or updates for applicability within 30 days of release from the identified source and create a remediation plan, or revise an existing remediation plan that addresses the vulnerabilities within a defined timeframe.”
No
Part 3.1 & 3.4 – We feel the word “or” makes the Requirement unclear. Are we to deter or detect or prevent malicious code? Or are we to deploy method to do all or a combination of the three. We suggest replacing “or” with “and” or “and/or”.
No
Part 4.1.4 states “Any detected potential malicious activity.” Is this code for “all activity”? Isn’t all

activity “potentially” malicious? We suggest removing the word “potential” from 4.1.4.
No
Part 5.1 – It’s unclear in the requirement whose credentials require validation. We suggest rewording as follows, “Validate user credentials before granting electronic access to each BES Cyber System. “ Part 5.2 and 5.3 deal with access authorization and identification. We suggest moving them to CIP-004-5 R6. Part 5.5.3 – Changing passwords based on an “entity-specified time frame” may lead to questions around time frame adequacy. We suggest specifying a minimum time frame and allowing the entity to shorten as needed. For example use “Change annually or more often as needed”.
Yes
No
Part 2.1 – Please consider revising as follows, “The incident response plans must be used when BES Cyber Security incidents occur and include recording of deviations taken from the plan during the incident or test.
Yes
Yes
No
Part 2.2 – We feel the phrase “reflects current configurations” is unrelated to testing if the information is usable. We think the test is valid and should be moved to Part 2.3.
Yes
Yes
Yes
No
Part 3.1 – We feel the reference to “security controls” is unclear. We ask that the drafting team list the minimum set of Requirements that require assessment.
Yes
Yes
Yes
Individual
Nathan Smith
Southern California Edison
Yes
-BES Cyber Security Incident An attempt to compromise an electronic access control system is not included in this definition and should be. -BES Cyber System Maintenance Cyber Asset should be rephrased to say Transient Cyber Asset. Also, as it is currently worded, the means by which the clustering of BES Cyber Assets into BES Cyber Systems is to be done is not clear. -BES Cyber System Information The definition does not address information artifacts where BES Cyber Systems or BES Cyber Assets are depicted but not marked as such. For instance a substation network diagram

showing relays not specially marked as BES CA or BES CS could be classified as not being a BES Cyber System Information artifact since an uninformed user of that information would not be able to distinguish them as such. -BES Reliability Operating Services The term is too broadly defined. There are many systems involved in distribution that would not degrade the BES if they malfunctioned, but none the less are programed to respond to changes on the BES. The suggested improvement is to specifically note that distribution assets are not in scope. -Should all of the BES services be in scope? Order 706 did not order controls on all BES services. -Control Center There is no verbiage to clarify geographically dispersed centers. -Electronic Access point ("EAP") Based on how this term is defined a Level 2 switch is not considered an access point. An EAP should be defined such that it is required only for devices that are accessible by dial-up or routable channels. -Cyber Systems Please provide a definition for Cyber Systems -Defined Physical Boundary This concept is an improvement over the current 'Physical Security Perimeter', is expected to increase security of the BES, and provides more flexibility for compliance. -Electronic Security Perimeter ("ESP") The definition should state that ESPs are valid only for dial up accessible or routable access points. For instance a fully serial HMI cannot be provided with an ESP because there is no access point other than the device itself. -Intermediate Device Does the word "and" just before (3) imply that an intermediate device has to meet all three of the noted criteria? -Reportable BES Cyber Security Incident Please clarify what the term "compromised" could mean, or elaborate on what a "compromised" system looks like. -Reportable BES Cyber Security Incident The compromise of an ESP without an appreciable loss in BES Reliability Operating Services capability would not be reportable based on this definition. It is not in line with the requirements of Order 706. For further suggestions regarding Definitions see comments provided by EEI

Yes

SCE provides these specifc comments for the SDT's consideration. For further suggestions regarding CIP 002 see comments provided by EEI. Attachment I Paragraph 2.5 Please clarify the requirements for the Cranking Path. The third graph on page 26 of 30 seems incorrect. Paragraph 2.12 What is the phrase "without human intervention" mean? The subject of the paragraph is automated load shedding. Could the intent of the paragraph be to identify automated load shedding systems that start load shedding without human intervention or could the intent of the paragraph be to identify automated load shedding systems to continue to shed load once initiated by a human? This requirement assumes that the entity already knows which Cyber assets are BES Cyber assets / BES Cyber systems and which are not based on the impact categorization prior to the application of the methodology. There is no requirement that entities first collect a candidate list that is then subject to the criteria listed in CIP 002. High Impact – A data acquisition node or protection relay that is essential to for monitoring or control functions performed by an EMS which are located at a BES facility that is not a control center would result in the BES facility housing such a node or relay being classified as a control center. Suggest including this sentence: A data acquisition node or protection relay that is essential for monitoring or control functions performed by an EMS which are located at a BES facility that is not a control center do not result in the BES facility housing such a node or relay being classified as a control center.

No

002-R1 Suggest adding this sentence to the end of R1: Justification of Low Impact BES Cyber Assets is not required. If a Low Impact BES Cyber Asset is not identified discretely is there a need to justify why it is not considered a High or Medium Impact BES Cyber Asset? R1.1 uses the word "intended to be in service". This does not account for scenarios where a system or facility is not intended to be in service for more than 6 months but due to planned or unplanned outage days, the total period where the system or facility is connected is greater than 6 months (although it was not actually in service for the entire period). For instance a pilot project that is intended for a 6 month test period is removed from service for 30 days for modifications, and the pilot project is run for 7 months to "make up" for the lost 30 days of testing would be considered in scope per this requirement.

No

002 R2 "Upon the effective date" should be restated to read "on or (within 30 days) prior to. A list of Low impact BES facilities is not required to be maintained, however, certain standards require controls to be enforced at these facilities. At the very minimum, the standard should require that the RE's approval of High and Medium lists should include a list of facilities and systems considered as potential candidates for the evaluation.

No

For suggestions regarding CIP 002-5 Violation Risk Factors and Violation Severity Levels see comments provided by EEI.
Yes
For suggestions regarding CIP 003 R1 see comments provided by EEI
Yes
For suggestions regarding CIP 003 R2 see comments provided by EEI
Yes
For suggestions regarding CIP 003 R3 see comments provided by EEI
Yes
CIP 003-5 R4 What does it mean for employees and contractors to “have access to BES Cyber Systems”? Is the intent here to indicate the employee or contractor has control over the asset? Suggest revising the sentence to say “Each responsible entity shall make individuals with control over BES Cyber Systems aware of elements…”
Yes
For suggestions regarding CIP 003-5 R5 see comments provided by EEI
Yes
For suggestions regarding CIP 003-5 R6 see comments provided by EEI.
Yes
For suggestions regarding CIP 003-5 Violation Risk Factors and Violation Severity Levels see comments provided by EEI.
No
For further suggestions regarding CIP-004-5 R1 see comments provided by EEI
No
For further suggestions regarding CIP-004-5 R2 see comments provided by EEI
No
For further suggestions regarding CIP-004-5 R3 see comments provided by EEI
No
SCE provides these specifc comments for the SDT’s consideration. For further suggestions regarding CIP 004-5 see comments provided by EEI R4.1 – Suggest current PRA’s already in place be grandfathered, such that those with a PRA need not meet the new requirements for the PRA until the initial one expires. R4.2 – Suggest providing flexibility not to cover the full scope of the PRA for those that are in states that impose limits on how much personal information can be assessed. Retention of records of 7 year background checks is not clearly stated. Also there is no consideration of existing background checks under NERC CIP standards that are currently in effect. Can a PRA under the current CIP requirements be used to validate R4.2 under Version 5? R4.3 The application guideline provides guidance where it is ‘not possible to perform a full seven year criminal history check.’ How is ‘not possible’ measured? Propose a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain.
No
For suggestions regarding CIP-004-5 R5 see comments provided by EEI
No
CIP 004-5 R6 Propose use of ‘legacy’ language where access is appropriate for the roles and responsibility over ‘minimum necessary’
No
CIP-004-5 R7 R7.1. Suggest requiring access be revoked within 24 hours, or “as soon as possible”. “At the time of termination or resignation” is vague and difficult to define. R7.5. Some Medium Impact assets that are programmable and have shared passwords are deployed in the field and have no network connectivity. Given these assets are distributed in a wide geographical area, many in difficult to reach places, it is not technically feasible to get to all the distributed assets and change their passwords within 30 calendar days; especially assets that are in or near hydro facilitates. Suggest modifying the standard to exclude medium impact assets in the Applicability section. R7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would

introduce a challenge with revocation 'at the time of' events. R7.3 – Propose use of 'approved BES Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled. Access revocation to protected information repositories is enforceable but revocation to hardcopies is difficult to prove. A control that acknowledges the difficulty of proving that access to hardcopies (Especially those in the possession of the person, not just those documents that are located in a locked cabinet or other storage areas) has been revoked should be added. A sign off form is an acceptable measure but not within the timeframe suggested. An outside limit of what is considered "at time of" should be provided. Language such as "access revocation should be completed within 24 hours" can be used.
No
Violation Risk Factors and Violation Severity Levels for CIP-004-5 Across all VSLs there is no consideration for the impact level of a particular violation. The Lower and Moderate VSL's should be made applicable to Medium Impact BES Cyber systems and their associated Cyber assets. For instance if a role is such that access is provisioned only to associated cyber assets and not to High or Medium or those assets deployed for protection, the violation should be a Lower or Medium VSL. R1, R2, R6 – Scale VSLs appropriately. R3, R7 - <1% of individuals for Medium Impact and associated cyber assets should be Lower VSL, 1-5% for Medium Impact and associated cyber assets should be moderate, 5-10% of any applicable BES cyber asset should be high, and any number greater than 10% of any applicable BES Cyber asset can be treated as severe.
Yes
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 005-5 see comments provided by EEI R1.1 Should the measures read "documented technical or procedural controls that exist…" in order to match the requirement? Please confirm the Low Impact assets do not have to be protected by an Electronic Access Point? R1.3 Although security wise this requirement adds protections, explicit outbound access permissions places a load on processors that slows down the computing capability, and therefore may make the grid operate slower. Please be aware of the trade-offs. R1.5 This requirement is dictating the need for an intrusion detection system at all High Impact and Medium Impact Electronic Access Points (with external routable connectivity at control centers). This is a high cost investment for industry to make in a short period of time,, and may not be accomplishable for field deployed programmable assets. Are the measures aligned with the requirement here, since the Requirement requires a method but the measures point to a system or systems? Please define "malicious communications"
Yes
For suggestions regarding CIP-005-5 R2 see comments provided by EEI
Yes
Violation Risk Factors and Violation Severity Levels for CIP-005-5 R1 – R1.1 A procedural or technical control for a low impact system should be scaled in and not bundled with violations for high of medium impact systems. Proposed change could state that a violation of R1.1 for <5% of low impact is moderate, greater than 5% is High and not a severe VSL for Low impact.
Yes
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 006 see comments provided by EEI R1.1 Suggest stating whether or not there is a requirement to implement the operational or procedural controls. R1.4. Suggest clarifying that issuing real time alerts for events at Medium Impact assets does not include pole top devices.
Yes
For further suggestions regarding CIP-006-5 R2 see comments provided by EEI
Yes
For suggestions regarding CIP 006 -5 R3 see comments provided by EEI
Yes
For further suggestions regarding CIP 006 Violation Risk Factors and Violation Severity Levels see comments provided by EEI
No
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding CIP 007 see comments provided by EEI R1.1 Suggest revising the requirement to provide an

exception related to dynamic ports and the inability to disable them. If a dynamic port is closed, the service that is needed by the BES system may not be available. Furthermore, it is not always known which ports and services vendors are using. R1.2 Restricting the use of physical USB ports may not be accomplishable. There are so many devices with physical ports it is impossible to monitor each one. In addition, because a USB port is in use by a mouse, and therefore not required to have access restricted to it, someone could easily remove the mouse from the USB port and install malicious software. This requirement creates a huge burden and is easily circumvented.
No
CIP 007-5 R2.1 Suggest revising the standard to say “security updates”, not just “updates”. R2.2 Suggest revising the requirement to allow for 30 days to identify applicable security updates or patches and 30 days to draft a remediation plan. R2.3 This requirement is not clear and does not match the measures. Please revise it. A TFE option for unsupported devices should be added. Also the standard does not specify a timeline within which a remediation should be completed or a scheduled review of the status of the remediation plan.
No
CIP 007-5 R3.2 Suggest revising the requirement to include quarantine of the malicious code. R3.4 Should this standard be applicable to Transient Cyber Assists? If so it should stated in the “Applicability Column” R3.1 and R3.2 Should allow for applicability at the system level or on a per asset level. Whitelisting of applications could be stated as a requirement rather than a measure. The requirement thus stated would add to the robustness of documenting BES Cyber Systems since the hardware of a “cyber system” cannot conceivably perform any functions without some onboard software. The standard language as currently stated seems to apply to the hardware and deviates from Order 706.
No
CIP 007-5 R4.1.4 Please define “Malicious Activity” R4.5 Reviewing logged events every two weeks is burdensome and can be expensive to automate, and there is little improvement in BES security from this activity. Please consider re-thinking this requirement. A TFE option should be provided within this requirement since devices that do not support functions as listed. The language of the standard assumes automated logging for each BES Cyber Asset.
No
CIP 007-5 R5.4 Should the applicability here be noted as High Impact and Medium Impact assets?
No
CIP 007-5 R1 – Moderate or High VSL for undocumented ports on Medium Impact Cyber assets. R2 – Moderate or High VSL for failure to identify source. Failure to identify source and failure to implement should not be treated the same way.
Yes
For suggestions regarding CIP 008-5 R1 see comments provided by EEI
Yes
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 008-5 see comments provided by EEI R2.1 Suggest removing consideration of a test from the requirement.
Yes
For suggestions regarding CIP 008-5 R3 see comments provided by EEI
Yes
CIP 008-5 R2 – Failure to annually test an IR plan should be a high VSL not severe. Failure to use a IR plan and failure to test an existing IR plan should be treated differently.
Yes
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 009 see comments provided by EEI R1.1 Should the standard note what conditions should apply to the recovery plans? If so what type of conditions should be planned for? R1.3 Suggest replacing the word “protection” with the word “handling” or please explain what is intended by the word “ protection”
Yes

CIP 009-5 R2.3 Are there suppose to be specific recovery plans that need to be in place and tested?
Yes
CIP 009-5 R3.2 Suggest adding “or recovery” after “exercise” R3.3 Suggest adding “completion of” before “review”
Yes
CIP 009-5 For suggestions regarding Violation Risk Factors and Violation Severity Levels for CIP-009-5 see comments provided by EEI
No
SCE provides these specific comments for the SDT’s consideration. For further suggestions regarding CIP 010 see comments provided by EEI R1. We recommend the CIP SDT consider removing physical location from Baseline Configuration in CIP010 R1, or replace it with logical location (logical placement within the control systems architecture.) • R1.1.1 requires Physical Location be part of a Baseline Configuration. In the Guidelines and Technical Basis, Physical Location is explained as follows: The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The underlined phrase seems to imply that controls are applicable to the environment in which the cyber assets are located, whereas Controls are required by CIP004, CIP005, and CIP006, by categorization of BES Cyber System, as required in CIP020. The Applicability Section of each requirement clearly requires the categorization of assets to be protected by the controls required by CIP040, CIP050, and CIP060, and not the Environment in which the assets reside. • CIP002 R1requires Responsible Entities to identify and categorize High and Medium Impact BES cyber asset and cyber system. Asset identification includes an asset inventory, or list(s) as described in CIP002 R1 M1. Asset Identification, per NIST SP800-128 titled "Guide for Security Focused Configuration Management of information Systems", includes an asset Inventory of systems and system components in which one of the data elements may include "phyiscal location (e.g., building/room number, see Page 27 of this document)". Both CIP002 M1 and NIST SP800-128 point to an asset inventory that should be kept, and includes Physical Location where the asset resides. • CIP002 R1.1 requires "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities..." A change of physical location where the BES Elements resides would require an update to the Asset Inventory or list. If the physical location is changed such that the BES Elements and Facilities are now outside of the already established controls, these controls will need to be re-established to comply with CIP004, CIP005, and CIP006. • CIP010 1.1 Change Rationale includes the following text: The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. DHS Catalog for Control Systems Security Section 2.6.2.2 includes the following text: The baseline configuration provides information about a particular component’s makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component’s logical placement within the control system architecture. and The inventory of control system components includes information (e.g., manufacturer, type, serial number, version number, and location) that uniquely identifies each component. Section 2.6.2.2 makes a distinction between a Baseline Configuration and an (Asset) Inventory of control systems components, and location is part of the inventory. Given this distinction in DHS Catalog for Control Systems, location (physical) should not be required to be part of a baseline configuration in CIP010. R1.1 Developing a baseline configuration is a huge task and should probably only apply to High Impact assets. R1.2 Please re-word the requirement – the meaning is not clear.
No
CIP 010-1 R2.1 Detecting unauthorized changes is burdensome. If the process is automated then that puts another load on processors and slows down computing. Please consider re-thinking this requirement only making it applicable to High Impact assets, and exclude serial devices.
No
For suggestions regarding CIP 010-1 R3 see comments provided by EEI
No
For suggestions regarding CIP 010-1 Violation Risk Factors and Violation Severity Levels see comments provided by EEI

Yes
For further suggestions regarding CIP 011-1 R1 see comments provided by EEI
Yes
For further suggestions regarding CIP 011-1 R2 see comments provided by EEI
Yes
For further suggestions regarding CIP 011-1 Violation Risk Factors and Violation Severity Levels see comments provided by EEI
No
SCE provides these specific comments for the SDT's consideration. For further suggestions regarding Implementation Plan see comments provided by EEI Schedule should be revised from 18 months to 24 months given the breadth of the increase in scope under version 5.
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
Yes
BES Cyber System Information Define "BES Cyber System Impact" as it is a capitalized term used in this definition and it is not currently defined. CIP Senior Manager Replace: "NERC CIP Standards" with "NERC CIP-002 – CIP-011 Standards." The CIP-001 Reliability Standard is not part of this set of standards and has not yet been approved for inclusion in EOP-004-2. This will give clarity to the limit of the definition. Control Center NRECA is concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be drawn in by an overly broad definition of Control Center. In this definition the SDT uses the defined term: System Operators which from the NERC glossary is: "An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." If the SDT's intent was to limit Control Centers to buildings that house a System Operator with 24/7 staffing and include BA, TOP, GOP and RC functions, then NRECA could support the definition (if other changes in our comments related to CIP-002-5 Appendix 1 are also satisfactorily addressed) and requests that the SDT make this limitation clear in the definition. If this is not the intent of the SDT then NRECA does not support the proposed definition of Control Center.
Yes
3. Purpose NRECA requests the SDT to use consistent language in this section. On line 2 the phrase "reliable operation of the BES" is used and on line 5 the phrase "reliability of the BES" is used. The same phrase should be used in both locations. 4. Applicability 4.1.2 Distribution Provider 4.1.6 Load-Serving Entity NRECA is concerned with the new inclusion of DPs in the version 5 standards and with the qualifiers proposed for LSE in the Applicability section. NRECA believes that inclusion of this broad group of DP entities will draw in many small entities with no BES operational capabilities or responsibilities and cause them to go through a paperwork drill of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. NRECA recommends that the SDT develop a simple method for DPs and LSEs to prove "No Impact" and be clearly exempt from CIP-002-5 – CIP-011-5. Attachment 1 1. High Impact Rating On line 2 the word "adversely" is used. This term can mean many things to many parties. Please provide additional clarity so that auditors and responsible entities have a better understanding of its use. 1.2 Add the following text to the end of the current 1.2: "for generation equal or greater than an aggregate of 1500 MW in a single Interconnection." NRECA strongly recommends the SDT to make this revision in order to stay as close to the CIP-002-4 criteria and to minimize cost impacts on entities that do not have a significant impact on the BES. 1.3 NRECA strongly opposes including "Transmission Owner" in this provision. Inclusion of RC, BA and TOP are appropriate, but the TO function does not rise to this same level of responsibility. NRECA requests that the TO function be removed from this section. Including the TO function here will make it very difficult for NRECA to change its vote to "affirmative" in the next ballot. If this is not changed for the next ballot, NRECA will likely recommend that its members vote "negative" on CIP-002-5. 2. Medium Impact Rating On line 2 the word "adversely" is used. This term can mean many things to many parties. Please provide additional clarity so that auditors and responsible entities have a better understanding of its use. 2.13 NRECA recommends that the proposed 2.13 language be deleted and replaced with the following: "TOP and GOP Control Centers not included in High Impact Rating and controlling 1500 MW or greater

of load or generation." Making this change will appropriately assign these control centers to the "medium" level and others not captured in the "high" or "medium" levels will be captured in the "low" level. Add new 2.14 Add: "2.14. Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers." Making this change will ensure that other appropriate Control centers will be categorized in either the Medium or Low level.
No
R1 Replace "30 calendar days" with "90 calendar days." The SDT uses a number of different calendar days for reporting throughout the CIP standards. NRECA recommends one consistent time of 90 calendar days.
No
R6 NRECA recommends changing "30 calendar days" to "90 calendar days" to be consistent throughout the CIP standards.
No
R4 On line 2 after "unescorted physical access" add "to BES Cyber Systems" to clarify what this requirement applies to. R4.2 Clarity is needed to understand if the phrase "six months or more" applies to the entire sentence or just to "attended school."
No
R5.2 The phrase "once every seven calendar years" may create confusion on exactly what it means. In order to minimize such confusion, please be more explicit on how often personnel risk assessments must be updated.
No
R6.4 The phrase "once each calendar quarter" could be interpreted to mean almost a 6 month time period. Please provide further clarification on what the phrase means so all parties understand its meaning. In addition, please provide clarification in this requirement on what the difference is between "provisioned" and "authorized."
No
R7.1 Footnote 2 does not help to clarify what "at the time" means. Please provide more explicit language in this requirement regarding what "at the time" means. It may be appropriate to treat resignations and termination differently. This requirement could allow access for a resignation to continue until the individual's employment ends. For terminations this requirement could require access to be disabled at the same time the individual is notified of termination. R7.2 Replace "by the end of the next calendar day" with "within 30 days." NRECA believes that this requirement is excessive when compared to the threat of cyber attack on the system by someone being transferred or reassigned for reasons other than disciplinary action. R7.5 In the second paragraph of this requirement the word "extenuating" is used and could be interpreted in many different ways. Please provide more explicit language so that all parties have a better understanding of what is meant here.
No

R1.1 and 1.2 In R1.1 the word “restrict” is used and in R1.2 the words “control and secure” are used in such a way that for auditing purposes these words could mean many different things to different parties. Please provide additional clarity in these requirements as to the meaning of these words to minimize confusion.
No
R2.2 The way this is currently written it leaves open interpretation concerning the extent of encryption required. NRECA believes that the data encryption requirement should only pertain to the portion of the data path that is transmitted over public networks. We are afraid if you have to provide data encryption from the specific cyber device on the critical network you would create overhead that could result in communications failures, software conflicts, and unnecessary latency. NRECA requests that this be clarified as requested to avoid auditor and registered entity confusion in demonstrating compliance.
No
R1 On line 1 after the words “physical security plans” insert “for BES Cyber Systems.” R1.4 and 1.5 More clarity is needed to better understand what is meant by the phrase “Issue real-time alerts.” Real-time related to what? The time of the unauthorized access? As currently written, this requirement appears to be unrealistic. Please modify this requirement to provide clarity regarding what is necessary to comply with this requirement. R1.6 The word “sufficient” in this requirement is very subjective. Please provide greater clarity as to what is required for compliance with this requirement.
No
R1.5.1. and 1.5.2. If an entity’s model includes differences between the test environment and the production environment, would that be a violation of R1.5.1.? NRECA requests clarification that this would not be a violation.
No
R3.2 If an entity’s model includes differences between the test environment and the production environment, would that be a violation of R3.2? NRECA requests clarification that this would not be a violation.
No
R1.3 NRECA requests clarification regarding whether “deficiencies identified during the assessment” are considered violations of the standard. NRECA believes these deficiencies should not be considered violations of the standard and asks the SDT to address this.

No
Implementation Plan: On page 1 in the “Compliance with Standards” section, the applicable functions are listed. NRECA requests that this be revised to match the “Applicability” sections of the CIP V5 standards which include qualifiers to a number of the functions.
Individual
William O Thompson
NIPSCO Northern Indiana Public Service Company
Yes
-BES Cyber Asset: NIPSCO requests that further clarification is needed for the phrase “unavailable, degraded, or misused.” Clarification is also requested in the phrase, “when required” in sentence one, because it is ambiguous and confusing and as it is applied to other CIP reliability standards proposed. In addition, NIPSCO does not know if there needs to be a 15 minute test to “verify” the impact of the BES? And if so, how would an entity show compliance? Furthermore, NIPSCO recommends removal of the second and third sentence, because they do not provide any clarity to the time frame stated above. In addition, the third sentence regarding redundancy appears to conflict with the first sentence, therefore it is recommended that the fourth sentence be removed. The last sentence regarding “transient cyber asset” be removed because it is considered not appropriate as a cyber asset. [NIPSCO recommends that these CIP reliability standards should not exist.] -BES Cyber Security Incident: NIPSCO requests further clarification on what is meant by an, “intent to disrupt” and an “intent to compromise” as it is applied to an event and how to show evidence of such intent. NIPSCO recommends to use either “compromises” or “confirmed attempt to disrupt,” to replace intent to disrupt and intent to compromise. In addition, NIPSCO requests that the word, “suspicious” be removed. If the phrase “suspicious” is not changed, NIPSCO requests the removal of the third bullet point be removed and how to show compliance. NIPSCO recommends that compromise and disrupt be included in the first and second bullet items and recommends removal of the third bullet point, because as it currently is written, this sentence creates a confilict with the visitor escort event, and recommends removal of the third bullet point. -BES Cyber System: “typically”? This doesn’t seem appropriate for a standard. NIPSCO recommends that this definition be eliminated, because the BES Cyber System definition is too similar to the BES Cyber Asset and creates further confusion between what is a System or an Asset. The classification of an item as a “system” or an “asset,” is a huge problem, because each entity could make up and classify whatever they want and be exempted from all. The entities should not be deciding what is required as a system as a whole and what is required for individuals. Furthermore the CIP is inconsistent of what is a BES Cyber System and what is a BES Cyber Asset throughout the proposed reliability standards. NIPSCO requests clarification and a definition of “Maintenance cyber” and how it is applied and show to show compliance or use “transient cyber” consistently throughout the CIP reliability standards. -BES Cyber System Information: NIPSCO requests further clarification on the phrases “security procedures” and “impact designations.” In addition, NIPSCO requests clarification that the listed items not be a complete list, but a partial list that is not exhaustive. The word “similar” is vague and request removal of the phrase “similar diagrams.” Furthermore, patch levels on the system needs to be defined and should not include “data in transit” and “data at rest.” In addition, further clarification needs to be made how it is applied and how to show compliance. Based on the scope of cyber assets included in CIP Version 5, the cyber information is over burdensome to the whole system. Since significantly more devices are identified in CIP Version 5, the information associated with those devices impose more items to meet CIP standards that are overly burdensome. -Is it BES Cyber System disaster or can it be BES Cyber System or Asset disaster…? -BES Reliability Operating Services: The use of the word “All”, is not appropriate within monitoring and control. The responsibilities listed in the operating services list are already defined in the NERC Glossary definition of terms and should not be included in the CIP reliability standards. The CIP committee does not have authority to create these definitions, because it incorrectly creates definitions, when the appropriate party to create these definitions is NERC. -CIP Exceptional Circumstance: It is unclear what is a “risk of injury or death,” and should be clarified. NIPSCO recommends to add the word “imminent” risk of injury or death. The term “exceptional circumstance” is provided as a NERC defined, however, this is inconsistent with the CIP standards, which allow entities to define what an exceptional circumstance is in their own policy. The CIP

standard should define what is an “emergency condition.” NIPSCO recommends to change the phrase from a “CIP Exceptional Circumstance” to a NERC standard to be used generally. -CIP Senior Manager – no comments -Control Center – NIPSCO requests clarification what is meant by a “BES facility” and a “control facility.” In addition, the definition of “control room” needs to be defined in order for the definition of “control center” can be better understood and defined. In addition, further clarification is requested as to what is meant by “two or more BES generation facilities or transmission facilities.” -Cyber Assets: NIPSCO requests what is the definition of “programmable” electronic device and what is included in such device. In addition, it is recommended that the word “data in those devices” be removed from the description. -Defined Physical Boundary (DPB): NIPSCO requests clarification of the phrase “physical border” and discuss what is appropriate to show DPB that meets compliance. It is also recommended that the change rationale be excluded from the DPB. -Electronic Access Control or Monitoring Systems: NIPSCO requests definitions of both “electronic access control” and “monitoring system,” because both of these terms seem to be the same thing and including both would be redundant. In the alternative, further explanation is requested as to how each of the control or monitoring systems are applied. Furthermore, the reference to the defined term, “Electronic access control” in CIP-006 appears to conflict with the Electronic Security definition here. Electronic Access Point (EAP): Could an internal switch be categorized as an electronic access point if it is restricting any type of traffic? NIPSCO requests further clarification as to what devices or items fall under restricted routable or dial-up data communications, therefore it is recommended to remove the word “restricts” from the description. As it currently is written, it assumes the routable or dial-up restricts access. Furthermore, NIPSCO requests whether the term interface on a cyber asset was meant to apply to local hosts. Finally, NIPSCO recommends that the language be changed to state, “a routable communication through an ESP.” -Electronic security perimeter (ESP): NIPSCO recommends that the description should not be scoped to BES cyber systems, but should apply to BES cyber assets. Would the ESP include the trusted and untrusted EAP’s? -External Connectivity: NIPSCO recommends that the description should not be scoped to just BES cyber assets, and should remove the word “BES,” from cyber asset. -External Routable Connectivity: NIPSCO requests that the term “cyber system” be changed to a “cyber asset,” and further clarification as to what is an external routable connectivity. As the statement currently reads, it appears to be more of a recommendation instead of a standard. In addition, the definition as it stands is unclear and provides little guidance as to its purpose in the CIP reliability standards and more explanation or discussion should be made to this definition. -Interactive Remote Access : NIPSCO requests elimination of “Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.” -Intermediate Device: Based on the external routable connectivity and external connectivity definitions, would this be sufficient if outside the ESP? NIPSCO requests clarification at “termination point” and whether it is meant to also include end points, such as a work station, and how and where it applies and how to show compliance. In addition, NIPSCO requests elimination of “Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more cyber assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” -Physical Access Control System: NIPSCO requests further review of the description and recommends that the description should include a defined list of what is included in the defined physical boundary. -Protected Cyber Asset: No comment -Reportable BES Cyber Security Incident: No comment -Transient Cyber Asset: Is this 30 days consecutively or collective, need clarification. -Define directly connected (Is this meant to answer the roaming laptop scenario?) NIPSCO requests that the term “maintenance” be defined and explained. NIPSCO recommends to remove the phrase, “or introducing malicious code,” and change “cyber system” to “cyber assets.” It is also recommended to add, “Assets used in vulnerability assessment.” NIPSCO also requests clarification whether removable media is included as a transient cyber asset.

Yes

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -How does an entity show that a System or Asset falls or does not fall with the 15 minute window? Would one need to show results that support that the asset/system can be down longer with no adverse effects to the BES? NIPSCO recommends that the CIP cyber assets clarify whether Attachment 1 applies to any BES that affects the BES or whether only a high risk or something that would critically affect the BES and classifies something as “high impact.” In addition, further clarification is requested whether Attachment 1 applies to high risk physical assets or high risk cyber assets. NIPSCO will have a better understanding of its position once the actual rules are

created.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -“Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” What does that mean? R1 does not require discrete identification of Low Impact. Does this mean an entity does require a list of the low impact assets/systems? -In 1.1 define BES Elements and Facilities. NIPSCO states that generally that the CIP reliability standards should be made up of requirements and measures and should not be inclusive of application guidelines, rationale, and technical background.
No
Comments: -Should it not read delegate(s) instead of just delegate? There could be more than one delegate. -The measure makes no mention of the delegate(s) approval? Need consistency between the Requirement and the measure. -1.2 Evidence Retention: Please explain what “Other evidence” would be required.
No
Comments: NIPSCO recommends that the high VRFs and VSLs are extreme and the definition of what is high, medium, or low violations are unclear and need to be clearly defined in order to show how entities can fully comply. -No mention of BES Cyber Systems throughout the VRF/VSL, only mentions BES Cyber Assets. -R2: There is no mention of the delegate(s) completing the annual review. Delegate is called out in the requirement.
No
Comments: NIPSCO states that generally that the CIP reliability standards should be made up of requirements and measures and should not be inclusive of application guidelines, rationale, and technical background.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -The requirement states one may delegate by position, yet the measures make no reference to position as being the only thing being listed. Does the documentation need to be updated when personnel change but the title/position doesn’t?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Under the purpose, should it read, “...physical access to BES Cyber Assets OR BES Cyber Systems”, instead of “and”? -Rationale states all personnel, yet in the table R1.1 has applicability to “All Responsible Entities”.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Should this requirement include Cyber Assets as well as Cyber Systems?
No

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Upon reading requirement 3.1 in the table, does it imply that all personnel who access the systems during a CIP Exceptional Circumstance require training after the fact? When reading the measures it appears that that is the case.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -With modifications to this standard, do current personnel with access have to undergo another background check, or will they be grandfathered in? -How are you going to audit to ensure it includes all the residency requirements? It will be difficult to be 100% sure of a “full seven year criminal check”. In addition, many schools are online now and how does an entity determine location from those? -Setting a hard line of when employee’s “fail” a PRA is difficult, as it may determine on what role the individual is performing. It might even be more difficult to have “fails” defined for each role within the organization. Could the registered entity have criteria that include HR using judgmental decision making? -Part 4.2 Requirements will need to negotiate with applicable unions and labor agreements.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - 6.2, measure (i) introduces “sampling”, where is this defined and what would be acceptable “sampling”? -6.3 also includes the word “sampling”. -6.4 may be overly onerous on entities. Is a list of the exceptions sufficient to meet the measurement?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Provide more definition/clarification of “at the time of the resignation or termination” and what is the timeframe allowed in order to meet compliance. -The measures for Part 7.1 (i) measure seem unattainable. While terminated employees should be immediately removed from the system, or as the text suggestions, even “prior to”; this seems like a very high goal. For instance, if one is terminated and they walk off the site with their badge at 10:00pm on Saturday night. How is the evidence of removal going to be captured the date of the termination action? -R7.2 It seems unreasonable to revoke all unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day, next business day would be more appropriate. Most transfers usually involve employees having possible dual roles for numerous days/weeks, this could be problematic for those type of employees and employees transferred on Fridays/Saturdays. -R7.3 Calendar day instead of business day. Calendar day could pose problems for all sizes of entities. -R7.1, R7.2 and R7.3 Reasonable time is required to allow for inter-company communications. Recommendation for 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require access. -R7.5 Clarify “extenuating circumstances”. Is this something that can be critiqued by an auditor?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – Provide a more granular break out if you only forget one quarter. Maybe a moderate vsl? -R1.1- Why does R1.1 apply to low assets when R1 only applies to high risks. -R3 – Provide a more granular break out also, possibly by percentage of total employees. As listed an entity could get a high vsl for “one” individual missing their training or for “200” individuals missing it. -R7 – Companies may have 10,000 employees or 100. It seems unreasonable if you miss 1 employee it can move either way (moderate-high or high-moderate), should this not go by percentages?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.5 Measure – when it asks for config files of an IDS deployed at an EAP, should it not read “for” an EAP. The Rationale mention IPS; however, the requirement only mentions IDS through-out. -Change rational for R1.5 states intrusion detection systems/intrusion protection systems. Does the “/” mean “and”, or “or”?
No

Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Verification that this does not include system to system communications in to the ESP. -R2.2 Clarification on where the encryption is required to start and stop? -R2.3 Where is the multi-factor authentication required?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.2 addresses restricting access to only those individuals that are authorized; however, the measures address egress badging. The requirements do not mention egress badging, but the measures do. -Requirements 1.4 and 1.5 address issuing alerts, but there is nothing about the response. -R1.4 – What is the definition of access point? (Window, hatch, door or all)
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - Clarification of the definition of continuous.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – High VSL lists a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. There is no mention of a time requirement within the standard. -R2 – Moderate VSL – The vsl states “each” however the requirement does NOT have the word each included. Is it implied? -R2 – High VSL – What are the requirements of “continuous escort”? Continuous escort is not defined, but it’s listed here. -Why does it apply to low but issues severe penalties?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1 – Screenshots as evidence for large companies could be overly onerous.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R2.1 – Clarification that the “updates for all software and firmware…” only applies to security related patches/updates. -R2.2 – Doesn’t define when a patch MUST be deployed, only that it has to be within a defined timeframe. Request clarification on what is an appropriate timeframe. -Does each patch require a remediation plan? (Or can there be generalized… Windows Tuesday update, etc...) -R2.3 – No mention of the 30 day requirement. Is this an oversight? It is mentioned in the “Change Rationale.” This should provide for a TFE.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. - R3.3 Provide clarification of availability. In requirement 2, it asks when an entity gets notified. Should this not follow the same process? Provide clarification of, “Update malicious code protections within 30 calendar days of signature or pattern update availability”. -R3.5 Provide clarification on where these logs can be kept. Can this be manual?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R4.1 – No TFE’s are allowed on this requirement. Concerned that not all devices can satisfy this requirement. -R4.1.4 – Very general statement, how would an entity define this? NIPSCO recommends removal of the word “potential” from the description. -R4.5 – Two week window with sampling is very tedious and time consuming. It is unclear what is defined as sampling? Is that one log, two logs, etc…? Would once a month or quarter be more appropriate?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R5.1 Measures – Define internal and remote paths. -R5.5.3 – There is no mention of a

measure for this requirement. Request to provide further clarification on the appropriate timeframe to change the password.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Request clarification on why the word “dated” has been added to the measures used throughout this requirement. -Do the suggested modifications in CIP-008 take into consideration Project 2009-01?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.5 –How does this address reliability or recovery of the BES? Even though you can TFE this requirement, this will be difficult to implement enterprise wide when individuals are concerned about recovery and not “mirroring drives”. How long do you keep this data (extra drives)? Protection of this additional drives/data could also become an issue.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R3.1 – Should this mean BES Cyber Assets or BES Cyber Systems? How many of the assets of the system?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.1.4 – Scripts could be anything from a customized startup script to a detailed script required for operations. Script is very vague and needs to be either removed or further detailed. -R1.1.5 and R1.1.6 – Request removal of the word “any” from the description. -R1.2 – A change advisory board is too large for many organizations and they don’t have them implemented. Provide a different example so entities won’t read that they are required to have CAB’s. -R1.4 – Determining security controls that could be impacted, where is the measure for this requirement?
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -Why is wireless review and scanning mentioned in the Guidelines section, but it’s not mentioned in the requirements? -Requesting clarification of “on the effective date,” and how to show compliance. -Request clarification of “vulnerability assessment” in a test environment.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on

this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R1.2 – Formatting issue at the Headers of columns CIP-011-1 Table R1, in which they all say “Part”
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard. -R2.1 – This requirement appears vague and request to review the description for more clarification. The word “cleared” appears to be essentially the same as “destroyed,” and request clarification on the appropriate method of clearing media and destroyed media that shows compliance. -The last paragraph in the Guidelines section actually still refers to “erased” and not “cleared”.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on this standard.
No
Comments: Until the proposed definitions are clarified, NIPSCO cannot provide an affirmative vote on these standards, therefore NIPSCO cannot provide an affirmative vote on the implementation plan.
Group
CenterPoint Energy
John.Brockhan@CenterPointEnergy.com
Yes
CenterPoint Energy suggests the following changes to the definitions: Page 1 – 2 – BES Cyber System/BES Cyber Asset/ BES Reliability Operating Services CenterPoint Energy does not agree with the introduction of these new terms and prefers the existing and familiar terms, Critical Asset and Critical Cyber Assets. The Company believes that the new terms and approach to determine covered assets lacks clarity, will be difficult to apply and audit, and creates ambiguity as to where the process ends. This is especially a concern considering the exhaustive list of BES Reliability Operating Services. If the SDT insists on retaining the BES Reliability Operating Services, CenterPoint Energy also suggests that the term not be added to the NERC Glossary, but be kept local to the CIP-002 Standard. The definition for BES Cyber Asset states that “Redundancy shall not be considered when determining availability.” CenterPoint Energy requests clarification on whether this concept has been reasoned for application in a substation environment, specifically in the instance of primary/backup relays and identical redundant systems. In the definition of BES Cyber System, the term “Maintenance” should be replaced with “Transient” in the definition of BES Cyber System to reflect changes in the terms and new definitions made available. Page 2 – BES Cyber Security Incident CenterPoint Energy believes “was an attempt” is vague and seeks clarification on how such an attempt will be determined. An alternative would be to delete the phrases “or was an attempt to compromise” and “or was an attempt to disrupt”. CenterPoint Energy also recommends that the 3rd bullet be deleted as it does not fit the term BES (Cyber) Security Incident. Page 2 – BES Cyber System Information CenterPoint Energy suggests that “computer” be added in front of network topology for clarification. The Company also suggests that the word “disaster” be deleted to be consistent with the way that recovery plans have been labeled in the current version. Disaster adds a qualification to recovery plans that could be limited to such situations (disasters). Additionally, CenterPoint Energy recommends that “Impact” be changed to begin with a lowercase “i” since a definition of BES Cyber System Impact has not been proposed. Page 2 – BES Reliability Operating Services Under Dynamic Response to BES Conditions, should “systems” be capitalized like the other items in the series (Elements, Facilities)? Please clarify. The criteria “Under and Over Voltage relay protection (includes automatic load shedding) -Sensors, relays & breakers” should be deleted as it is duplicated. Under Inter-Entity Real-Time Coordination and Communication, CenterPoint Energy questions the use of the term “operational directive” and would like to ensure that the SDT has considered NERC’s efforts underway to define “reliability directive”. Page 6 – CenterPoint Energy recommends that “or other, similar incident” be added to the definition of CIP Exceptional Circumstance to add some flexibility and “BES” be added in front of “Cyber Security Incident”. Page 6 – The Company proposes that the definition of CIP Senior Manager is not needed as a glossary term,

but is acceptable in the requirement description. Page 7 – CenterPoint Energy views the change in term to Defined Physical is unnecessary. Could not the definition of Physical Security Perimeter be updated with the meaning given to Defined Physical Boundary as seen with other existing terms? Page 7 – CenterPoint Energy requests clarification on the relationship between the EAP and ESP. Page 7 – CenterPoint Energy requests that the SDT use the definition from CAN-0024 for this term, External Routable Connectivity. Page 8 – CenterPoint Energy proposes that "consecutive" be added in front of calendar days for clarification. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy is concerned that the language (as stated in 2.7) will result in identifying substations as critical/medium impact when, in fact, they are not. Line count does not necessarily mean that issues at particular substation will have a significant impact on the BES. Such impact can only be determined by studies and risk-based analysis of an entity's assets. Thus, CenterPoint Energy is in support of language similar to that in CIP-002-3/CIP-002-4 for identifying substations that are critical to the reliable operation of the BES. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy suggests that the SDT consider continuing the concept of starting with assets as an alternative approach. CenterPoint Energy proposes that the approach be based on an identification of High, Medium, and Low assets and then proceed with identifying Critical Cyber Assets at those facilities. Page 19 - 21 - "Operations Service" should be "Operating Service". CenterPoint Energy would like to request the removal of the extra bullet under Managing Constraints as it appears that criteria may be missing. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy proposes that documentation errors should rarely if ever be deemed high/severe. Only violations that could have an immediate impact on the reliability of the BES should be considered high/severe. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy supports the concept of assigning a senior manager as outlined in the existing standards/requirements. However, the rationale for changing the language and numbering of this requirement is not obvious as the changes are immaterial and appear to have no effect on the implementation of the requirement. There will be an impact on compliance and compliance tracking for no substantial benefit. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Similar to the previous comment on R1, CenterPoint Energy supports the concept of establishing a cyber security policy as outlined in the existing standards/requirements. However, the rationale for changing the language and numbering of this requirement is not obvious as the changes are immaterial and appear to have no effect on the implementation of the requirement. There will be an impact on compliance and compliance tracking for no substantial benefit. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
See comment for R2. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the SDT revert to the CIP Version 3/Version 4 language for this requirement as the changes are immaterial in writing yet could prove moderate in interpretation and implementation. The change is also not supported by a FERC directive. The Company would also like to propose that this requirement should be limited to the applicability of High and Medium impact BES Cyber Systems as it pertains to the categories and formatting. CenterPoint Energy also suggests that "unescorted" be added in front of all references to "access". CenterPoint Energy recommends that the

last 3 bullets under Measures (M4) be deleted as bullet 1 or 2 should be sufficient to prove compliance. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the SDT revert to the CIP Version 3/Version 4 language for this requirement as the changes are immaterial in writing yet could prove moderate in interpretation and implementation. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
The footnote reference should be reformatted. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy views the VRF/VSLs for R4 and R5 as unreasonable and proposes that they be lowered. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests clarification on who should receive the on-going reinforcements. Alternatively, the SDT should revert to the CIP Version 3/Version 4 language. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests clarification on role-based training and suggests that “and the training needed.” Be added to Requirement 2.1. CenterPoint Energy also suggests that 2.2 be deleted and 2.3 and 2.5 be combined for simplification and clarity. Additionally, Requirement 2.7 should also be deleted and its concepts combined with 2.9. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 14 and 15 - R3.1 and R3.2 - CenterPoint Energy requests that “Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems” be removed from the applicability as it is seen as an expansion in scope that is not supported by a FERC directive or rationale. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the applicability for this requirement be set to match that of R5.
Yes
CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy does not agree with this requirement and proposes that the SDT refer to the CIP Version 3/Version 4 language. There are also concerns on the measures and the amount of evidence required to demonstrate compliance. The first measure should be adequate. Also, the description of evidence on the 3rd measure is unclear. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 29 - R7.1, CenterPoint Energy suggests that the SDT change "at the time" to "concurrent or prior to the date of" to minimize the issue of time alluded to in footnote #2. Page 30 - R7.2 – CenterPoint Energy believes that the time limit of “by the end of the next calendar day” is unreasonable for reassignments or transfers and proposes that the SDT consider extending the time limit. CenterPoint Energy understands that access of transferred individuals should be reviewed and updated; however, there is usually a period of transition and such personnel changes are within the same organization. “Accumulating unnecessary authorizations through transfers” usually happens over a time period that is longer than the 7 days which is the current requirement. Page 31 – R7.3 – CenterPoint Energy requests clarification on tracking access to BES Cyber System Information. It appears that removing access to the system and physical facilities would be satisfactory. Page 33 – R7.5 – CenterPoint Energy is concerned with the applicability of this requirement to Medium Impact BES Cyber Systems. Implementation would have a significant impact on substation operational procedures. CenterPoint Energy questions if the removal of physical access for Medium Impact BES

Cyber Systems sufficient. For entities that do not network assets, this is not technically feasible. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Most of the VRF/VSLs are High/Severe. CenterPoint Energy believes that such classifications are not reasonable for most requirements given that minor exceptions would not lead to an interruption to the BES. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy recommends that the words “and monitor” in the Rationale for R1 be deleted as it does not fit with the definition or concept of Electronic Security Perimeter. Under Summary of Changes, “points” should be capitalized. Page 11 - R1.1 – Under Measures, “technical and procedural” should be changed to “technical or procedural” to reflect the language in the requirement. Additionally, CenterPoint Energy proposes the following wording for the measures: Evidence may include, but is not limited to, existing documented technical or procedural controls. Page 11 – R1.2 - CenterPoint Energy requests that “Associated Physical Access Control Systems” be removed from the applicability as it is seen as an expansion in scope that is not supported by a FERC directive or rationale. CNP suggests that “with external routable and dial-up connectivity” be added to “Associated Protected Cyber Assets”. Also, proposed alternative wording for the requirement is as follows: Control and secure all instances of external connectivity through the use of identified Electronic Access Points (EAPs). Page 12 – R1.3 – CenterPoint Energy suggests replacing “granting or denying” with “denying access by default”. Page 13 – R1.5 – CenterPoint Energy seeks clarification on whether this requirement is for host-based or network based intrusion detection systems or is it optional. The Company also suggests that “at each EAP” be changed to “at each ESP”. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy seeks clarification on when encryption initiates and terminates. CNP also requests that the SDT consider splitting this table into specific requirements for dial-up and requirements for routable. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations instead of all being rated, “Severe.” CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 11-12 – R1.2 &1.3 - CenterPoint Energy is concerned that tracking for ingress and egress is not available for many physical access control systems and a TFE might be necessary. This is also a change in scope that is not supported by a FERC directive or rationale. Page 13 - R1.4 – CenterPoint Energy requests clarification or a description of a “real-time alert”. In reference to a “response to an unauthorized physical access”, please clarify if this means real or attempted as a pure population of real or especially attempted events would be hard to track. In the case of unauthorized badge swiped, yet the system does not open the door, is that an “attempt”? Page 14 – R1.6 - CenterPoint Energy requests clarification on the retention required. Will entities be required to have 90 days as in the current standard or 3 years? Storage for three years of logs that are not related to an event could prove costly and burdensome for no benefit. CenterPoint Energy also has concerns regarding implementing this requirement in the substation environment given the group work that occurs under the direction of a crew leader. Does each person have to be identified? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
Yes
CenterPoint Energy supports the comments submitted by Edison Electric Institute (EEI).
No
Page 18 – R3.1 - CenterPoint Energy requests clarification on what the SDT expects to be done at a door/fence/gate. Page 18 – R3.2 – CenterPoint Energy suggests that “or Monitoring Systems” be deleted under applicability. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy supports the comments submitted by Edison Electric Institute (EEI).

No
Page 10 – R1.1 - CenterPoint Energy foresees a substantial impact given this revised wording and suggests that the SDT consider the CIP Version 3/Version 4 language. Specifically, the change in “documenting compensating measures” (CIP Version 3/Version 4) versus “documenting the need” (CIP Version 5) could prove difficult for dynamic ports with little benefit and may not be technically feasible for all systems. CNP believes that intention and results would be the same if the legacy language was retained. Page 10 R1.2 – This requirement is very broad. Alternate wording could be included as follows: “Protect against the use of unnecessary physical I/O ports”. CenterPoint Energy also requests that the SDT consider provisions for procedural controls. The inclusion of removable media on this requirement is also a concern. CNP suggest that the term, removable media be deleted. The Company also does not believe that signage provides solid security benefit. Logical restriction and placement in a Defined Physical Boundary appears adequate to meet the requirement. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 12 – R2.1 - CenterPoint Energy requests that the SDT clarify that a null list is acceptable or include provisions for a TFE for this requirement as implementation may not be possible for all substation systems or assets. Also, add “security related” in front of updates. CNP also requests that the last sentence of the measures be deleted: “The list could be sorted by BES Cyber System or source.” Page 13 – R2.2 – CenterPoint Energy suggests the following as alternative language: “Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 60 days of release from the identified source.” Page 14 – R2.3 – CenterPoint Energy believes that the measures go above and beyond the requirement which only calls for a process. Detailed records would depend on the contents of the process. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 17 – R3.1, 3.2 - CenterPoint Energy suggests that the applicability be updated to reflect application to “Medium Impact BES Cyber Systems with External Routable Connectivity”. R3.2 – The measures do not align with the requirement. CNP suggests deleted bullets, 2 and 3. Page 18 – R3.4 – CenterPoint Energy requests that references to Transient Cyber Assets be deleted. The measure regarding logs should be moved to R3.5. Page 19 – R3.5 – CenterPoint Energy requests clarification on the implementation of this requirement as the Company foresees it to be burdensome and unrealistic, especially in a substation environment. Is this intended to be a system or manual log? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 21 – R4.1 – CenterPoint Energy requests that “BES” be added in front of “Cyber Security Incident” and provisions for a TFE are made. CenterPoint Energy also recommends that the applicability for this requirement be set to match that of R4.4. Page 22 – R4.2 - CenterPoint Energy requests that the SDT revert back to the CIP Version 3/Version 4 language or provide a description for “real-time alert”. Page 23 – R4.3 – Add "after failure is identified or made aware of" in the requirement. Page 23 – R4.4 – CenterPoint Energy requests that the SDT revert back to the CIP Version 3/Version 4 language as there is no substantive change or related FERC directive. CNP also suggest that the measures sentence end before “and”. Page 44 – R4.5 - CNP suggests that the requirement ends before “and”. CNP also suggest that the measures sentence end before “and dated evidence…”. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 27 – R5.1 - CenterPoint Energy recommends the following alternative language: “Authenticate individual and shared account access before granting electronic user access to each BES Cyber System where technically feasible.” Page 28 – 30 - R5.2, 5.3, and 5.5 – CenterPoint Energy recommends that the “Medium Impact BES Cyber Systems” applicability for these requirements be updated to “Medium Impact BES Cyber Systems with External Routable Connectivity”. Page 31 – R5.6 – In regards to the applicability, Medium Impact BES Cyber Systems at Control Centers, CNP requests clarity on the types of devices that fit this description. Consoles only? CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint

Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 11 - R1.1 – CenterPoint Energy requests that the phrase “or Defined Physical Boundary of BES Cyber System and” be deleted as it should not be included with Cyber Security Incidents. Provisions for physical incidents are covered under CIP-001 and EOP-004. Page 12 – R1.3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 13 – R2.1, 2.2, 2.3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, Page 15 - 17 – R3 – CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 5 – In the Purpose statement, CenterPoint Energy requests that the sentence end before “and” since business continuity and disaster recovery is beyond the scope of this Standard. Page 16 – R3.2 – Thirty calendar days is not enough time. CNP proposes that the requirement be updated to state “within 30 days of determining actual cause”. Page 16 – R3.3 – Add “if necessary” to the end of the sentence. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CNP also recommends that the “Requirement R1” paragraph under Guidelines and Technical Basis be deleted as entities should be able to refer to the definitions. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 10 – R1.3 - Delete "protection of information” as it is required in CIP-011. Page 11 – R1.4, R1.5 – Check Table R1 headings. R1.4 - CenterPoint Energy requests that the SDT clarity what “verified” means in the requirement. (ex. A log showing status – “Successful”) CNP also asks that “after significant changes to the system" be added to the end of the sentence. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI). R1.5 – CNP proposes the following alternative language: “Preserve data for analysis or diagnosis of the cause of an event that triggers activation of the recovery plan as required in Requirement R1 when it does not impede or restrict restoration.”
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. Page 13 – R2.2 – CenterPoint Energy suggests replacing “Test any information” with “Test a sample of information”. Page 14 - R2.3 – Delete “Medium Impact BES Cyber Systems at Control Centers” from applicability. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 15 – R3.1 – Delete “or when BES Cyber Systems are replaced” from the requirement. Page 16 – R3.2 – Delete “incident” from the requirement and the measures. Thirty days is not enough time to perform the exercise and document lessoned learned. CenterPoint Energy suggests 60 days. Page 17 – R3.4 – CenterPoint Energy suggests the following as alternative language: “Update recovery plan(s) within thirty calendar days of any organizational or technology changes that impact that plan.” CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).

No
CenterPoint Energy believes that the R1 requirements would be burdensome, not realistic for every day operations and difficult to implement for every asset, especially in the substation environment. Implementation is complicated further by the details listed in the baseline configuration (R1.1). CNP suggests that this requirement be modified to accommodate general testing and significant changes. Additionally, R1.5 seems to imply that there must be a test environment. Some testing may have to be done in the production environment. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Page 15 - R2.1 - CenterPoint Energy believes this requirement would be overly burdensome especially in a substation environment that is not networked. CNP proposed that the applicability “Medium Impact BES Cyber Systems” be updated to “Medium Impact BES Cyber Systems with External Routable Connectivity. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy proposes that the description does match vulnerability assessment and requests that the SDT clarify or refer to CIP Version 3/Version 4 language. CNP also suggests that “cyber” be added in front of security controls. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Generally, CenterPoint Energy requests that the SDT revert back to CIP Version 3/Version 4 language since only minor wording changes are included that are not related to a FERC directive. CNP also suggests that the applicability for Medium Impact be with the qualifier of “with External Routable Connectivity” or “at Control Centers” and “Associated Protected Cyber Assets” deleted. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy suggests that 2.1 and 2.2 be combined and Associated Protected Cyber Assets be removed from applicability. Additionally, the term media could refer to a long list of devices for which this requirement would be difficult to track and enforce. CNP also requests clarification on the term reuse. (ex. Can assets be reused/redeployed as long as they remain in the Defined Physical Boundary and for the purpose of BES Cyber Assets/Systems?) CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
CenterPoint Energy requests that the SDT consider a more gradual scale for violations. CenterPoint Energy also supports the comments submitted by Edison Electric Institute (EEI).
No
Given the scope expansion and anticipated impact of CIP Version 5, CenterPoint Energy suggests that 18 months is not sufficient time to implement. CNP also requests that the effective date not be set in the month of December or January considering various business processes conducted at the end of the year.
Group
LCEC CIP Team
Ed Nagy
Yes
BES Cyber Asset: This section of the definition is confusing and should be omitted: This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The reference to a “Cyber Asset” within the definition includes a number of devices that might need further clarification due to the word “programmable”. Would a relay that is “configured” be considered a Cyber Asset even if the configuration does not involve any kind of network, telecommunication or IP based network connectivity? BES Cyber System Information: Information about a BES Cyber System or Asset could

include vendor provided manuals and should not be included. Cyber Assets: Need to clarify what is meant by the term “Programmable” A Cyber Asset should imply that some form of connectivity is required to access the device otherwise it would simply be an Asset. Electronic Access Point & External Connectivity These definitions do not touch on serial interfaces that are not dial-up. Does this mean that serial communications will not be considered External Connectivity?
Yes
Attachment 1 criterion 2.13 categorizes all Transmission Operator (TOP) and Transmission Owner (TO) Control Centers as Medium impact to the BES. This criterion is too inclusive as it includes Control Centers of low impact Radial Transmission Owners and Operators unnecessarily. This results in the applicability of security controls that are not at all aligned with the risk that these Control Centers could have on the BES. To avoid this situation, Criterion 2.13 could be aligned with criterion 2.7 but instead of focusing on a single station or substation; consider all of the facilities that the Control Center controls. If the “total aggregate value” of all Transmission Facilities does not exceed a value of 3,000; the Control Centers should not be designated as Medium impact. For Example: 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners with a “total weighted aggregate value” that exceeds 3,000 for all Transmission Facilities controlled by the Control Center per criterion 2.7; or (2) generation control centers that control 300 MW or more of generation. This modification is well aligned with the NIST risk management framework and the drafting team’s approach to focus on the impact to a shared resource like the BES. Criterion 2.7 must have been developed with an engineering basis that relates to the impact of Transmission Facilities on the BES. With this in mind, the same impact to the BES can only be realized if the sum of all facilities managed by a Control Center exceeds this same criterion. In the NOPR for CIP-002-4 and the subsequent response to the NOPR by NERC the NIST Risk Management Framework is discussed in section 5. In this section the stated goal is to “Categorize BES Cyber Systems based on their function and impact”. In addition, “A tiered approach to security controls which specifies the level of protection appropriate for systems based on their importance to the reliable operation of the Bulk-Power System” is discussed. The drafting team’s approach to categorization is in fact “Based on the “impact” or compromise or of the scope of control of the BES Cyber System”. In this example, it makes sense to modify the criterion to remain consistent with the categorization based on the impact and scope of control of these Low Impact Control Centers. In the NOPR for CIP-002-4 and the subsequent response to the NOPR by NERC, “Potentially unprotected Control Centers” are discussed in section 6. The FERC concern that many Control Centers are left with “No obligation to apply cybersecurity measures” under CIP-002-4 is legitimate. The response however should not be to include all remaining Control Centers as Medium Impact assets as is the current approach in CIP-002-5 criterion 2.13. The best approach is to continue to align security controls with the risk and impact to the BES. Many of the Control Centers that FERC is concerned with will be included as Medium Impact BES Cyber Systems if this change is made while others have cybersecurity measures required as is appropriate for Low Impact Assets.
No
R1.1 This requirement states that documentation needs to be updated within 30 days if BES/Facility changes result in a change to the categorization of BES Cyber Assets or Systems from a lower to a higher category if intended to be in service for more than 6 months. What is the expectation for compliance with the additional standards as a result of this change in categorization? It will be difficult to determine “intent” from an auditing perspective. What happens if there is “intent” but the six months is exceeded or the intent changes? In addition, this requirement doesn’t state what the expectation is for new Cyber Assets or Systems or Cyber Assets or Systems that may move from a High to Medium or Medium to Low Category. Is there any requirement to document these changes other than during the annual review process in R2? Table of Compliance Elements For both R1 & R2 Lower VSL, what is the VSL if less than 30 days for updates in R1 or Review and approval for R2? Is there such a thing as having NO VSL?
Yes
No
Table of Compliance Elements For both R1 & R2 Lower VSL, what is the VSL if less than 30 days for updates in R1 or Review and approval for R2? Is there such a thing as having NO VSL?
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
R2.1 The requirement does not call for the identification of training that is needed for each role but this is listed in the measures section of the table. Need to add this to the requirement.
Yes
Yes
Yes
Yes
No
R7.1, R7.3, R7.4, R7.5 Resignation and termination are very different and need to be treated as such. A resignation may take place weeks prior to the last day of service which is when access needs to be revoked.
No
R1.1 This requirement calls for technical or procedural controls for Low Impact BES Cyber Systems with External Routable Connectivity. Since there is no requirement to identify these assets or systems, it will be difficult to audit this.
Yes
Yes
No
R2.1 The requirement for continuous escorted access of visitors makes sense but it is difficult to prove compliance with this requirement. The measures include language in a visitor control program AND additional evidence to demonstrate compliance such as visitor logs. Visitor logs DO NOT demonstrate compliance with this requirement. Recommend removing the AND from the measures section of the table. R2.2 Need to clarify what meant by “point of contact” for the visitor. Cell phone? Office Phone? Email address?
No
3.1 and 3.2 The applicability section is unclear, are the “Associated Physical Access Control or Monitoring Systems” referring to security systems that protect Medium or High Impact Cyber Assets or Systems only?

Yes
Yes
No
R3.1 & R3.4 Need to clarify if this requirement is deter or detect or prevent Or deter and detect or prevent Or deter and detect and prevent The wording is highly subjective and should be clarified. R3.4 & R3.5 Need to clarify if manual logs are acceptable for audit proof or if all systems need to be able to generate a log to show when Transient Cyber Assets have been connected. (Auditors will likely ask for system logs) This may not always be technically feasible for removable media on all assets. In addition, the connection may be via a network connection as opposed to a physical connection.
No
R4.4 Retention of logs for 90 days will not meet the expectation of auditors that will demand to see logs to demonstrate compliance for the entire reporting period. This standard should clearly state that the entity is not required to maintain these logs beyond 90 days and that the auditor should audit the process and/or select a test sample from the population of available logs.
Yes
Yes
No
R1.1 and R1.2 In order to identify, classify and respond to BES Cyber Security Incidents the entity would need to identify all of the Assets or Cyber Systems. This is not a requirement for Low Impact BES Cyber Systems but it is implied by these requirements.
No
See Response to Question 34
No
See response to question 34
No
1.4 Need to clarify what is meant by “verified” initially after backup
No
R2.2 Need to clarify what is meant by “test initially” and at least once each calendar year. Does this imply that a full recovery must be performed for each backup? If so, the best practice of completing more frequent back-ups may be bypassed to achieve compliance. Suggest removing “test initially” from the requirement. Also need to clarify that back-ups will likely not contain the most current configuration unless they are performed frequently.
Yes
Yes
No
R2.1 The “where technically feasible” statement implies that monitoring should be automated in some fashion and that if this is not possible, that a TFE will be generated. This will result in significant TFE’s which do not add value from a security perspective. In addition, the baseline that is referenced in section 1.1 includes the physical location. How will this be monitored without performing a physical inventory and at what cycle?
No
R3.1 This requirement calls for a paper OR active assessment of the security controls to determine

the extent to which the controls are implemented correctly and operating as designed. The terms “implemented correctly” and “operating as designed” seem to imply technical controls which will be difficult to validate with a paper based assessment. The paper review is a good option for entities so I would recommend that the results section of the requirement be rewritten as follows “to determine the extent to which controls are implemented and/or operating as designed.”
Yes
Yes
Yes
Individual
Curt Wilkins
Douglas County PUD No.1
No
No
No
The Rationale for R1 appears to imply a two-step process in the identification and categorization of BES Cyber Assets/Systems, i.e. “Once they have been identified, they must be categorized according to their impact…” However, in R1 as currently written, the word “identify” comes after the statement that the requirement applies to Entities that own BES Cyber Assets/Systems. This implies that the identification step has already occurred. So, does the word “identify” refer to identifying High and Medium Impact BES Cyber Assets/Systems,” or does it refer to identifying which Cyber Assets/Systems are BES Cyber Assets/Systems? If the former, it seems that “identify” is redundant with “categorize” since, identifying which BES Cyber Assets/Systems have High or Medium Impact would be the categorization step. If the latter, then “identify” seems to be misplaced in the sentence since, in the introduction to R1, Responsible Entities have already determined that they own BES Cyber Assets or BES Cyber Systems. Suggest rewording R1 to clearly identify the two-step process or adding a new R1 for the identification step: New R1: “Each Responsible Entity shall identify its BES Cyber Assets or BES Cyber Systems by determining which of its Cyber Assets or Cyber Systems perform or support any BES Reliability Operating Service and could impact the reliable operation of the BES.” Evidence could be a list of Cyber Assets or Cyber Systems with a determination of the BES Reliability Operating Service(s) they perform, if any. BES Cyber Assets or BES Cyber Systems would be those Cyber Assets/Systems on the list that could adversely impact the BES Reliability Operating Service, per definition. It seems that this would aid the Entity in audit preparation by having a complete audit trail of its BES Cyber Asset/System identification and categorization processes. New R2: “Each Responsible Entity that owns BES Cyber Assets or BES Cyber Systems shall categorize them according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. BES Cyber Assets and BES Cyber Systems that it owns that are not categorized as High or Medium Impact shall be deemed to be Low Impact and do not require discrete identification.” Evidence would be the same as the currently written M1. The “BES Reliability Operating Services” paragraph, CIP-002-5 page 8, appears that it should be edited. Sentence 2 states “In order to identify them, Responsible Entities determine whether BES Cyber Assets perform or support any BES Reliability Operating Service.” If it’s a BES Cyber Asset, then it has already been identified and determined. Suggest removing “BES” prefix to Cyber Assets: “In order to identify them, Responsible Entities determine whether Cyber Assets or Cyber Systems perform or support any BES Reliability Operating Service.” Also suggest truncating sentence 4 after BES Cyber Systems to avoid the redundancy of “that perform or support BES Reliability Operating Services,” i.e. “This ensures that the initial scope for consideration includes only BES Cyber Assets and BES Cyber Systems.”
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Typo in R6, should be "change" not "change2".
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
DOPD agrees with the intent of R2, but makes the following suggestions for Part 2.1: (1) “when incidents occur” seems redundant with “When a BES Cyber Security Incident occurs,” (2) “or test” appears to be tacked on to the end without being mentioned earlier in the requirement, and (3) suggest using the word “exercise” instead of “test” to correlate with Part 2.2. Suggested rewording “When a BES Cyber Security Incident occurs or the BES Cyber Security Incident Response Plan is exercised, the incident response plans must be used and include recording deviations taken from the plan during the incident or exercise.” In the Measure for 2.1, suggest adding “or exercise” at the end of the measure: “…deviations taken from the plan during the incident or exercise.”
Yes
Yes
Yes
The column headings for CIP-009-5 Table R1 for Part 1.4 and 1.5 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part. DOPD agrees with the intent of Part 1.5 as it applies to preserving forensic data for analysis of potential cyber security incidents or cyber events. Many triggers of the recovery plan(s) could be for physical, non-cyber events such as damage or failure due to fire, water, earthquake, power failure, etc. Taking the time to preserve data for these non-cyber events may increase the time it takes to recover the cyber assets. Suggested wording: “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any cyber event that triggers activation of the recovery plan(s) as required in Requirement R1.”
Yes
Yes
The column headings for CIP-009-5 Table R3 for Part 3.4 and 3.5 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part.
Yes
Yes
Yes
Yes
Yes
Yes

The column headings for CIP-011-1 Table R1 for Part 1.2 and 1.3 need to be corrected to “Applicability,” “Requirements,” and “Measures,” rather than Part, Part, Part.
Yes
Yes
Yes
Individual
Brenda Frazer
Edison Mission Marketing & Trading
No
No
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
We do not think it should be required to badge out and we think it could present a problem if there were an emergency. And if it is being said that you do not have to badge out to open the door to exit - then are we not opening ourselves up to multiple violations/self reports and possibly fines?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Black Hills Corporation Registered Entities (NCR00089, NCR05030, NCR05031 & NCR11186)
Bob Case - NERC Compliance Manager (605) 721-2716
No
Yes
The reference to “Change Management” in Attachment 1 (looks more like a capital (i) in the standard) of CIP-002-5 under Situational Awareness carries multiple meanings in the industry… e.g. the human reaction to change, managing changes in resource and transmission capabilities, and the validation process of security and upgrade patches. In the context of Attachment 1, the “managing changes in resource and transmission capabilities“ example is preferred.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
If the expectation is that delegation of approvals is required down to BES cyber system gate keepers (asset owner), then this requirement is considered overly prescriptive.
Yes
No
For R2: Suggest that a Moderate VSL be added that reads as follows: “The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required parts 2.1 to 2.10”. Change the High VSL to read as follows: “The Responsible Entity has implemented at least one cyber security policy, but has failed to address more than one of the required parts 2.1 to 2.10”. Change the Severe VSL to read as follows: “The Responsible Entity has not implemented any cyber

security policy." For R4: Add a Moderate VSL: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Less than 5% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function." Change the High VSL to read: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Greater than 5% but less than 50% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function." Change the Severe VSL to read: "The Responsible Entity has made some, but not all, individuals who have access to BES Cyber Systems aware of elements of the cyber security policies appropriate for their job function. Greater than 50% of those individuals who have access to BES Cyber Systems were not made aware of the cyber security policies appropriate for their job function."
No
The Measures section in Table R1 is worded in a way that may cause confusion. The wording "…and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed." may be interpreted to mean that more than the quarterly reinforcement material was necessary. Suggest changing to: "…and additional evidence to demonstrate that this program was implemented and awareness materials were identified and delivered to meet timeframes specified in the regulations." Also, since security awareness may be general in nature and a key contributor to a good corporate security program, it makes sense to add the ability to encourage vendors to provide their own awareness materials to their employees and allow the RE to accept documentation of that vendor awareness as compliance for this requirement relative to contractors and/or vendors with access to BES systems. The specific addition to the Measures section could read: "Documented evidence of awareness for contractor and/or vendor employees with access the BES systems may include evidence of the vendor's documented security awareness program and additional evidence to demonstrate that the vendor's program was implemented and awareness information was identified and delivered to the vendor/contractor employees to meet the content and timeframes specified in the regulations."
No
Delivery of cyber security training to vendor support staff who, most often, are never physically on site at a Registered Entity's facility can be difficult to document. For Table R2 Measures section for sub-requirements R2.2 – 2.10, retain the first paragraph in each sub-requirement as written, but add a second paragraph as follows: "Evidence to support contractor/vendor training may include, but is not limited to, vendor's attestation/certification that Responsible Entity's role-specific training has been delivered to all contractor/vendor employees with access to Responsible Entity's BES Cyber Systems."
No
Delivery of cyber security training to vendor support staff who, most often, are never physically on site at a Covered Entity's facility can be difficult to document. For Table R3 Measures section for sub-requirement R3.1, retain the first paragraph in each sub-requirement as written, but add a second paragraph as follows: "Evidence to support contractor/vendor training may include, but is not limited to, vendor's attestation/certification that Responsible Entity's role-specific training has been delivered to all contractor/vendor employees with access to Responsible Entity's BES Cyber Systems."
Yes
Yes
No
This language appears to change the access granting process significantly by requiring the CIP Senior Manager or delegate to authorize all electronic access. We believe this responsibility is typically job role (specific asset owner) based, and is not based on an individual delegation. Recommend that the language remain as identified in CIP-004-3, with updates as follows to retain the consolidation of access requirements found in CIPs-003, 004, 006, and 007": R6.1: Recommend the following language: "The responsible entity shall authorize electronic access based on minimum necessary work requirements except for those situations meeting the definition of "CIP Exceptional Circumstances". R6.2: Recommend the following language: "The responsible entity shall authorize unescorted physical

access to BES Cyber Systems based on minimum necessary work requirements except for those situations meeting the definition of “CIP Exceptional Circumstances”. R6.3: Recommend the following language: “The responsible entity shall appropriately manage and grant access to BES Cyber System information based on minimum necessary work requirements except for those situations meeting the definition of “CIP Exceptional Circumstances”.
No
R7.2 and R7.3: The language used fails to address issues related to ongoing access requirements during ‘transition periods’ associated with employee transfers. Recommend the following addition to the Requirements Section of Table R7: “For retirements and reassignments, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems by the end of the next calendar day after access is documented as no longer required.
No
There are many administrative requirements where zero tolerance is inappropriate. Missing a re-training date by a day or a week should not be considered a High or Severe violation level.
Yes
Yes
Yes
No
R1.3 needs to clarify the need for multiple access controls vs. multiple physical access layers.
No
Intentions of change are good, however, the change description and justification in table 2 (R2.2) do not seem to reflect the current wording of the requirement.
Yes
Yes
Yes
No
The statement at the bottom of CIP-007-5 Table R2 “This is the same concept as in the current CIP-007 R3.2 wording however a 30 day window was given to allow for documentation of the actual implementation in a less time constrained manner where manual processes are used” confuses the expectation for the implementation vs. the implementation plan needing to be done within 30 days.
No
No definition of transient cyber assets or transient cyber asset connections is provided within the standard, but is needed. Realize that is defined in supporting documents, but terms should be defined in the NERC Glossary, or the standard directly.
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
CIP-009-5 Table R1 in Part 1.5 requires preserving data, where technically feasible. This suggests that a TFE will be required if preserving data is not technically feasible. Do not understand how a TFE can be completed in its current form (compensating factors) since this would occur post-incident, and if the data is gone, it's gone.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Request clarity in R1.3 as to whether discovering a document not properly handled during an assessment constitutes a violation, even though the process was in place.
Yes
Yes
Yes
Individual
David Kiguel
Hydro One Networks Inc.
Yes
Refer to additional comments submitted for Question 49. "Suspicious" is not an auditable term, and should be removed. What is an "attempt"? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident: • A malicious act that: Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under "BES Reliability Operating Services": • "Identify and monitor flow gates" under "Managing Constraints" appears to be missing its bullet. • Recommend that "Change management" under "Situational Awareness" be clarified to changes in the BES instead of IT change management. • Recommend clarification that "Facility" is the NERC Glossary term--in "facility operational data and status" under "Inter-Entity Real-Time Coordination and "Communication": • Request clarification of the scope of this "Operational Directives". Does it include a company's messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions." • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.

Yes
Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all regions, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOP, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appealing?
No
For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation.” For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities).” The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize Cyber Assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No

The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical.”
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except…” to “authorize electronic access to BES Cyber Systems, except…” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary.” For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP." Is that inside, outside or both? Regarding CIP-005-5, the

Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. This would make the CIP standards consistent with the Results Based Standards concept.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." As written, the proposed Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress." Request that Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls." Is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress." Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. to "issue real time alerts for detection of breach through an access point." For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis."
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices."

No
Request clarification on 1.1. Is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1. Why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard. Screenshots seem to be excessive for this requirement. Documenting the need for each network-accessible port is sufficient.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow having an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process? How do we address the risk of the patch affecting the potential reliability of the BES upon testing, prior to release? What is the recourse if not applied within the 30 days when potential issues have been identified?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3. Does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks." We recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types?" Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the

need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.

No

Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2".

No

For 1.3, request clarification of the “protection of information.” Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not, what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rational? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Do “backup media” include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments.” What is the scope? All network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the

Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Recommend changing 1.3 to avoid double jeopardy from "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment." to "in a production environment or a test environment." to allow Entities more flexibility in meeting this Requirement.
No
Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are

different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5.\ There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Request that footnote 2 in 2.1 be moved into that Requirement.

No

The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 has not been yet approved by FERC, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry. Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with the implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

Individual

Michelle Denike

Wolverine Power Supply Cooperative, Inc.

Yes

Definition needed for BES Cyber System Impact.

Yes

High and Medium Impact Ratings use the term "adversely". This needs to be defined. This is too subjective of a term. Under 2.13 what is meant by the term "control" in (2) generation control centers

that "control" 300 MW or more of generation? Does this mean physical control only or does it include verbal commands? Also, does the 300 MW refer to name plate rating or some other method AND is that 300 MW only for BES generation or all generation that generation controls?
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
What is the difference between "provisioned" and "authorized"?
No
7.5 The term "extenuating" can be interpreted many different ways. Clarification is needed here.
Yes
No
R1.1 and R1.2 Clarity is needed for the terms "restrict" and "control and secure".
No
Yes
No
R1.6 The term "sufficient" is very subjective and needs to be clarified.
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Individual
Ron Donahey
Tampa Electric Company
No
In general, Tampa Electric supports the Comments from EEI for CIP002 with the following additional clarifications and suggestions: Tampa Electric suggests that SDT provide examples of potential assets for control center, transmission substations, and power generation in each type (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.) How far does the BES Cyber System extend? EMS is definitely a BES Cyber System; does it extend to the switches, routers, time & frequency devices, Digis, Front End Processors etc.? Tampa Electric recommends that the SDT improve the definition of the BES Cyber Asset related to "adversely impact" one or more BES Reliability Operating Services in order to provide clarity. The SDT may wish to consider the current definition of Adverse Reliability Impact in the NERC Glossary of Terms. Alternatively, adversely impact should be defined as an "impact greater than the Reserve Sharing Group"; otherwise the term is vague. Tampa Electric believes that the definition of Transient Cyber Assets is too broad and could include USB, CD, and external drives. It should be focused on equipment that includes a processor such as a laptop pc or mobile computing device.
No
Tampa Electric supports the Comments from EEI for CIP002 Attachment 1 with the following additional clarifications and suggestions: For Control Centers, substations and generation – Tampa Electric suggests that SDT provide examples of assets in each type of this new breakout/definition (BES Cyber System, BES Cyber Assets, Associated Electronic Control & Monitoring, Associated Physical Access Control, Electronic Access Point, etc.) Tampa Electric also requests that the SDT provide supporting documentation similar to Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets. Tampa Electric also notes that significant effort is required to classify BES CS as High, Medium or Low Impact with very little differentiation within the actual requirements of the standards themselves. At a minimum, all VSLs should be evaluated to determine if the levels of severity should mirror the impact categorization. Tampa Electric also suggests the following for consideration: 2.1. Generation with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. This language does not address the following: Under Guidelines and Technical Basis, on page 24, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Tampa Electric recommends that the item 2.1 be re-worded to incorporate the concept of only generation systems with common mode vulnerabilities. 2.12: Tampa Electric recommends that the Standard Drafting Team review of the Application Guidelines related to 2.12. 2.12 define as Medium Impact the 300 MW UVLS or UFLS; there is a reference to 2.13 for UVLS/UFLS. We believe this is a typo and should be 2.12. 2.13: Tampa Electric recommends SDT review of the Application Guidelines related to 2.13. The criteria includes "generation control centers" (lower case); however, on page 30, the Application Guidelines specifies "Transmission Operators and Owners Control Centers" (upper case). Since Control Center (upper case) is a defined term, it is unclear if "generation control center" (lower case) is a newly introduced term and exactly what this is referring to. For example, is this referring to a single control room at a single generation facility that controls more than 300MW or is it referring to a control center for multiple generation facilities?
No
Tampa Electric agrees with the EEI comments with the exception of their suggestion to add the requirement to identify lows. Tampa Electric proposes the identification of Low Impact BES CS at a Facility level, not by listing all the Cyber Assets associated as this would add administrative burden and not provide additional BES CS security or BES reliability. 1.2. Evidence Retention - For instances where the evidence retention period specified below is shorter than the time since the last audit, Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer. Tampa Electric recommends that the document retention period should follow the requirement; as stated, the evidence retention period is open ended.
No
Tampa Electric agrees with the EEI comments.

No
Tampa Electric is concerned that the time based VSLs for updating documentation are too severe based on the potential risk to the BES. We propose that updating documentation should be categorized to allow a longer period of time before moving from low to moderate VSL.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we recommend that the following be added to the Measures: or, a corporate level policy naming the CIP Senior Manager.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally Tampa Electric recommends changes to Guidelines and Technical related to Requirement R2: 2.2 3rd bullet: Identification of trusted and untrusted resources – Tampa Electric suggests a clarification of the definition of resources to indicate whether a resource is a person, a device, a system, or something else. 2.3: Are these bullets to be considered as requirements of the standard e.g. CIP005? 2.4: Monitoring and logging of egress will place undue burden upon the responsible entity. These bullets are not included in CIP-006 except for logging for visitor exit which is accomplished via the Visitor Control Program. Should they be including this guidance in CIP-003 or should this be included in the standard to which it is applicable? 2.9: Information Protection bullet 2 notification of unauthorized information disclosure. This does not appear to be a requirement of the standard.
No
Tampa Electric agrees with the comments submitted by EEI.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we note that the Measures—2nd bullet requires extensive recordkeeping with little security benefits.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we question whether this implies a signature form. Requiring a signed document for each change of an approver places an undue administrative burden. These updates should go through the Entity's normal approval process. Tampa Electric requests clarification of the first sentence of Requirement R5, specifically does this requirement apply only for those CIP requirements that have a "required approval"? For Measure M5 – 3rd bullet indicates that the CIP Senior Manager approves the delegations for physical security also. We recommend that this measure be re-stated to state that delegations be approved by a member of management or delegated by a member of management but not the CIP Senior Manager. For many organizations, personnel responsible for approvals will span many different departments, many of which may not be under the direct control of the CIP Senior Manager. This requirement places an undue burden on such organizations by requiring CIP Senior Manager's involvement in personnel changes for delegation throughout the organization.
No
Tampa Electric agrees with the comments submitted by EEI. Additionally we note a typo (from change2 to change 2) Please refer to comments in question 10 above related to undue burden.
No
Tampa Electric agrees with the comments submitted by EEI.
Yes
No
Tampa Electric agrees with the EEI comments. In addition, Tampa Electric considers that there will be an administrative burden (may have many versions of training programs tailored to individual roles). Maintaining such training programs, reporting, and compliance will be difficult with little additional security benefit to the Bulk Electric System.
No
Tampa Electric agrees with the EEI comments. Additionally, Tampa Electric is concerned over the statement in the Measures related to the identification of the date access was first granted, particularly for those individuals already in compliance with NERC CIP version 3 requirements since that was not previously tracked.

No
Tampa Electric recommends modification of this requirement to include the use of a National Criminal Research Database which would cover all of these requirements and show reasonable due diligence. Individual background verifications at all locations of residence, employment, and education is less thorough and creates more of an administrative burden for recordkeeping.
No
Tampa Electric recommends modification of this requirement to include the use of a National Criminal Research Database which would cover all of these requirements and show reasonable due diligence. Individual background verifications at all locations of residence, employment, and education is less thorough and creates more of an administrative burden for recordkeeping.
No
Tampa Electric agrees with the comments from EEI. In addition, Tampa Electric offers the following concern: The measures for 6.3 and 6.4 indicate that a Registered Entity needs to verify the list of who has access against a listing of those who have been authorized. The wording is unclear on what this means.
No
Tampa Electric agrees with the EEI Comments. Reassignments may also be processed retroactively, and the requirements should take this into account.
Yes
No
Tampa Electric agrees with the comments submitted by EEI. In addition, for Requirement 1.3 Tampa Electric requests that the SDT provide clarification on what is meant by “explicit access”. Rules can include group objects for cyber assets or port strings. Stating “explicit” could be construed to mean all objects or ports must be explicitly stated. Is it the SDT’s intent that an Entity must explain the specific criteria for each and every Cyber Asset granted access through the access point? Or is it sufficient to provide explanations for groupings of assets? Requirement 1.5 seems to indicate that an Entity would need IDS at each EAP (i.e., host IDS). The “Guidelines and Technical Basis” section has a very good statement concerning communications. The wording excludes serial, non-routable connections. This wording needs to be included in the actual requirement – similar to 1.2 and 1.3. Tampa Electric recommends that the requirement allow for technical feasibility exceptions or deployment of alternative measures of network based IDS where host based IDS may not be possible.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI on VRF and VSLs.
No
The language requires significant clarification. Tampa Electric agrees with the EEI comments.
No
Tampa Electric agrees with the EEI comments. The version lacks clarity.
No
Tampa Electric agrees with the EEI comments.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the changes proposed by EEI for Requirement 1.1. is a major clarification that greatly reduces the scope of ports that must be included for compliance.
No
Tampa Electric agrees with the comments from EEI for Requirement 2.1.
No
Tampa Electric considers that R3.4 introduces a cyber asset that Entities have not yet had to identify or account for. This will make it difficult to prove compliance. Please also refer to our concerns in the

definitions question 1 related to Transient Cyber Assets.
No
Tampa Electric agrees with the comments submitted by EEI for R4.3 and R4.4. In addition, Tampa Electric shares the following comments: 4.1 Tampa Electric is concerned that there are devices that do not produce the level of event logging that is required. Recommend adding “where technically feasible” to the requirement. 4.2 – Requires alerts for events, but fails to specify alerts for security. Recommend that the requirement state “Generate alerts for security events that…” 4.5-Requires a manual review of sample of logs every two weeks. This requirement provides no security benefit; it is unclear as to what an adequate sampling would be. The requirement is redundant, given the other requirements in R4, and should be removed entirely.
No
Tampa Electric agrees with the comments submitted by EEI. Requirement 5.2 could be interpreted that the CIP Senior Manager must authorize each individual use of administrator and shared default accounts rather than the individuals who have the authority to use those accounts. We suggest that the SDT delete this requirement.
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI. Additionally Tampa Electric proposes a format change on R 1.3 Measures as follows: Proposed format change o Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; ♣ BES Cyber Security Incident response personnel, ♣ BES Cyber Security Incident handling processes or procedures, ♣ Communications processes or procedures.
No
Tampa Electric agrees with the comments from EEI. For Part 2.2 Tampa Electric recommends that the Standards Drafting Team consider adoption of the Homeland Security Exercise and Evaluation Program described below: Rationale: The homeland Security Exercise and Evaluation Program https://hseep.dhs.gov/pages/1001_About.aspx#TerminologySection1 “There are seven types of exercises defined within HSEEP, each of which is either discussions-based or operations-based. Discussion-based Exercises familiarize participants with current plans, policies, agreements, and procedures, or may be used to develop new plans, policies, agreements, and procedures. Types of Discussion-based Exercises include: Seminar. A seminar is an informal discussion, designed to orient participants to new or updated plans, policies, or procedures (e.g., a seminar to review a new Evacuation Standard Operating Procedure). Workshop. A workshop resembles a seminar but is employed to build specific products, such as a draft plan or policy (e.g., a Training and Exercise Plan Workshop is used to develop a Multi-Year Training and Exercise Plan). Tabletop Exercise (TTX). A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures. Games. A game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedure designed to depict an actual or assumed real-life situation. Operations-based Exercises validate plans, policies, agreements and procedures; clarify roles and responsibilities; and identify resource gaps in an operational environment. Types of Operations-based Exercises include: Drill. A drill is a coordinated, supervised activity usually employed to test a single specific operation or function within a single entity (e.g., a fire department conducts a decontamination drill). Functional Exercise (FE). A functional exercise examines and/or validates the coordination, command, and control between various multi-agency coordination centers (e.g., emergency operation center, joint field office, etc.). A functional exercise does not involve any "boots on the ground" (i.e., first responders or emergency officials responding to an incident in real time). Full-Scale Exercises (FSE). A full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims). “
No
Tampa Electric agrees with the comments from EEI.
No
Tampa Electric agrees with the comments from EEI.

No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R1.
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R2.
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R3.
Yes
No
Tampa Electric supports the comments from EEI. Additionally, Tampa Electric submits the following comments for consideration: R1.1.3 Recommended language to requirement: “Any commercially available application software (including version) intentionally installed on the BES Cyber Asset for normal and emergency operation.” Measures: Tampa Electric considers that the language is unclear as to what are “required items” – Does this mean based on ports & services or normal/emergency operation of the asset? Suggest the following wording change: “required items as identified in R1.1.1 through 1.1.6 of the baseline configuration” R1.2 Propose that the CIP Senior Manager delegation be addressed. Delegation process as stated in CIP-010 creates an administrative burden for the CIP Senior Manager. Tampa Electric recommends that this measure be re-stated such that delegations be approved by a member of management or delegated by a member of management but not the CIP Senior Manager.
No
Tampa Electric supports the comments from EEI.
No
Tampa Electric supports the comments from EEI.
No
No
Tampa Electric agrees with comments submitted by EEI. In addition, Tampa Electric recommends the following: Add phrase “information protection” as follows: “Each Responsible Entity shall implement one or more documented information protection processes that collectively include each of the applicable…” R1.1 – insert “readily”, e.g., “One or more methods to readily identify…” R1.2 – table headings have typos (Part, Part, Part). Measures – 1st bullet – change to “Records indicating information that is stored, transported, and disposed of in a secure manner, consistent with the documented processes.” 2nd bullet – Current language: Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis; Proposed language: Records demonstrating that access to systems containing protected BES Cyber System information is implemented on a need to know basis. 1.3 - table headings have typos (Part, Part, Part).
No
Tampa Electric agrees with the comments submitted by EEI. In addition, Tampa Electric suggests the following: Insert ‘storage media re-use and disposal’ in front of ‘processes’. Also in the guidelines for R2, an analysis of whether a BES Cyber System can be released is mentioned – does this analysis need to be documented and stored as evidence? R2.1 Insert ‘storage’ in front of ’media’ in the requirement. For Measures, add phrase to sentence: “, or that information residing on the storage media is encrypted.” Definition in footnote should be added to definitions document. 2.2 Insert ‘storage’ in front of ’media’ in the requirement. For Measures, add phrase to sentence: “, or that information residing on the storage media is encrypted.”
No
R2 – lower VSL could be if process not documented but we are performing. Moderate VSL could be if process not followed in certain situations. VSLs should take into account extent of condition, e.g., 1 tape not degaussed – that shouldn’t be high severity.
No
Tampa Electric recommends that any requirements that are to be performed prior to or on the

effective date of the standard (“initially upon the effective date of the standard) be included in the Implementation Plan rather than in the body of the standards/requirements.
Individual
Michael Schiavone
Niagara Mohawk (National Grid Company)
Yes
There has been a significant change in the framework from version 4 to version 5 regarding definitions and core concepts such as Critical Assets, Critical Cyber Assets, etc. These proposed changes are not a requirement of FERC Order 706, do not enhance cyber security controls and create administrative burdens when migrating to version 5. There should be a correlation between BES Cyber Systems and the facilities that these systems serve. The current version of the CIP standards provides the correlation and recognize that systems (CCAs) do not operate independently of facilities (CAs). Therefore, applying physical and electronic controls is more transparent. We propose maintaining the current Critical Asset and Critical Cyber Asset definitions and concepts. High, Medium and Low categorizations can still be utilized with the legacy CA and CCA concepts. Regarding the use of the term “annual” throughout the standards, we suggest that the registered entity be allowed to maintain it’s own definition of “annual” based on CAN-0010 guidelines. 1) For all definitions please include the old term that the new term is replacing, as applicable 2) The time periods included in the first and second sentence of the definition of “BES Cyber Asset” are confusing. The 15 minutes discussed in the first sentence and the “delay” discussed in the second sentence are unclear. Suggest re-wording as follows: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The 15-minute period begins to run when the asset is operated, mis-operated, or fails to operate when necessary, regardless of the time period between the asset was degraded or misused and the time the asset is then operated, mis-operated or fails to operate when necessary. 3) BES Cyber System Definition - Maintenance Cyber Asset needs to be defined or if appropriate changed to Transient Cyber Asset
No
Yes
Yes
Yes
Yes
Yes
Yes
No
We recommend eliminating this requirement and moving it into CIP-004 R2 and include policy as part of the training required. This way, all awareness and training would be in CIP-004.
No
We propose retaining the current language in CIP-003-3 R2
Yes
There should not be a foot note in the standard – make this part of the requirement.
No
R.2 – We suggest a "Lower" VSL for "The Responsible Entity has implemented the required cyber security policy or policies but has failed to adequately document the policy or policies." R.4 – We suggest Lower to Severe VSLs be based on a failure to take action, rather than a specific number of

employees who are aware. As drafted, it would be a "high" violation to miss one single employee. That seems overly strict and does not match well with the requirement and measures, particularly when measures suggested includes making an internet posting. We suggest the following: "Lower" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but has not adequately documented the measures"; "Moderate" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 30% -50% of individuals who have access"; "High" VSL = "Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 50% -70% of individuals who have access"; and "Severe" VSL = "Registered entity has taken no measures to make any individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function OR Registered entity has taken measures to make individuals who have access to the BES Cyber Systems aware of the cyber security policies appropriate for their job function, but the measures were not designed to target 70% or more of individuals who have access" R.5 - Why do the VSLs begin at medium for the failure of one delegation? We recommend "Lower" VSL = failure of one delegation; Moderate = failure of two delegations; High = failure of three, and Severe = failure of "four or more". R.6 – We suggest VSLs structured similarly to CIP-002 - Lower = Change to one delegation was not documented within 30 days, but was documented within 31-41 calendar days of the effect vive date ; Moderate = Change to two-three delegations was not documented within 30 days OR change to one delegation was not documented within 30 days, but was documented within 42-52 days of the effective date; High = Change to three-four delegations was not documented within 30 days OR Change to one delegation was not documented within 30 days, but was documented within 53-63 days of the effective date; Severe = Change to more than four delegations was documented within 30 days of the effective date OR Change to one delegation was not documented within 74 days of the effective date.
Yes
No
We do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training on CIP, as required under current version, is all that should be required.
Yes
Yes
Yes
No
There is no added security by requiring the CIP Senior Manager or delegate to authorize access. We suggest using legacy wording that only requires access to be authorized.
Yes
No
It seems harsh to include the failure to document a security awareness program as a severe VSL. We recommend the following as a "Lower" VSL "The Responsible Entity implemented, but failed to document a security awareness program" and change the Severe VSL to "The Responsible Entity failed to implement and document a security awareness program." Additional comments around adding “Missed a quarter and/or target audience (authorized physical or authorized electronic)?” R.2: No comments. R.3: The annual training requirement assumes that the initial training was completed before access was granted, therefore, missing a small number of employees with the subsequent annual training does not necessarily indicate high risk to the bulk electric system because these employees presumably had received prior training when their access was granted. We recommend a tiered approach to the VSLs for missing the annual training requirement so that failing to meet the

annual requirement for a low percentage of employees (like 10% or less) is a lower VSL, failing annual requirement for between 11-20% is moderate, failing the annual requirement for 21-30% is high, and failing to meet the annual requirement for over 30% OR failing to do the initial training is severe. R.4: No comment R.5: A documentation error should not be a "severe" VSL. Delete the "OR/documentation" part from the Severe VSL and make a Lower VSL that reads "The Responsible Entity implemented, but failed to document a process for personnel risk assessments." R.6: For most utilities, there could be 100s of employees with access, and it seems unrealistic to base the VSLs on one failure with regard to one or two employees. We recommend changing the values in the Moderate - Severe to percentages of employees 10%, 20%, 30%or more. R.7: Same comment as R.6 - change values of one to three employees to percentages.
Yes
No
Requirement 2.2 specifies encryption for all Interactive Remote Access sessions, but does not specify where the encryption is required. If the intent is to require encryption from the user to the Intermediate Device the requirement should specify that clearly. Not all assets currently support encryption, so requiring encryption from the Intermediate Device to the Asset is not practical nor necessary if encryption is being employed outside of the ESP.
No
R.1 and R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
Yes
No
R.1: There should be lower VSL where the processes listed on the tables are implemented but not documented. Add to the Lower VSL: "OR the Registered entity has implemented but failed to document the required physical access controls" R.2: There should be lower VSL where the processes listed on the table are implemented but not documented.
Yes
Yes
No
Requirement 3.5 requires logging of each Transient Cyber Asset connection. This is not practical as many assets do not have the capability of logging when someone makes a direct physical connection to the asset. Many assets are not capable of logging to centralized logging systems. Also, in a typical day, and engineer in the field may connect a Transient Cyber Asset to many different assets and it would be impractical for one to log each connection.
No
4.1 - The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement. 4.3 - The activity level of some devices is such that they may not generate a logged event every day. Therefore, responding to an event failure with a day may not be possible. 4.3 & 4.5 – there is a conflict between these two. 4.3 requires a response to logging failures before the end of the next day. But, 4.5 requires bi-weekly sampling of logged events which would uncover logging failures. If the logs are being reviewed bi-weekly then logging failures may not be detected and responded to within the next day.
No

Items 5.4 & 5.6 in Table R5 includes the phrase “where technically feasible”. Does that mean a TFE will be allowed? If so, we believe that phrase should be removed and replaced with “as supported by the BES Cyber System” to eliminate need for TFE
No
R.1 We have the same comment here about percentages for open ports (similar theme from above). What is written in high should be in moderate. What’s in severe should be broken down by percentages/numbers. R.2 Consider severity of patch as recommended by the vendor and the percentage of assets that may not have had a remediation plan associated with that patch. R.3 Consider putting some wording in here around the percentage.
No
There is some concern that multiple plans would prevent one single entry point into the Cyber Security Incident Response Process. We’d like to make the argument that only one plan is necessary and supporting documentation can be created as necessary that supports that plan
No
The Applicability section of the tables refers to “All responsible entities”. We suggest using the same wording that all the other standards use (High Impacts, Medium Impact, Associated, etc) In R 2.2 In the first sentence, we recommend replacing the word “implement” with “exercise.” This is really about exercising the plan on a regular basis as the plan is already implemented. In 2.3, the "measure" for "relevant documents" does not give adequate guidance to the industry regarding what documents may be acceptable to demonstrate compliance. The "measure" indicates any "dated documentation related to" the reportable incident may be accepted. Please give some additional examples of the specific types of dated materials could be considered acceptable.
No
3.1 The terms “accuracy” and “completeness” are referenced but in terms of completeness there’s not a specific benchmark to compare the document again what should be quantified as complete. The suggestion is again to define a minimum set of information that would be expected in an Incident Response Plan. 3.2 - We recommend that clarity be added to ensure that language represents that review occurs 30 days after closure of the incident rather than invocation; rationale is that you might still be remediating and won't have learnt all lessons. We recognize the importance of the requirements to review the lessons learned, update the Incidence Response plan, and communicate the updates. However under the current structure it creates a rolling compliance effort following each incident. That is, an auditor will require that after each incident one has recorded lessons learned review, changes to the response plan or that none were necessary and updated communications or that none were necessary. It would be easier to update the plan on a quarterly basis based on the previous quarter’s incidents and not have so many auditable events to track.
Yes
No
1.5 – The requirement to preserve data for analysis or diagnosis may slow down the recovery process. There are times when recovery is urgent and must be done in a timely fashion. Is your intent to include this when you say “where technically feasible”? If so, language should be added spelling it out.
No
2.2 – We recommend removal of the phrase “and reflects current configurations” from the requirement. It is acceptable to have backup information that is less than current configuration and still perform a successful recovery. If this phrase is not removed, it will require a backup to be taken and tested for even the most minor configuration changes which is unnecessary.
Yes
No
We recommend the following VSLs for number of days until plan is reviewed in R3: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating plan. We also recommend the following VSLs for number of responsible personnel that the plan updates have not been communicated to: 1 person missed = Moderate, 2-4 = high and 5 or more is severe. We like the

VSLs in CIP-010 R3. These recommendations attempt to make CIP-009 R3 consistent to CIP-010 R3
Yes
Yes
No
We recommend considering emergency equipment replacement (partial outage) as “Exceptional Circumstances” . Based on the nature of our typical outages we would consider this practice to hinder the restoration efforts and bringing systems back on-line in a timely manner. We would certainly be good with language that allowed us to bring systems back on-line, ensure they are stable and then run a scan.
No
We recommend the following VSLs for number of days until documentation is updated in R1: 31-41 days = Lower, 42-53 days = Moderate, 53 plus is High and Severe for never updating documentation. R3 We like this structure. We’ve suggested this approach a number of times We aren’t talking about whether or not this is violation, but rather about the severity of the violation and then rating the severity. We think this is a really good approach.
Yes
No
The footnote here should be part of the requirement
No
We recommend the following VSLs on R 2: If the process to prevent unauthorized retrieval wasn’t done on 1 device that would be low 2-5 moderate, more than 5 is high
No
Due to the current status of version 4 (not FERC approved), there is potential for overlap of implementation with version 5 that could create extensive rework in a short period of time. This will cause an unnecessary expense to entities while not providing any additional cyber security benefit.
Individual
Jonathan Appelbaum
United Illuminating Company
Yes
• BES Cyber Security Incident – Proposed Change o Original Text – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or ♣ Results in unauthorized physical access into a Defined Physical Boundary. o Proposed Change – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or Defined Physical Boundary ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. o Rationale – The revised definition leverages legacy language from NERC’s ‘Glossary of Terms Used in NERC Reliability Standards,’ combining Electronic Security Perimeter and Defined Physical Boundary into the single bullet. It also raises ‘physical attempts to compromise’ into the category of BES Cyber Security Incident. • BES Cyber Security Incident – Proposed Change o Original Text – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or ♣ Results in unauthorized physical access into a Defined Physical Boundary. o Proposed Change – A malicious act or suspicious event that: ♣ Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or Defined Physical Boundary ♣ Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. o Rationale – The revised definition leverages legacy language from NERC’s ‘Glossary of Terms Used in NERC Reliability Standards,’ combining Electronic Security Perimeter and Defined Physical Boundary into the single bullet. It also raises ‘physical attempts to compromise’ into the category of BES Cyber Security Incident. o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and

Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact designations; equipment layouts that contain Medium or High BES Cyber System Impact designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – Information for Medium and High impact Bes cyber Systems location should be protected. This is consistent with the notion of protecting those assets that have greater impact on the BES and also all BES Cyber systems per CIP-002-5 have at a minimum a Low impact. • BES Reliability Operating Services – The services should focus on real time and hour ahead horizons. This horizon presents risk to reliability that requires immediate reaction. A service that occurs in the Current Day horizon can be reacted to in a reasoned and controlled manner. Additionally, what is Change Management as a reliability service? • Other terms which would benefit from definitions • Adverse - The SDT is utilizing the concept of "adverse impact" to properly scope High to control center cyber assets but the term adverse is not defined. UI is concerned that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS is not limited to the assets supporting the application and may extend into the substation and field RTU and devices. o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter ♣ Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • The services should focus on real time and hour ahead horizons. This horizon presents risk to reliability that requires immediate reaction. A service that occurs in the Current Day horizon can be reacted to in a reasoned and controlled manner. • Additionally, what is Change Management as a reliability service? • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent. • UI is concerned that the universe of cyber assets supporting a TOP/BA/RC SCADA or EMS is not limited to the assets supporting the application and may extend into the substation and field RTU and devices. The SDT is utilizing the concept of "adverse impact" to properly scope High to control center cyber assets but the term adverse is not defined.

No

1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. UI proposes Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and

Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. UI proposes that the phrase "BES Cyber Assets and BES Cyber Systems" used in this requirement be changed to "BES Cyber System". A single BES Cyber Asset may comprise a BES Cyber System. The Requirement should be to list the BES Cyber System and the impact categorization. This appears to match the diagram on page 7 that identified BES Cyber Systems. c. The phrase "placed in operation" requires clarification. Facilities (e.g. HVDC Converters, SVC, FACTs, Generators) are often initially tested and commissioned connected to the BES but are not in commercial operation. Being specific such as "placed in operation, post-commissioning testing". d. UI requests clarification on the composition of the list required by this Standard. A BES Cyber system may be composed of multiple BES Cyber Assets. Would this list only contain the single BES Cyber System , or the five BES Cyber assets, or the BES Cyber System with the five BES Cyber assets listed? For example a High impact Control Center has an EMS with 5 BES Cyber Assets in the Control Center (two servers and three workstations). For compliance to this Requirement is the EMS listed, or the 5 BES Cyber assets? e. UI requests on the requirement to update. If a single BES Cyber Asset is added to an existing BES Cyber System does that initiate the 30 day update process for the list? For example if a Control Center with a High Impact adds a single workstation to an existing EMS, does that require a 30 day update to the list? A workstation is not a BES Element or Facility, but is a BES Cyber Asset.

No

1. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems have been properly identified and categorized. 2. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale –Instances in which tasks are required to be completed in advance of the effective date of the standard should be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame. 3. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale –

The requirement only asks for Senior Manager (or delegate) approval. Instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1 – The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a 'High" VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. 2 – For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days
Yes
Yes
UI supports the Guideline for what a Policy should contain. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.
No
Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry. . Instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale –The scope as written would include visitors. UI does not believe that a visitor should be made aware of the CIP Policy or portions appropriate to the visitor's purpose.. Additionally, making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy. An Entity should make the Policy available for viewing. The awareness of the meaning Policy should be conducted in the CIP-004 training.
No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706) provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.

No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. Use a more gradual scale rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
No
From the Guidance "The security awareness program is intended to be an informational program, not a formal training program." But the Measure for R1 states "Evidence must include the documented security awareness program." UI observes that requiring a documented program as evidence conflicts with an informal compliance guidance. The Measure should state "Evidence may include a documented security awareness program, and additional evidence to demonstrate that this program was implemented such as, but not limited to, the quarterly reinforcement material that has been distributed."
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. UI proposes the following change to R2 to conform to the rationale box. As written R2 may not be clear that not all topics listed in 2.1 through 2.10 is applicable to each role. Proposed change "Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems. For each role identified by the Responsibility Entity only include the topics in CIP-004-5 Table R2 – Cyber Security Training Program that are applicable to that role." 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope.
No
Measure 3.1 where it calls for the date access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. R4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. Provide a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain 2. R4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. R4.3 a. UI favors a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' 4. R4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain

BES Cyber Assets remotely.
No
Version 5 standards should indicate whether previous PRA's would be valid for this requirement
No
1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary' a. 'Minimum necessary' as identified as difficult to prove within an audit context 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts which do not provide enhanced security and may impact reliability efforts when recovery processes are activate. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead.
No
1. R7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. R7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. R7.3 – a. Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled. b. Propose to include in Guidance that access to BES Cyber System Information is considered revoked for electronic storage is NOT dependent on revocation of user account to electronic files provided remote access has been revoked. Similarly if paper records or electronic access is contained in a controlled physical perimeter access to BES Cyber System Information is considered revoked once the credential to access the physical security perimeter is revoked".
Yes
No
The Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Requirements – Propose content change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points. 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed

Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.

No

1. Table R2 1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted is decrypted prior to allow for further access controls would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.

No

1. Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.

No

1. Table R1 a. R1.1 i. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – 'different and complementary' may not provide adequate guidance. Measure R1.3 only references 'different.' 1. Propose adding language to support single devices which may provide multiple access control measures (i.e. physical access card with PIN) ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Applicability – Presently states Associated Physical Access Control Systems. Is it Physical Access Control Systems Associated with all Low, Med, and High Bes Cyber Systems? I understood that wherever the Applicability uses Associated that there would be a Low/medium or High BES cyber system designation also. ii. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals

responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.

Yes

No

Table R3 1. R3.1 a. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.

Yes

The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5

No

R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.

No

R2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for all related software and firmware associated with BES Cyber System or BES Cyber Assets. c. Rationale - Only security updates to software and firmware should be sourced. It is possible that at some point

security updates for a product will be sourced from a separate repository from non-security updates. 2. Measures – Propose striking the last sentence “The list could be sorted by BES Cyber System or source.” It introduces additional requirements with no clear security benefit or alignment with FERC Order 706.

No

1. R3.2 – Although CIP-007 v3 currently requires mitigation, UI believes that the actions to respond to a Virus (disarm or remove) is part of the CIP-008 Response Plan. The SDT used this approach in proposed R4.5. 2. R3.3 a. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). b. Measures – Format (i) and (ii) to a bulleted list signifying ‘or’ criteria 3. R3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. R3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append “to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets” to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.

No

R4 1. R4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE’s are not required in instances in which devices cannot log a particular event. 2. R4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of ‘real-time’ as it presents concerns demonstrating compliance. 3. R4.3 a. Requirements – Content Change i.

Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. R4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. R4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No

R5 1. R5.1 a. General Comment – The act of being presented a Log-On screen means that a person has accessed the BES Cyber System. The requirement should allow access to a BES Cyber System to perform the log-on/access process. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of technically feasible was made as technical capabilities currently in place may not adequately demonstrate compliance with this. 2. R5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. R5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. R5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identify the multiple methods which can be used to mitigate default passwords. 5. R5.5 a. Requirements i. Change BES Cyber Systems to BES Cyber Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. 6. Please be consistent with the use of Term BES Cyber System versus BES Cyber Asset.

No

Violation Severity Levels 1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial

paragraph doesn't align with a requirement, propose striking.
No
1. General – Guidance or definitions should be provided to illustrate the expectation of this Standard. An Response Plan may solely contain the organizational structure, roles and responsibilities, and process to respond to an incident; but not include the specific steps required to resolve a specific type of incident on a specific BES Cyber Asset. For example I can describe an incident response for removing malware on a windows machine without being any more specific then contact Information technology group to remove Malware. 2. R1.1 1. Applicability – Content Change 1. Original Applicability ♣ All Responsible Entities 2. Proposed Applicability ♣ High Impact BES Cyber Systems ♣ Medium Impact BES Cyber Systems ♣ Associated Physical Access Control Systems ♣ Associated Electronic Access Control and Monitoring Systems ♣ Associated Protected Cyber Assets 3. Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 3. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
1. R2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No

1. R3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rational – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. R3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. R3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.

No

No

• Overall 1. References to ‘implement’ should be changed to ‘exercise’ regarding recovery plans to better capture activation of the plan vs. ‘release and publish’ efforts. 2. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. R1.3- Remove protection from requirement because protecting information is covered in CIP-011. Proposed language: One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality. For R1 Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance R1.4 The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rational – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. R1.5 Original Content – Preserve data,

where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. General Comment: Please provide Guidance: Does the Recovery Plan for each BES Cyber System require to be tested each year, or only one Plan. For example the EMS system will have a Recovery Plan, and the associated Physical Access Control System will have a recovery Plan, so do both plans get exercised each year or only one Plan. R2.1 1. Requirements Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. R2.2 Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. R2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? R2.3 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
1. R3.1 Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. R3.2 Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. R3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit.
Yes

No
1. R1.1- In General UI does not agree with the addition of the new requirement. The existing Change Management requirement in CIP-003-3 is sufficient. The proposal is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1 And R1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 3. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 4. R1.4 What is the meaning and scope of cyber security controls 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.
No
R2.1 1. Applicability – Propose removal of Medium Impact BES Cyber Systems. ♣ Rationale – The

technology required to monitor/detect for changes is relatively new and not aligned to BES Cyber Systems which would be in place within a Medium Impact facility (substations, etc.). 2. Requirements – Propose content change ♣ Original Text – Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010_ R1, Part 1.1) and document and investigate the detection of any unauthorized changes. ♣ Proposed change – Where technically feasible, detect and document unauthorized changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1).
No

R3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rational • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rational – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. R3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. R3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes
No
R1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed

Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.2 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.3 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R1.3 Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. R1.3 Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No

R2.1 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. R2.1 Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of

BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. R2.2 Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.

No

No

References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. Implementing version 5: The implementation period should be no less than 24 months however it is impossible to propose a likely implementation period until the final basket of requirements take shape. The reasoning to support the minimal 24 months is that certain changes will require a capital expenditures and equipment acquisition. The SDT should consider that new capital expenditures require inclusion with the next budget cycle and then the process to procure and implement/install new equipment. Actions cannot be started until FERC completes its rulemaking process to define the basket of actions to take. Second, the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions will require some Entities to create solutions from clean slates. . In the event that Low Impact assets are a component of the enforceable requirements on day 1 it is likely that additional time would be required. Finally, Entities currently subject to CIP standards are managing a zero defect CIP program and possible preparing for audits while implementing version 5. Planned Changes: UI agrees that if when an Entity plans a change the impact on BES Cyber System designation should be considered and any required security upgrades and CIP items should be completed prior to the Change. In some requirements that require periodic activity it would not increase security to force the activity outside the Existing Entities Schedule. For example, many entities rely on a consultant to perform a cyber vulnerability assessment once per year. This implementation plan would require a separate cyber vulnerability assessment on the new asset prior to placement into operation which will result in the additional expense of multiple assessments per year. Unplanned Changes in Impact designation: UI is concerned with unplanned changes. Changes to impact designations may require significant investment in equipment, process documentation, and personnel to implement a cyber security program and the compliance obligations. Every circumstance and situation can not be anticipated in the implementation plan. UI proposes that additional guidance is provided to state that the obligation to be compliant begins 12 months after notification, and an Entity that can not fully meet its compliance obligation will file a single mitigation plan with it Regional Entity providing a plan and timeline to come into compliance with each of the requirements.

Individual

Joe Petaski

Manitoba Hydro

Yes

-BES Cyber Asset: Some devices, such as digital relays, may operate independently, and neither send nor receive "instructions". It is unclear that an output contact status change would be considered an "instruction". -BES Cyber System: Maintenance Cyber Asset is not defined. Should this be Transient Cyber Asset? -BES Cyber System Information: The same phrase that applies to floor plans and equipment layouts – “that contain BES Cyber System Impact designations” – should also be added after “network topology or similar diagrams”. It is difficult to know how prescriptive the three examples are within the parentheses. Use the same wording used extensively throughout the CIP

standards: “Examples may include, but are not limited to: network addresses, security patch levels, list of logical network accessible ports.” -Dynamic Response to BES Conditions Operating Service: This definition is complex and inconsistent in approach. Parts of the definition are too specific, such as Protection Systems - Current, frequency, and phase. These are input quantities to Protection Systems, and we suggest that this line be deleted. Parts of the definition are too broad - Monitoring and Control - All methods of operating breakers and switches. Does this include manual operation? For clarity and consistency, we suggest using the NERC definition of Protection System instead of the term relay protection, and also remove the bullets which detail "sensors, relays & breakers". We suggest replacing "x-former" with the word "transformer". -CIP Exceptional Circumstance: Please clarify the meaning and intent of the phrase "an impediment of large scale workforce availability". How would this be measured? -Electronic Access Control and Monitoring Systems: It’s unclear whether only the monitoring of access to ESPs and BES Cyber Systems is meant, or all monitoring of ESPs and BES Cyber Systems (including for example the monitoring for malware). Suggest rewording to “Cyber assets used in the control or monitoring of electronic access to Electronic Security Perimeter(s) or BES Cyber Systems.” -Electronic Access Point (EAP): This definition is too broad and it should focus on BES Cyber Asset Protection. Suggest change for “between Cyber Assets” to be “to BES Cyber Assets”. -External Connectivity: Since the term “external connectivity” is not used anywhere in the standards, delete this definition. -External Routable Connectivity: When determining whether external connectivity is routable, is the Responsible Entity required to check only the parts of the communication system that it administers, or is it also responsible to investigate whether a routable protocol is in use anywhere within the communication systems of its communication service providers, even though those communication systems have been exempted from the CIP standards? This definition is unclear. Suggest the following wording: “The use of a routable protocol through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.” -Interactive Remote Access: The sentence "Remote access can be initiated from: ... contractors and consultants." is guidance information, and restricts the definition to only applying to Responsible Entity Cyber Assets, employees, vendors, contractors, and consultants. By definition, this would exclude interactive remote access by anyone else (public, non-legitimate users) from scope. We suggest removing the last sentence and providing this information in a guidance document. -Intermediate Device: As currently written, an Intermediate Device may perform none of the functions listed. We suggest “A Cyber Asset that performs one or more of the following functions: provides the required multi-factor authentication for the interactive remote access; or provides a termination point for required encrypted communications; or restricts interactive remote access to only authorized users.” The sentences “Intermediate devices are sometimes called …. Or in a DMZ network…” are examples which should be moved to the guidance section. -Physical Access Control System: This definition should be consistent with Electronic Access Control or Monitoring Systems. Suggest to added “monitoring” into the title and the definition. -Protected Cyber Asset: Protected Cyber Asset: Please clarify to what the Cyber Asset is connected. The BES Cyber System? To a device outside the ESP? To any device in the ESP? -Reportable BES Cyber Security Incident: A BES Cyber Security Incident has already been defined. How BES Cyber Security Incidents should be handled, including whether they should be reported is better described within the standard than in a definition. -Transient Cyber Asset: Please clarify the meaning of "directly connected" is unclear.
Yes
-Attachment I 1: High Impact Rating (H): We suggest deleting " ... that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services ...", since the phrase is included in the definition of BES Cyber System. Repeating that phrase is redundant and does not capture all the details in the definition. We suggest removing the phrase to improve clarity and readability of High Impact Rating. Attachment I 1 requires the High Impact asset / system to be located at EACH (i.e. every) Control Center or Back-Up Center. Is this really what was intended? If not, “each” should be replaced with “a”. -Attachment I - 1.3 & 1.4: It is not reasonable that a control center is classified as (H) High Impact Rating asset if it controls one or more Medium Impact Rating assets as defined in Section 2. As written, if a utility Control Center only controls a single Medium Impact Rating generation asset and some Low Impact Rating generation assets, its Control Center becomes a (H) Control Center that has the same classification as a large Transmission Owner Control Center facility! We suggest changing from “includes control of one or more of the assets...” to “includes control of two or more of the assets…” in Section 1.3 and 1.4. -Attachment I 1.4: The reference to 2.12 should be deleted. Underfrequency load shedding and undervoltage load shedding is not applied at generation, and the underfrequency load shedding

standards and undervoltage load shedding standards (PRC-006 through PRC-011) are not applicable to Generator Operators. -Attachment I 2.1: To improve clarity and readability, we suggest the wording "Generation facilities ..." -Attachment I 2.2: To improve clarity and readability, we suggest the wording ... "Facilities with an aggregate ..." -Attachment I 2.5: It is unclear from this criterion and the accompanying diagrams as to what the "generation unit to be started" would be in the case of a generating station which has multiple units but only some are designated as blackstart. -Application Guidelines Transmission Part 2.6: If the guidance describing the categorization of the collector bus for a generating plant is an exception to the 500kV criteria, then this should be clearly stated in the actual requirement, not only indicated in the Guidelines. -Attachment 1 2.7: The intent of this criteria was based on considering average MVA ratings of lines and considered that loss of 3-1300 MVA 345 kV lines should be similar to 5-700 MVA 230 kV lines. Calculating the weighting factor for 5-230 kV lines (3500), 3-345 kV lines (3900), and presumably 2-500 kV lines (4000), it seems that an appropriate bright line criterion is 3500 MVA. Rather than use an arbitrary average MVA rating, it is suggested that the drafting team permit actual line ratings to be used and to have the Planning Authority or Transmission Planner calculate the total MVA of the substation. The responsible entity could draw a circle around the entire substation and add up the MVA of each transmission line between 200 and 499 kV. If the total MVA exceeds 3500 MVA then the substation has a medium impact. At Manitoba Hydro, our 230 kV lines have average MVA ratings around 300-400 MVA. Loss of substation with five 230 kV transmission lines does not have an Adverse Reliability Impact. However, using the proposed methodology, considering a 700 weighting factor, several substations in Manitoba would be classified as having a medium impact. In addition, it is unclear in this criterion as to whether the intention is to capture only station level cyber systems or whether it is also intended to capture cyber systems associated with the transmission lines which caused the impact assessment in the first place. The concern is that transmission line protection cyber systems may require the identification of assets located at facilities other than the originally identified facility and it will very quickly multiply the number of stations requiring compliance. -Attachment I 2.13: Should "generation control centre" be" generation Control Centre", as used in the Application Guidelines, or does " generation control centre" have a different meaning than "Control Centre"? The Application Guidelines indicates that the 300 MW threshold for generation control centres is the same value used for the UFLS and UVLS. This is not a valid equivalence. UFLS and UVLS programs "provide last resort system preservation measures" and "provide system preservation measures", as stated in the purpose of NERC standards PRC-006 through PRC-011. The reliability impact of 300MW during abnormal system conditions which require underfrequency or undervoltage load shedding is significantly different than the reliability impact of 300MW under normal system conditions. Even if 300MW is an appropriate CIP impact threshold for UFLS and UVLS systems, it is not automatically appropriate for generation control centres. It is also unclear what is the difference in reliability impact of a 300MW generation control centre, a 300MW generating station, or a 300MW generating unit. The generation control centre concept needs to be revised.

No

-R1: To improve clarity, we suggest expanding the language when referring to several levels of impact or assets and systems. As currently written, "High and Medium Impact" could be interpreted as meaning an asset or system which is both High and Medium Impact. The same interpretation could be applied to BES Cyber Assets and BES Cyber Systems. To clarify, we suggest the wording "... High Impact BES Cyber Assets, High Impact BES Cyber Systems, Medium Impact BES Cyber Assets and Medium Impact BES Cyber Systems ..." We suggest this change be adopted in all applicable CIP standards. -R 1.1: If this requirement was intended to apply to changes to BES Elements and to changes to BES facilities, then this sentence should be reworded to refer to "a change to BES Elements OR Facilities…". As drafted, the change would have to be to both a BES Facility and Element before the requirement applies. From a grammatical perspective, the phrase "IS placed into operation" should be "BEING placed into operation". -M1: There are no controls specified in CIP-002-5. It is unclear how categorization of Low Impact would be measured.

No

-R2: If R2 was intended to require the CIP Senior Manager or delegate to approve the identification and categorization changes as per R 1.1 within the 30 day period, then this section needs to be clarified. As drafted, the CIP senior manager or delegate is only required to approve the change within the calendar year. -R2: For clarity, we suggest changing " ... even if it ... " to "... even if the Responsible Entity ...". -M2: We suggest changing "... records to demonstrate ..." to "records which

demonstrate ...". -M2: For clarity, we suggest changing " ... even if it ... " to " ... even if the Responsible Entity ...".
Yes
No
-R2: This requirement is too vague. The phrase “represents the Responsible Entity’s commitment “is unclear. Is the policy intended to document the Responsible Entity’s procedures for implementing CIP standards related to the itemized topics, or is it intended to be broader than standards- related requirements? Can the policy state general policy goals, but not detail the procedures? We suggest incorporating the language in the current CIP-003-4 "The cyber security policy addresses the requirements in Standards CIP-002-5 through CIP-009-5, and CIP-010-1, and CIP-011-1." Also, for clarity, we suggest changing “remote access” to “Remote Electronic Access". -Guidelines R2: Bullet "Identification of possible disciplinary action for violating this policy", and any similar statements should be deleted. Internal disciplinary actions for policy violations are not NERC reliability compliance issues. -Guidelines R2 Item 2.4: We suggest changing "ingress and egress" to "access and exit (for visitors only)" since monitoring of exit is only required for visitors, as per CIP-006-5 R2 Part 2.2. Guidelines R2 Item 2.8: The term "break-fix processes" is unclear.
No
R3: It does not state the purpose of the review or any action to be taken as a result of the review, yet the stated Rationale refers to ensuring that the policy is kept up to date. If that is the intent, then the requirement should state that the policies must be updated, presumably to reflect changes that have occurred since the last year‘s review / adoption. However, MH notes that this implies that R2 would then be interpreted to mean that the policy being implemented need not be kept current. This requirement needs to be clarified as between R3 and R2.
No
R4: Awareness of the policies should also include individuals who have access to BES Cyber System Information, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.
Yes
Yes
No
Measures 1.1: The reference is no longer to ‘may include’ but to ‘must include’ and ‘acceptable evidence’ – are these references an intentional shift from the ‘may include’ language?
No
-Measures 2.1: The reference is no longer to ‘may include’ but to ‘must include’ and ‘acceptable evidence’ – are these references an intentional shift from the ‘may include’ language? -R2 - Applicability: The Applicability for the training program in R2 should match the implementation of the training program in R3. -R2.7: Please clarify "associated notifications". Do the "associated notifications" refer to CIP-008-5 R1 Part 1.3?
No
-R3: To provide consistency with the language in R2, please specify which assets are in the scope of Requirement R3. -R3.1: “Access” should be “electronic or unescorted physical access”. -R3.2: It seems to be missing the words ‘between training’ at the end of the requirement.
No
-R4 - Applicability: The Applicability for the personnel risk assessment program in R4 should match the implementation of the personnel risk assessment program in R5. -R4.1: It fails to specify what ‘initial’ means – is it upon hiring? Upon access being granted?
No
-R5 - Applicability: The Applicability for the personnel risk assessment program in R4 should match

the implementation of the personnel risk assessment program in R5.
No
-Rationale for R6: for clarity, we suggest "... perform such grants and is included in the delegation process referenced in CIP-003-5." In the second paragraph, we also suggest "... against records of individuals authorized to access the BES Cyber System...." -6.5 Requirement: It is unclear if "all accounts" refers to system level accounts or cyber asset accounts. -R6.6: For clarity, we suggest changing from "Verify ... of access privileges ..." to" Verify … access privileges"
No
-R7.1: The extenuating circumstance clause within R7.5 should be included for all parts of Requirement 7. An example of why this would be required would be where an employee resigns at the end of the day with no notice, this would make meeting R7.1 virtually impossible. -R7.2: We agree with a timely access review for reassignments and transfers. To provide more clarity, as well as consistency with the Measures, Rationale and Guidance, we suggest changing "revoke" to "review", and adding more text as follows: -For reassignments or transfers, review the individual's needs for electronic and physical access to BES Cyber Systems by the end of the next calendar day. Document and implement a revocation plan, including dates. -R7.3: For clarity, we suggest changing "access" to "electronic access or unescorted physical access". -R7.4: More than 30 days may be required for access revocation conducted through manual processes. We suggest an entity defined revocation schedule for manual revocation processes. -R7.5: More than 30 days may be required for access revocation conducted through manual processes. We suggest an entity defined revocation schedule for manual revocation processes. It is unclear if the password change is at a system or cyber asset level. Shared account password changes may not be technically feasible for all cyber assets.
No
-Rationale for R1: To improve clarity, we suggest changing " ... external boundary ..." to "... external electronic boundary ..." -R1: In R1 and R2, all requirements should refer to applicable "requirements" in a table, rather than "items" in a table. -R1.2: As written, R1.2 requires that ALL ROUTABLE connectivity for a BES Cyber System must be controlled through the use of EAPs, which would INCLUDE routable connectivity between BES Cyber Assets in the same BES Cyber System. If the intent is to address external connectivity outside of the ESP, we suggest changing "…routable and dial-up connectivity" to "…routable and dial-up External Connectivity." -Measures: The wording in the Measures is unclear. Regarding the bullet "A list of uniquely identifiable Cyber Assets within the BES Cyber System and associated EAPs ": is this a list of Cyber Assets which comprise the BES Cyber System and a list of the EAPs on those BES Cyber System, which does not include Protected Cyber Assets; or is it a list of Cyber Assets which comprise the BES Cyber System and a list of Cyber Assets within the EAPs, which includes the Protected Cyber Assets, but is not a list of EAPs? -R1.3: Corresponding with the EAP asset level approach for ALL routable and dial-up communications in Item 1.2, this requirement would apply explicit permissions at each communications interface (EAP) for each device in a BES Cyber System. This may not be necessary or possible for all devices within a BES Cyber System. If the intent is to address external connectivity outside of the ESP, we suggest changing "…using routable protocol" to "…using external routable connectivity". In addition, it seems more appropriate for "including" to be "and" as people would think of establishing criteria for granting permission as a separate requirement from requiring permission at EAPs. -R1.5: We disagree with the requirement prescribing malicious communication detection. Change Rationale: It is not apparent from FERC Order 706, p 496 - 503 that the two distinct measures "is not simple redundancy of firewalls". The Order in p 501 does state that "... The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity has at least two security measures unless it is not technically feasible to do so. The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment." Based on the direction in the Order, the Responsible Entity should have some flexibility in determining the appropriate second security measure, and should be allowed to claim a TFE if necessary. In addition, we suggest the wording "Document and implement a method ...." to provide consistency with the other requirements.
No
-R2: We suggest adding " ... and Associated Protected Cyber Assets, Electronic Access Control or Monitoring System, and Physical Access Control Systems ..." -R2.1: The meaning of "... directly

access ... " is unclear. Also, there are no requirements for remote access management for Electronic Access Control or Monitoring Systems, and Physical Access Control Systems. We suggest that remote access management be applied to these systems. -R2.1: As written, R2.1 requires that ALL ROUTABLE connectivity for a BES Cyber System include an Intermediate Device. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity." -R2.2: As written, R2.2 requires that ALL ROUTABLE connectivity for a BES Cyber System include encryption for all Interactive Remote sessions. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity." -R2.3: As written, R2.3 requires that ALL ROUTABLE connectivity for a BES Cyber System include multi-factor for all Interactive Remote sessions. If the intent is to address external connectivity outside of the ESP, we suggest changing the applicability to Cyber Systems with "…routable and dial-up External Connectivity."

No

-R1.1: Applicability and Requirement: Associated Physical Access Control Systems (for High and Medium BES Impact Cyber Systems) are not required to be located in a Defined Physical Security Boundary while the High and Medium Impact BES Cyber Systems must be in a Defined Physical Security Boundary. It is inappropriate to use the Associated Physical Access Control Systems in the applicability for R1.1. This approach is inconsistent with the other requirements and standards since the Associated Physical Access Control Systems do not have any identified High Impact BES Cyber Systems or Medium Impact BES Cyber Systems. High Impact BES Cyber Systems and Medium Impact BES Cyber Systems should be added to the Applicability. -R1.2 - Applicability: CIP-006 local definition of Associated Electronic Access Control or Monitoring Systems and Associated Protected Cyber Assets is for both High Impact BES Cyber Assets and Medium Impact BES Cyber Assets. This applicability will lead to confusion (especially considering how R1.3 is written) with respective High Impact BES Cyber Assets requiring protection under R2 & R3. We suggest changing from "Associated Electronic Access Control or Monitoring Systems" and "Associated Protected Cyber Assets" to "Associated Electronic Access Control or Monitoring Systems associated with a corresponding Medium Impact BES Cyber System" and "Associated Protected Cyber Assets associated with a corresponding Medium Impact BES Cyber System". -Associated Physical Access Control Systems should require equivalent access controls (as they do under the CIP-006-4c) to the Medium (or High under R1.3) Impact BES Cyber Systems. We suggest adding" Associated Physical Access Control Systems associated with a corresponding Medium Impact BES Cyber System" under the Applicability to make the Associated Physical Access Control Systems have the same measures as Electronic Access Control or Monitoring Systems. -R1.2 – Measures: The reference to egress should not be included in the measures. The requirement only refers to access. -R1.3 – Applicability: We suggest changing from "Associated Electronic Access Control or Monitoring Systems" and "Associated Protected Cyber Assets" to "Associated Electronic Access Control or Monitoring Systems associated with a corresponding High Impact BES Cyber System" and "Associated Protected Cyber Assets associated with a corresponding High Impact BES Cyber System". -Associated Physical Access Control Systems should require equivalent access controls (as they do under the CIP-006-4c) to the High Impact BES Cyber Systems. We suggest adding" Associated Physical Access Control Systems associated with a corresponding High Impact BES Cyber System" under the Applicability to make the Associated Physical Access Control Systems have the same measures as Electronic Access Control or Monitoring Systems. -R1.3: "Where technically feasible" should not be necessary for High Impact BES Cyber Systems as the requirement should be achievable for the High Impact BES Cyber Assets. -Secondly, if "where technically feasible" is deemed to be a necessary part of the requirement, then we suggest "... establish one or more Defined Physical Boundaries, where technically feasible, that restricts ..." so that "technically feasible" does not apply to the portion of the requirement associated with authorized users. -R1.3 – Measures: The reference to egress should not be included in the measures. The requirement only refers to access. -R1.3 – Change Description: For clarity, we suggest "FERC Order 706 p575 directives are addressed by providing the examples of physical security defense in depth via multi-factor authentication or layered defined physical security boundary(s) in the guidance document." -R1.4: We suggest changing "access through any access point" to "entry into each defined Physical Boundary protecting applicable BES Cyber Systems, Protected Cyber Systems, and Access Control and Monitoring Systems ...". The suggested change creates a more general statement which allows the

entity flexibility in implementation, and is consistent with the language in Part 1.6. -R1.6: We suggest changing "date" to "date and time", which would better support investigations.
No
-R2 Rationale: For clarity, we suggest "To provide access control when personnel without authorized unescorted physical access are in any Defined Physical boundaries as applicable in Table R2." -R2.2: For clarity, we suggest "... the first entry and the last exit ...", and "... the visitor's name, and the individual contact personnel's name."
No
-R3.1 - Applicability: Capitalize "Locally mounted hardware ... Boundaries" as indicated in the Background Applicability section. -R3.1: For clarity, we suggest “Prior to placing in service,”.
No
-Table of Compliance Elements, R1 – Lower VSL: R1.7 that is referred in this table doesn’t exist in CIP-006-5 Standards. -Table of Compliance Elements, R1 – High VSL: “15 minutes” timeline is referred from R1.6, but R1.6 doesn’t have such a timeline.
No
Introduction - Purpose: Does "unavailability" refer to the BES Reliability Operating Services, or to the BES Cyber System? We suggest changing "... availability ..." to "... availability and integrity ..."
No
-R2.1 - Measures: An entity should be allowed to group like BES Cyber Systems and BES Cyber Assets for patch monitoring. In general, the information provided in the measures is guidance, and should be moved to the Guideline section. -R2.2: “a defined timeframe” is not clear. Who defines the timeframe, the identified source or Responsible Entity?
No
-R3.1: We suggest changing "... prevent malicious code ..." to "... prevent addition of malicious code ...”. -R3.2: Suggest rewording to “Disable, quarantine, or remove identified malicious code. -R3.3: We suggest that the Responsible Entity be permitted to define a time interval for the signatures or patterns which are updated through manual processes. These BES Cyber Systems are typically isolated from any communication network, and therefore at lower risk. -R3.4: Suggest changing from “when connecting them to BES Cyber Assets or Protected Cyber Assets” to “when connecting them to applicable BES cyber Assets or Protected Cyber Assets”. -R3.5: The purpose and value of logging each Transient Cyber Asset connection is unclear. While R3.4 improves the security of BES Cyber Systems, R3.5 does not improve security, and as such R3.5 should be deleted. Note that the requirement for Acceptable Use banners has been removed for a similar reason.
No
-R4.1: Suggest changing from “Cyber Security Incident” to “BES Cyber Security Incident” to ensure that the glossary’s definition is being used. -R4.1 – Measures: We suggest changing "... paper ..." to a more generic term "... manual ..." -R4.3: Event logging should refer to R4.1, otherwise it is too broad. How and when is the event logging failure detected? Suggest wording: “Activate a response to event logging failures before the end of the next calendar day when detected.” -R4.5: We suggest improved clarity by removing the word "unanticipated". The term "event logging" is too broad and should refer to R4.1. For clarity, we suggest "Before the end of the next calendar day, activate a response to rectify any deficiency identified from the review."
No
-R5.1: We suggest adding "where technically feasible". For example, for some High Impact BES Cyber Assets, their user electronic access is only a front panel which does not require any credentials (e.g. frequency deviation meters used for AGC). It is unclear how grouping this cyber asset into a BES Cyber System could be considered to make it compliant with R5.1, so a Technical Feasibility Exception would be required. -R5.4 – Applicability: The use of "All Responsible Entities" in the Applicability column of the table is confusing. Are these the entities identified by Functional Entities in Section 4 Applicability, or are the "All Responsible Entities" defined by the bullets in Section 5 Background Applicability? To maintain consistency and clarity with all the other requirements, we suggest replacing "All Responsible Entities" with the specific Cyber Assets in scope, for example, BES Cyber Assets. -R5.6: The wording is unclear. We suggest "A process to limit the number of unsuccessful authentication attempts or generate alarms after a threshold of unsuccessful login attempts, where technically feasible.

No
-Rationale for R1: To create a complete sentence, we suggest "Incident reporting and response planning ensures consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems." We also suggest changing "exploited" to "discovered", since not all incidents involve exploits. The Summary of Changes has not been completed. -R1.1 – Measures: under Measures, the last portion of the sentence beginning 'targeting…' does not seem necessary. It overlaps with, and encompasses part of, the definition of Cyber Security Incident. -R1.2: A BES Cyber Security Incident has already been defined. How BES Cyber Security Incidents should be handled, including whether they should be reported is better described within the standard than in a definition. We suggest moving the Reportable BES Cyber Security Incident to here. -R1.2 – Measures: The word 'also' at the end of the sentence should be deleted. -R1.3: For clarity, we suggest "Incident communication plans which include internal staff and external organizations."
No
-R2: Specific responses to Cyber Security Incidents should not apply to Low Impact BES Cyber Systems due to the large number of systems included and their low impact. By the definition, entities are required to treat all malicious or suspicious events resulting in unauthorized physical access into a Defined Physical Security Boundary as a BES Cyber Security Incident. This imposes an unnecessary burden on the entities and provides little value. -R2.1: For clarity, we suggest rewording for R2.1: "When a Cyber Security Incident occurs, the incident response plans must be used and include recording deviations from the plan during the incident." -R2.2: The word "full" in the phrase "full operational exercise" is unclear. Since even tabletop exercises are allowed, it should also be allowable to run an operational exercise that is somewhat limited in scope. Suggest removing the word "full" from both the Requirement and the Measures. -R2.2 – Measures: The words 'between executions of the plan(s)' should be added after 'not to exceed 15 months'.
No
-R3.1: the words 'the plan' should be added after 'update' -R3.1 – Measures: The words 'between reviews' should be added after 'not to exceed 15 months'. -R3.2: Since the definition of a BES Cyber Security Incident is very broad (i.e. it includes all suspicious events, all attempts to compromise an ESP, all attempts to disrupt a BES Cyber System), it is likely that many of them will be detected (e.g. port scans at a firewall). Suggest adding language whereby a Responsible Entity may document for itself criteria of which types of BES Cyber Security Incidents it will review.
-Table of Compliance Elements, R1 – the language in this table does not seem to match the language of the requirements exactly which leads to lack of clarity. Under Severe VSL, second paragraph - the words 'include a process to identify' should replace the words 'identify'. -Table of Compliance Elements, R2 –There does not seem to be any violation for failing to test the response plan upon the effective date of the standard – is this intentional? If not, the words 'upon the effective date of the standard' should be added. Table of Compliance Elements, R3 – High VSL – the first paragraph references a 30 day timeline for updating the response plan, but the requirement itself references 60 days. Need clarification. -Table of Compliance Elements, R3 – Severe VSL – the last paragraph is missing the requirement that the communication occur with 30 days of the completion of the update of the plan – is this intentional? If not, the 30 day timeline should be added.
No
-Title: We suggest changing "Systems" to "BES Cyber Systems". -Purpose: The apparent purpose of CIP-009-5 addresses more than just the "... storing of backup information ...". We suggest that the Purpose be revised to more fully reflect the intent of the standard. -Rationale for R1: Not all incidents involve weaknesses that were exploited. We suggest changing "exploited" to "discovered". For added clarity to the Summary of Changes, we suggest the wording "Added data protection provisions to facilitate event investigation after activation of the recovery plan." -R1.4: We suggest the wording "Process for the identification of information essential to BES Cyber System recovery that is stored on backup media." The statement "shall be verified ... successfully..." should indicate that the process is included in the plan, since the act of verification is addressed in Table R2 Part 2.2. The measure for R1 Part 1.4 should be revised to agree with the information identification and verification process. -R1.5: For clarity, we suggest changing "Preserve data ..." to "Process for preserving data,". -R1.5 – Measures: the word 'important' is unnecessary.
No

-R2.1: The need for the word “full” in the phrase “full operational exercise” is unclear. Since even tabletop exercises are allowed, it should also be allowable to run an operational exercise that is somewhat limited in scope. Suggest removing the word “full” from both the Requirement and the Measures. Note that the wording for R2.3 already refers to “operational exercise”, not “full operational exercise”. -M2.1: The relevant timing (i.e. ‘upon the effective date of the standard’, and ‘between executions of the plan’) is missing from the Measures but included in the Requirements, should also be in the Measures -R2.2: We suggest removing the word "any" since it is too broad. For clarity and consistency with the Measure, we suggest changing "initially" to "initially stored". -R2.3: We suggest "... every 3 calendar years". We also suggest "... representative environment that reflects the production environment, where technically feasible..." to address potential issues with legacy systems. Under Requirements and Measures, seems to be some discrepancy between the language of the Requirement and the Change Rationale and VSL in referencing ‘every 3 years’ and referencing ‘every 39 calendar months’. Is the intention that the testing occur every 3 years, with not more than 39 months between tests?
No
-R3.1: Under Requirements and Measures, from reading the Change Justification, it appears as though the review is to occur after system replacement in addition to the regular testing each calendar year. However, the way the Requirements and Measures are drafted using the word ‘or’, it could be interpreted to mean the testing can occur either once a year or when systems are replaced. We suggest "or" to be replaced with an "and" in Requirements and Measures -R3.2: For clarity and consistency with the Measure, we suggest changing "... exercise,” to "exercise in 2.1 and 2.3...". Also, from the current wording “the completion of the exercise”, it appears that the review is supposed to take place after every annual exercise. However the wording “or actual incident recovery” seems to imply that a review would be required after every recovery incident throughout the year. Since large systems may have hundreds of disks there may be many disk failure recovery incidents a year, but it is difficult to see the value of a review after each of these. Suggest deleting the words “or actual incident recovery”. Alternatively, suggest adding language whereby a Responsible Entity may document for itself criteria of which types of recovery incidents it will review. -R3.4: The word "any" is too broad. We suggest "Update the recovery plan(s) within thirty calendar days of any organizational or technology changes that impact that plan." This change is consistent with similar language in CIP-008-5 Table R3 Part 3.4 Requirement. -R3.5: For clarity, we suggest changing "... responsible under ..." to "... identified in ...".
No
-Table of Compliance Elements, R1 – High VSL – the section does not include a violation of 1.1, only 1.2 through 1.5 – is this the intention? -Table of Compliance Elements, R2 – High VSL – The same comments as in R2, 2.2 and 2.3 above.
No
-R 1.1.3: We suggest changing "available" to "developed", since commercial application software may still be in use, but not currently available. -R1.1.4: we suggest that the "and" be changed to "or". -R1.2: For consistence of tenses, we suggest changing "Authorization" to "Authorize". "Delegate" should be "Delegate(s)". -R1.3: The requirements referenced from the other CIP standards must be explicitly listed in this requirement. The drafting team should also ensure that the 30 day window does not conflict with the referenced requirements. We also suggest that not all of the "documented required" needs to be updated within 30 days, and could be allowed a longer update period. -R1.4.2: The words seem to be missing here, we suggest “following the change, verify that the required cyber security controls….” -R1.5: We suggest deleting "... for Control Centres..." since High Impact BES Cyber Systems only includes control Centres, and therefore this wording is redundant.
No
R2.1: For clarity, we suggest "Monitor for changes to the baseline, where technically feasible, (as defined ....". The technical feasibility should apply to the monitoring, not to the entire requirement, including documentation and investigation.
No
-R3.1: The language for requirements with time intervals should have a consistent format, beginning with the action, and ending with the time interval. In addition, the “security controls” must be specified. Does this include background checks or training? Suggest wording “the technical security controls that are covered by CIP-007-5”. -R3.2: Suggest deleting “not to exceed 39 calendar months

between assessments" -R3.2 - Measures – language regarding timeline should match the language used in the requirement itself. -R3.3 – Applicability: The Associated Physical Access Control Systems should be included in the Applicability. -R3.3: For clarity, we suggest "... perform a vulnerability assessment of the new Cyber Asset."
No
-VSLs - R3, Lower VSL – reference is made to assessments on 'each' BES Cyber Systems, but the timeline talks about the time between assessments on 'one of' the BES Cyber Systems. For entities with multiple BES Cyber Systems we need clarification whether the timeline runs between assessments on a particular Cyber System basis, or whether it runs between assessments on any Cyber System. -VSLs - R3 – Active Vulnerability Assessments is capitalized in the VSLs but is not elsewhere
Yes
No
-R2.1: We suggest using local definition instead of the footnote.
No
-R1, High VSL: There is a reference to assessing 'periodically' while the requirement itself sets out a specific timeline. It needs to be changed to reflect requirement.
No
-Unplanned Changes Resulting in a Higher Categorization: If the intent is to address changes made outside of the Responsible Entity's electric system as unplanned, then we suggest wording "an action by an external entity is performed outside of that particular transmission substation ...", and "... power flows would have been performed by the external entity ...". Is the intent to only capture changes by a neighboring entity? -What is the notification process for Responsible Entities to become aware of unplanned changes? When is the start time for compliance implementation for Entity A when Entity B makes a change to the BES which causes a higher categorization of Entity A's BES Cyber System? -We suggest 18 months for all the scenarios for unplanned changes to correspond with time period allowed for the initial effective date of the CIP V5 standards, due to the scope of the work required. -For clarity, we suggest "12 months for requirements not applicable for Low Impact or Medium Impact".
Individual
John Bee
Exelon
Yes
We support the comments submitted by EEI with the following additions: BES Cyber Asset – Add a statement "Support systems such as voice communication (e.g., 900 MHz Radio system), ventilation, power supply systems, and similar supporting systems are not considered BES Cyber Assets." CIP Exceptional Circumstance – Change to read (modified text underlined or crossed out) "A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability, or an emergency support to restore operation of BES Cyber Asset or BES Cyber System by a supplemental vendor not already authorized for electronic access." Background: - This addresses emergency situations. Current wording seems to be biased towards physical assistance, but not electronic. - While electronic should be accounted for in BES Cyber asset Recovery plans, the current wording does not address large vendors such as Microsoft or Oracle that may be needed to restore the BES Cyber System or Asset.
Yes
We support the comments submitted by EEI with the following additions: Dynamic response – TOP is listed in the table but not on the list in the next section.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.

No
We support the comments submitted by EEI.
Yes
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with the following addition: R3, M3 item 2 – Please Add wording to the end. “Electronic signature is acceptable.”
No
We support the comments submitted by EEI with this addition: We would instead prefer the existing wording of CIP-003-4 R1.2 “The cyber security policy is readily available to all personnel who have access to, or are responsible for…” If an “awareness” of policy requirement is needed we feel it would be better addressed in CIP-004-5 R1 or R2.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with these additions: R7.2 Personnel reassignments must be processed and access revoked by end of day, yet terminations are by end of NEXT calendar day - seems backwards. Exelon has concerns that this revocation of access for internal transfers as proposed will significantly increase administrative burden and costs in an area with no commensurate reduction in risk to the reliability of the BES. In order to implement this requirement as proposed, Exelon would need to completely reprogram its HR systems which currently run in batch mode every night. This would be a major expense without a commensurate increase to BES reliability. The SDT has failed to provide a technical justification for this change. Additionally, it is unclear if the major software vendors for Human Resource systems can such a major process change. R7.3 – Change capitalization as shown in measures “BES Cyber System Information”. R7.5 – b. Need a definition of “extenuating circumstances”
Yes
No
We support the comments submitted by EEI with these additions: R1.1 a. Update wording in Measures per mark-ups: “Evidence may include, but is not limited to, documented technical and or procedural controls that exist and have been implemented.” The requirement has “or”. We would like the text of measures to match the text of the requirement. R1.2 Applicability wording should not

include the Physical Access Control Systems. Currently CIP-006-4 R2.2 does not require the protective measures of CIP-005-4 R1 Electronic Security Perimeter and sufficient protections exist in the other requirements. R1.3 Suggest using existing CIP-005-4 R2.2 wording for this item or at least removing the "or denying" wording since we should only have to specify access permissions, not all the things we deny access to. As proposed, this would add significant administrative burden without a commensurate reduction in risk to the reliability of the BES.

No

We support the comments submitted by EEI with this addition: R2.2 Please identify where encryption is required? Do we have to encrypt on entity trusted networks or between the Intermediate device and the Electronic Access Point (EAP)?

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI with these additions: Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. Table Item 1.1: “Medium Impact BES Cyber Assets with no External Connectivity” should be added to the applicability wording Table Item 1.2: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 1.4: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 1.6: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Suggest removing the "protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems" wording from the requirement since that is part of the Defined Physical Boundary definition.”

No

We support the comments submitted by EEI with these additions: Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. Table Item 2.1: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”. Table Item 2.2: applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity”.

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI.

No

We support the comments submitted by EEI with these additions: In cases where the intent of the drafting Committee was not to submit TFEs when an asset was not capable of meeting a requirement explicitly state “Devices that cannot … “ do not require a TFE to be generated.” (Similar to EEI comment on R4.1) Several requirements list BES Cyber Assets, but Applicability does not. Either delete BES Cyber Assets from requirement, or list them in Applicability.

No

We support the comments submitted by EEI with these additions: R2.3 – a. Provide more clarity for

this requirement – does “any exceptions for CIP Exceptional Circumstances “ mean that we temporary suspend normal patching activities when “CIP Exceptional Circumstances” occur, or does it address situations where certain BES Cyber Assets cannot be patched, and this would be documented as “CIP Exceptional Circumstances”. b. R2 no longer allows TFEs, so we need to account for the assets that cannot be patched. Provide clarity around this. c. Include in Measures document showing any exceptions for CIP Exceptional Circumstances related to remediation plan.
No
We support the comments submitted by EEI with these additions: Rationale for R3 - No definition of “Maintenance Cyber Assets”, it should reference Transient Cyber Assets R3.4 – a. Add Transient Assets to the Applicability column b. There will be a significant issue with vendor assets – may want to distinguish between companies’ corporate assets vs. vendor assets. We have external vendors coming to substations or accessing remotely, and no control over their assets. c. Delete from Measures “logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets”. 1) This measure is more applicable to 3.5, and 2) There is no requirement in 3.5 to log when removable media were connected. R3.5 – Add Transient Assets to the Applicability column
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with these additions: R5.5 – a. Measures include personal attestations. This may be required from a large group people and these attestations would need to be managed. b. If we submit an exception to our internal policy, will this automatically be compliant? This addresses 5.5.3 “password change on entity-specified time frame …” we may still have accounts where passwords cannot be changed. No TFEs are allowed. Provide clarity. 5.6 – b. The requirement specifies “A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts. ” In cases where we cannot limit number of unsuccessful authentication attempts but we can generate alerts, will we still need a TFE? Add clarity around that to the requirement.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with the following additions: R2.1 – add wording to 1st bullet of requirement “by recovering from an actual incident involving a BES Cyber System or an equivalent system in the test/lab or pre-production environment, or …” R2.2 – Add wording at the end of the requirement “Testing of information for every BES Cyber Asset is not required. Testing of information for a representative sample is sufficient.” R2.3 – Add wording at the end of the requirement “Testing of recovery plans for every BES Cyber Asset is not required. Testing for a representative sample is sufficient.”
No
We support the comments submitted by EEI.
Yes
No

We support the comments submitted by EEI with the following additions: R1.4 – Update wording “For a change to the BES Cyber System that deviates from the existing baseline configuration as required by R1.1: ” Add the term “Cyber Security Controls” to definitions, and include examples of what you consider cyber security controls.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
Yes
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI.
No
We support the comments submitted by EEI with this addition: Timing should be at least 24 months due to the large number of Low Impact BES Cyber Assets that need to be inventoried and security settings documented.
Individual
David Martorana
Tenaska, Inc.
Yes
1. In the definition of BES Reliability Operating Services clarification of which aspects of “Spinning Reserve” “AVR” and “AGC” as they relate to the NERC Functional Model are included. It is not clear which Aspects of the Balancing Load and Generation apply to the GO and GOP. Add a Definition of Multi Factor Authentication
No
2. Section 2.3 in Attachment I, may be problematic as it allows Planning Coordinators or Transmission Planners to “arbitrarily” move GO and GOP entities from Low to Medium. In order to maintain a competitive market place and not place a disproportionate regulatory burden on less vertically integrated entities, bright lines for this determination must be drafted. I am not sure how subjective TPL-003 and TPL-004 are.
No
3. 30 days may not be enough time to assess, identify, and categorize if a whole facility is brought from Low to Medium by a Planning Coordinator or Transmission Planner. Does this revision say how long we have to apply the security controls after a BES Cyber Asset or System reaches an elevated Impact Rating. Is it considered an unplanned change per the Implementation Plan?
Yes
No
5. R1 VSL should take into consideration comment 3.
Yes
Yes
Yes
No
9. This requirement appears to be redundant and should be removed as it is covered with CIP 004

Yes
Yes
11. This seems fine, but it might need to be stated that the delegated authority can be exercised prior to the documentation being completed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
20. R7 individuals should not be plural
Yes
Yes
22. Provide diagrams showing examples, (i.e. SSL VPN, with firewall as Intermediate Device) providing secure Interactive Remote Access. Allow the definition of Multi Factor Authentication to include Credentials on Vendor Network, ESP Firewalls by Vendor IP, and Credentials on BES Cyber Asset.
No
23. Should a lower VSL category be created for an outage associated with the IDS, or is that covered elsewhere?
Yes
Yes
Yes
Yes
27. In R3 the High VSL description should be moved to Moderate, also it would be helpful to note what elements are included in an acceptable “outage record”
Yes
Yes
Yes
30. The use of the word connected in the definition of Transient Cyber Asset, should be more clearly defined.

No
31. Requiring an Entity to rectify a deficiency by the next calendar day will require capital outlay, and eliminate the economic benefits of shared spares.
No
No
No
No
Yes
36. It is not clear if a change in 3.4 includes devices that reach an elevated Impact Rating, i.e. from Low to Med, is this in reference to a planned and unplanned change in the Implementation Plan?
Yes
37. In R1, Which appropriate organizations must an entity have evidence of contacting during a drill to avoid a High VSL? A lower VSL should be associated with partially using the Incident Response Plan, or define “does not use”.
Yes
Yes
Yes
40. Consider the recovery efforts, and that more time might be needed for documentation (3.3) following an actual incident recovery. (3.4) may be hard to comply with if technology changes are made in response to an actual incident recovery. The CIP Exceptional Circumstance language used in CIP-004, or Disaster Recovery in the Implementation Plan could be used to ease this concern.
Yes
41. It is not clear if the Severe VSL would apply if 99% of all BES Cyber Assets were addressed, and one was missed, consider a lower VSL for this circumstance.
Yes
42. This requires for most entities currently complying with CIP, the creation, modification, or expansion of a configuration management system, and modifications and additions to the security status monitoring systems.
No
Yes
Yes
45. Provide additional time for documentation for CIP Exceptional Circumstances
46. It is not clear what labeling methods are acceptable for Electronic Information (File Name, Watermark, etc.)
Yes
Yes
Yes
Individual
Robert Solomon

Hoosier Energy
Yes
The first two sentences in the definition of “BES Cyber Asset” are difficult to interpret. After considerable discussion among our staff, our understanding is as follows: the definition makes the distinction between when an asset is “rendered unavailable, degraded, or misused” and its actual “operation, mis-operation, or non-operation” under such conditions. If the asset impacts the BES “within 15 minutes” of its actual “operation, mis-operation, or non-operation,” then it is a “BES Cyber Asset,” regardless of how long since it was “rendered unavailable, degraded, or misused.” We recommend editing this definition for clarity as it took a number of our staff numerous reads and discussion to arrive at this understanding that we are still not sure is what the drafting team intended. The distinction should be clarified. Also, we question the necessity of such a distinction and whether the value it adds is worth the confusion it produces. Additionally, it is unclear whether the “timeframe” referred to in sentence three applies to the “within 15 minutes” timeframe or the “regardless of the delay” timeframe. How does the responsible entity know if a BES Cyber Security Incident was malicious? Understanding if an act was malicious implies an understanding of intent. We do not believe that intent is something that can always be quickly and easily understood. Consider the recent case of the failure of the water pump at a Springfield, Illinois water utility that was initially attributed to hacking because it was accessed from a Russian IP address. It turned out it was accessed by a contractor on vacation in Russia at the request of the utility. Obviously, this example demonstrates intent takes time to determine. The Project 2009-01 Disturbance and Sabotage Reporting even stated this in their recent posting for the reason they decided not to define sabotage because intent is so difficult to determine. Thus, we recommend striking malicious from the definition. BES Cyber System includes the capitalized term Maintenance Cyber Asset. The capitalization is an indication that the term is defined in the NERC Glossary. Neither can we find such an existing definition nor is it the definition proposed in this standards project. Either the capitalization needs to be removed or the term needs to be defined. We recommend the latter. BES Reliability Operating Services should not be a NERC defined term. Many of these services are similar to the Policy 10 – Interconnected Operating Services that was never passed because industry could not agree on it. It is doubtful industry is going to agree on this broad definition that could apply outside the CIP standards. Furthermore, there are several issues with the definition. First, it is not clear what is intended by including contingency reserve in parentheses after spinning reserve. Contingency reserve can include spinning and non-spinning components as long as it can respond in 15 minutes to meet DCS. Spinning reserve does not necessarily relate to contingency reserve directly in that it can include unloaded on-line reserves that respond in more than 15 minutes. Furthermore, NERC has two conflicting definitions of spinning reserve: Spinning Reserve and Operating Reserve – Spinning. One definition limits the spinning reserve to what can respond in 15 minutes and the other does not. Second, it is not clear what is intended by including contingency reserve in parentheses after non-spinning reserve. Per NERC definition, non-spinning reserve is time limited but not necessarily limited to the 15 minute limit set in DCS and, thus, on contingency reserves. Thus, while some contingency reserves may be non-spinning, not all non-spinning reserves will be contingency reserves. Third, under the Managing Constraints section of the BES Reliability Operating Services definition, ATC is identified. It should be removed. ATC is not used to manage constraints but rather to sell transmission service. That transmission service may never be used. While ATC is calculated using reliability components, it is not a reliability service but a commercial service. FERC even acknowledged that the MOD (ATC) standards were designed primarily “to ensure non-discriminatory allocation of transmission capacity among transmission market participants” in paragraph 30 of the order approving FAC-013-2 (137 FERC ¶ 61,131 Docket No. RD11-3-000). Fourth, the Inter-Entity Real-Time Coordination and Communication section of the BES Reliability Operating Services definition should be struck as it is just a supporting activity for all the other services. CIP Exceptional Circumstance should be modified to include a clause that other circumstances of similar nature and/or impact could be included as a CIP Exceptional Circumstance. Otherwise responsible entities could be put in a position of having to choose to violate some the CIP requirements because the SDT did not think of a particular exceptional circumstance that should have been included. CIP Senior Manager should be struck along with all references to CIP Senior Manager in the CIP standards. This definition and associated requirements dictate a corporate governance structure for no apparent reliability reason. A responsible entity should be free to have two, three, or more personnel oversee various portions of the CIP program. The responsible entity will still be required to meeting the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential

for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards. It is not clear that Control Center needs to be defined. EOP-008-1 (Loss of Control Center Functionality) was written without defining control center. We are concerned that this definition could cause confusion with EOP-008-1 and believe the definition needs to be coordinated with that standard. Reconvening the SDT that worked on EOP-008-1 may be necessary to accomplish this. For Interactive Remote Access, how do Cyber Assets used by the Responsible Entity differ from those used by employees? It is not clear why Responsible Entity is delineated in such a way. Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.
Yes
In the Background section, the SDT describes that the responsible entity will have a choice to evaluate BES Cyber Assets individually or collectively in a BES Cyber System. The opening paragraphs for High Impact or Medium Impact criteria need to be modified to make this clear. As written they do appear to provide a choice by stating "Each BES Cyber Asset or BES Cyber System". However, it does not make clear whose choice that is. The auditor might decide the choice belongs to them. Thus, these paragraphs need to be modified to make clear the choice belongs to the responsible entity. While similar and conforming changes need to be made to the Low Impact Rating as well, one additional change needs to be made. "All other BES Cyber Assets and BES Cyber Systems" should be changed to "All other BES Cyber Assets or BES Cyber Systems". Otherwise, there is no choice because both have to be included. This change would also conform Low Impact Rating to the Medium and High Impact Rating sections. While there are limitations on the TOP Control Centers such that not all TOP Control Centers will be included with a High Impact, there is no such limitation on the BA Control Centers. We recommend a similar limitation be place on a BA Control Center such that if the BA is not controlling assets that meet certain criteria in the Medium Impact they should not be included. There many small BAs that simply won't have a broad impact on the Interconnection and, thus, should not be included. Criterion 1.4 which obligates certain GOP control centers to be rated High Impact includes criterion 2.12 as one of those reasons. 2.12 should be struck as it deals with UVLS and UFLS which are not GOP functions. Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. It is implied because there are not any requirements in any standard including the TPL standards that require the TP or PC to designate generation necessary to avoid BES Adverse Reliability Impacts. In fact, BES Adverse Reliability Impact is not even used in any requirements that pertain to the PC or TP. The implied obligation creates a compliance conundrum. Since it is only an implied obligation and not an explicit requirement, the PC and TP will never be required to meet it. How then, does the GOP or GO insure they get the information they need from the PC or TP? They have no recourse. Use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. For Criterion 2.5 regarding Cranking Paths, the last two bullets are confusing and the wording should be clarified. The graphic provided on page 26 in the Application Guidelines help with that clarification and the drafting team should consider adding this as an attachment so that it will remain with the standard. It is premature to base criterion 2.7 on the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index". It is still a work in progress. This document and approach is being developed under the purview of the Planning Committee's (PC) Reliability Metrics Working Group (RMWG). The PC has not approved any of the indexes. The only thing the PC approved was the approach and framework. At the December 2011 PC meeting, it was clear that the RMWG has additional work to do to finalize the indexes. Thus, it is premature to use any of these indexes in the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" in a standard. At the very least, use of them should be coordinated with the PC and RMWG. Criterion 2.9 is redundant to Criterion 2.8. FACTs devices are Transmission Facilities and are covered in 2.8. Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. This is not likely. An SPS or RAS may be implemented for a specific contingency for example. As an example,

when that contingency happens, certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. Criterion 2.13 has control centers in lowercase. This would mean that the proposed NERC glossary definition does not apply. Is this the intent? If so, how would this meaning of control center be different?

No

We think Requirement 1 and associated Attachment 1 should focus on identifying the BES Facilities that are important and then the associated BES Cyber Systems and BES Cyber Assets. Otherwise, all BES Cyber System and BES Cyber Assets will have to be inventoried. While the Background section states "Requirement 1 only requires that discrete identification of BES Cyber Systems and BES Cyber Assets for those in High and Medium categories", we do not see how a responsible entity can demonstrate that it has correctly identified all High and Medium Impact BES Cyber Systems and BES Cyber Assets unless it has a complete inventory of all BES Cyber Assets and BES Cyber Systems. We can envision auditors asking for such an inventory. Part 1.1 needs to be further refined regarding what kinds of changes are included. By the NERC Glossary definition, Facility can include relay equipment associated with protecting a transmission line as part of the "set of electrical equipment that operates as a single Bulk Electric System Element". Thus, a change to a relay setting could be could be inadvertently included. It should not be. We suggest the changes be limited to topological changes, generator interconnections and generator uprates and equipment retirements. While other changes such as permanent derates may allow that responsibility entity to lower the categorization of BES Cyber Systems and/or BES Cyber Assets, the reduction in compliance burden will cause them to do this. Thus, we don't need to increase their compliance burden by requiring them to do it for permanent derates.

No

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won't accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories. Because there is no question dealing with other sections of this standard, we are adding comments regarding those sections here. We disagree with all the specificity in the applicability and facilities section for Distribution Provider (DP) and Load Serving Entity (LSE). These sections are not consistent with the Compliance Registry Criteria and will only cause confusion. There is no specific compliance registry criterion for including a DP that has been included in the Transmission Operator's restoration plan. Because NERC clearly states in their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2) that they will not enforce the standards against entities that are not registered, the standard simply couldn't be enforced against such an entity included in the TOP's restoration plan unless they were already registered. Furthermore, the Compliance Registry Criteria already allow NERC to register a responsible entity as a DP and LSE if that entity "owns, controls, or operates facilities that are part" of a required UFLS or UVLS program, special protection system (SPS) or transmission protection system. Since the DP or LSE with a required UFLS or UVLS program, SPS or transmission protection system, is already registered, how does this applicability section provide any more clarity? The DP or LSE will know whether they own or operate these facilities and simply will provide the appropriate response in any required CMEP submissions such as audits and self-certifications. If the responsible entity is not registered as an LSE or DP even if they own these facilities, then again NERC can't enforce these proposed CIP standards against the entity per their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2). In the Facilities section, we are concerned that non-BES Facilities will be included in the standard. Non-BES Facilities should not be included at this juncture given that the Project 2010-17 Definition of Bulk Electric System drafting team is just beginning its work on the second phase of defining the BES. Until this work is completed, non-BES Facilities should not be included and, then, they should only be included with significant justification. There should be a high bar for deviating from the BES definition particularly since it will be recent and have considered all issues facing the industry at that time. The application guidelines have not clearly

identified all functional entities that might have some responsibility for the various BES Reliability Operating Services. For instance, in the Dynamic Response section, Special Protection Systems responsibilities are attributed to only TO but this could be a GO or even DP responsibility. UFLS and UVLS are only attributed the DPs but the TO could choose to implement these systems on the transmission system. Governor Response could also be a GOP responsibility. Another example would be the current and next day planning in the Situational Awareness section. It is only attributed to the TOP even though there are NERC standards that require the RC to perform next day planning. In the Managing Constraints section, the responsibility for interchange schedules is attributed to the TOP and RC. It should be attributed only to the Interchange Authority or Interchange Coordinator. In the Restoration of the BES section, the responsibility for off-site power for nuclear facilities is attributed to the TOP. In the NUC standard, it is actually attributed to the transmission entity which could be one of eleven functional entities. Since there many errors (we did not identify all of them) in attributing responsibility in this section, we suggest the drafting team completely review this section and update it or consider removing the responsibilities altogether as their purpose is not clear. We believe the statements beginning on page 23 and continuing on page 24 of the High Impact section of the applicability guidelines regarding TOP delegation to the TO should be removed. If the TOP has delegated some functions to the TO that would otherwise have been carried out in the TOP Control Center and might have resulted in additional TOP BES Cyber Assets and BES Cyber Systems being categorized as High Impact, this delegation should not have an impact on the TOs categorization of BES Cyber Systems and BES Cyber Assets. First, the TOP is still responsible and can't pass that responsibility on through a delegation agreement. Thus, the TOP and TO will have to address this in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO. The TO likely owns these BES Cyber Assets and BES Cyber Systems, and they should be classified according to the criteria established for TOs in Attachment 1. Use of the term asset in the definition requires ownership by the responsible entity. If is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third, control Centers for TOs are not addressed in Attachment 1. Fourth, this appears to address some concerns regarding some RTO/ISO's TOP registration models that have been expressed in various forums by regulators. These concerns should not be addressed in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. Fifth, there is nothing in the requirements that requires these BES Cyber Assets and BES Cyber Systems to be categorized in this manner. The application guidelines are not requirements and cannot modify the requirements. They can only help explain the requirements. However, these statements are fundamentally altering the requirements and how the attachment 1 criteria are applied. In the first paragraph on page 25 in the application guidelines, there is statement that indicates there may not be a Planning Coordinator for a given area. This statement is contrary to the Section 501.1.4 of the NERC Rules of Procedure. This section states that the registration process shall ensure that "no areas are lacking any entities to perform the duties and tasks identified in and required by the reliability standards". In the third paragraph on page 25 in the application guidelines, Category D contingency should be removed. The TPL standards only require a Planning Coordinator or Transmission Planner to document the impacts of Category D contingencies. There are no performance requirements for Category D contingencies. Thus, it is highly unlikely that any Planning Coordinator or Transmission Planner could ever justify the costs for reliability must run unit through Category D contingencies to its regulator, and, thus, there likely will not be any. In several places in the application guidelines (occurs on pages 26, 27, and 29), exceeding an IROL is discussed when the SDT really means violating an IROL. An IROL by definition has two components. It has a limit and a time constant called Tv. This time constant can be up to thirty minutes and usually is. The time constant is set based on how long the IROL limit can be exceeded without exposing the BES to an unacceptable risk. Thus, an IROL is only violated once the limit has been exceeded for a time greater than Tv. An IROL is exceeded but not violated when the time of the exceedance has not reached Tv. We suggest the drafting team modify the application guidelines in this standard and any other standard with the appropriate use of exceed or violate for the IROL consistent with this explanation. In the third bullet on page 29, the term regional load shedding requirement needs to be made consistent with the new UFLS standard. The UFLS program will be developed by the Planning Coordinator and not the Regional Entity. The NERC adopted version of the standard does not even require a regional version of the standard as was originally proposed.

No

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES

Cyber Assets or BES Cyber Systems. The VSLs drop the “or delegate” language which implies the CIP Senior Manager has to approve the categorization and identification. The “or delegate” language should be added back.
No
This requirement should be struck along with all references to CIP Senior Manager in the CIP standards. This requirement dictates a corporate governance structure for no reliability reason. An entity should be free to have two, three or more officers or personnel to oversee various portions of the CIP program. The responsible entity will still be required to meet the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management’s attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards.
No
We agree there should be “one or more documented cyber security policies that represent the Responsible Entity’s commitment to the protection of its BES Cyber Systems and addresses” the required ten topics seem. However, the items that a “Responsible Entity should consider” for inclusion in its cyber security policy as stated in the Guidelines and Technical Basis section (application guidelines) of the standard appear to be written as requirements and the drafting team should consider moving them to R2 if auditors will ultimately treat them as requirements. This will reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the drafting team can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. Furthermore, we believe the fourth bullet in section 2.3 Remote Access regarding including language in contracts with vendors, consultants and contractors requiring them to follow the responsibility entity’s cyber security policy should be modified. The bullet should apply to future contracts and not existing contracts to avoid the need to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. In addition, M2 bullet 2 says “Records that indicate the required ten topics were implemented.” What exactly does “implemented” mean in this case? That the items the responsible entity should consider for each of the topics are included in the policy(ies)? This needs to be clarified.
No
What does “initially upon the effective date of the standard” mean? It could be interpreted that the cyber security policies would need to be reviewed and approved on the date the standard is effective which is not reasonable for a myriad of reasons. A couple of those reasons could include that the effective date could be a holiday or weekend or the CIP Senior Manager is not available (they could be incapacitated). Ultimately, we believe that the intent is for the cyber security policy to be in effect and approved by the effective date rather than on the effective date and to ensure that is has been reviewed recently particularly since the implementation plan is a minimum of 18 months. Then going forward subsequent reviews and approval would take place at least once per calendar year not to exceed 15 calendar months. If this intent of this requirement, there really is no way to ensure the review occurred recently without making the requirement retroactive which clearly cannot be done within a requirement. In addition, M3 bullet 1 implies that a Responsible Entity needs to have a “document management system.” The word “system” could mean an application to manage documents. It could also mean a process for managing documents. Rather than leave it open to interpretation, we recommend eliminating the phrase, “from a document management system.”
No
Awareness of a security program is covered in depth in CIP-004-5 and ensuring accessibility and availability of cyber security policies goes hand in hand with this. We recommend removing R4 from CIP-003-5.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security

policy. However, we do not agree with the use of “CIP Senior Manager” in this requirement based on our comments for R1 in question 6.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security policy. However, we do not agree with the use of “CIP Senior Manager” in this requirement based on our comments for R1 in question 6.
No
We disagree with the VSLs for R2. More gradations could be provided based on the number of parts missed. Since there are 10 parts, there is plenty of room for four VSLs. The VSLs for R6 should consider using the numbers of days that documentation of the change to the CIP Senior Manager documentation is late. Use of number of days late is a common way to write a VSL and allows more gradations.
No
For Part 1.1, the rationale box does not appear to agree with the requirement. It states the need to ensure everyone with authorized access receives this awareness was removed. Yet, the requirement applies to the responsible entity and does not appear to exclude anyone with authorized access. Which is it? Furthermore, the rationale box should be more specific and use the full names of both types of access which are: authorized electronic access and authorized unescorted physical access. Otherwise, generically referring to authorized access could mean one or the other but not both, or it could mean both.
No
We agree with the concept that training should be role based. As an example, a system operator who is an end user of an EMS does not need most of the training identified in the various parts of Requirement 2. The system operator certainly does not need training on recovery plans for BES Cyber Systems but might need training on the visitor control programs and how malicious actors might use social engineering to gain access to the EMS. The problem we see with the requirements and it parts is that it does not make clear anywhere the need to identify what training each role would receive. Rather it only states that roles must be identified and then identifies training in the various requirement parts that apply to the main requirement which could be construed as applying to the whole training program including all roles. The paragraph references in the rationale boxes for parts 2.6 and 2.7 are inaccurate. Paragraphs 632-634, 688, and 732-734 refer to CIP-007 and CIP-009. There are no references to issues in CIP-004. While paragraph 413 does discuss CIP-004, it only describes what is in the standard and not any changes directed to the standard. In regards to Part 2.6 and storage media, the only mention in Order 706 of storage media is in paragraph 635 and it directs NERC to determine what it means to prevent unauthorized retrieval of data using storage media.
No
This requirement needs to be clarified that it only is intended to require appropriate role-based training for each individual with authorized electronic access or authorized unescorted physical access based on their specific job responsibilities and not the entire cyber security training program identified in R2. Use of the word “needing” is problematic. An entity cannot grant authorized electronic access or authorized unescorted physical access unless it is needed per CIP-007-5 R5. We suggest changing “each individual needing authorized electronic…” to “each individual with authorized electronic…” For consistency across the standards and clarity, we suggest every use of “authorized electronic or unescorted physical access” be replaced with “authorized electronic access or authorized unescorted physical access”. This will help to avoid similar confusion that arose in previous versions of the standard in which it was not clear if “authorized” applied only to electronic access or unescorted physical access. It will further make it clear that authorized electronic describes one type of access. Regardless of how it is written, it needs to be consistently used across that standards and it is not.
No
Part 4.2 may not be possible to complete. While we agree with the need to conduct seven year criminal history checks, obtaining all addresses may not be possible. The responsible entity can verify the current address or a recent address from reviewing a driver’s license but after that the responsible entity cannot with certainty verify that it has all of the former work, home and school addresses of the employee. The employee may not provide the addresses and the background check may not provide these additional addresses. The requirement needs to be clear that the responsible

entity may request this information from both the vendor providing the background check and the employee but will not be held accountable for either party's failure to provide a complete list of addresses. Part 4.3 could be problematic for a responsible entity and needs to be clarified that the responsible entity does not need to establish hard and fast criteria that must always be followed. Finding qualified personnel to work in these highly specialized fields is challenging enough without adding this additional constraint. Background checks may certainly reveal problems with an otherwise qualified person. While some of these problems would be obvious reasons to disqualify a person, others may simply require further research and explanation from the individual for why it is not a problem.
No
In general, we agree with the requirement but believe the requirement should be further clarified, perhaps in the measurement, that in no circumstance should a responsible entity be asked or required to show the personnel risk assessment for an individual to auditor and enforcement personnel. There are a myriad of reasons not to show the actual personnel risk assessment including privacy concerns and other applicable laws may prevent this.
No
The application guidelines on page 44 state that access authorization and provisioning should not be performed by the same person. While this is a laudable goal, it should be clear that small entities may simply not have the staff to accommodate this guideline. We suggest adding "where possible" to this statement.
No
It is not clear why resignations are separated from terminations in Parts 7.1, 7.3, 7.4 and 7.5. Resignations are voluntary terminations. We are unsure what the drafting team intends to accomplish by splitting them out. Where do retirements and layoffs fit in? Since there does not appear to be any different requirements on resignations and terminations, we suggest to use only the generic termination to avoid this confusion. Part 7.2 does not address the situation for phased transfers. For many entities, a transferred employee could continue to need authorized electronic access and authorized unescorted physical access for a long period of time to provide support particularly if a new employee is being trained. This could occur long after the transfer date. While the application guidelines do address this issue, they are simply not requirements and NERC is not bound to follow them. Thus, we suggest making Part 7.2 more generically state that the authorized electronic access and authorized unescorted physical access should be terminated once management determines it is no longer needed. We are a little surprised that the application guidelines state in the scenario table that no action is required to revoke access in the event of a death. While we agree there would be no immediate additional risk for obvious reasons, access should still be revoked at some point.
No
VSLs for Requirements R2 and R3 should have more gradated levels. For R2, there could easily be several roles which would allow for more than two VSLs. Since there are 10 parts to the requirement, four VSLs could easily be written based on the number of parts missed. For R3, more VSLs could be written based on the percentage of individuals that were not trained. The Severe VSL for Requirement R5 incorrectly includes personnel risk assessments (PRA). PRAs are dealt with in Requirement R4.
No
The requirements of Parts 1.2 and 1.3 make no mention of egress while the associated measures specifically mention it. Does the drafting team intend for there to be procedural or physical access controls regarding egress? If so, that is not clear in these standards at all and could set up a responsible entity for a compliance violation. We do not believe that egress controls should be necessary. Only ingress controls are necessary to prevent access to unauthorized individuals. Egress really only helps in knowing who is currently within the Defined Physical Boundary which might provide some value but the expense of installing egress physical access controls would likely far outweigh any benefit. It is unclear how the "operational and procedural controls" required in R1.1 differ from the "physical access controls" required in R1.2 and R1.3. Suggested methods for restricting physical access are given in the "Guidelines and Technical Basis" (application guidelines)

section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. Also, regarding the application guidelines, it would be helpful if the section labeled “Requirement R1,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
We believe that this proposed requirement improves upon the existing requirements. However, we believe that individual point of contact could be confusing. We recommend changing it to escort and making it clear in the application guidelines that this would be the main escort with responsibility for the visitor but not necessarily someone who is with the visitor the whole time. Others could also temporarily escort the visitor. Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 2,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 3,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
A visitor control program is intended to identify and log visitors to the Defined Physical Boundary (DPB). They cannot gain access due to other requirement such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training requirements of CIP-004-5 compel a responsible entity’s personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the DPB. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF.
No
Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending “if less than three character types” to the end of the requirement for further clarity.
No
Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
No
EOP 4 in the Rationale box should be replaced with EOP-004. While Part 1.2 requires a process to identify Reportable BES Cyber Security Incidents, there is no indication of who is to receive these reports. There is only Part 1.3 that requires the responsible entity to identify internal and external staff to which to communicate the “incident”. Does that mean the list of recipients is totally up to the responsible entity and could be null? If not, then the drafting team needs to identify the minimum list of recipients. In Part 1.3, we assume the drafting team means Reportable BES Cyber Security Incidents by the use of the term “incident”. If this assumption is correct, please replace “incident” with “Reportable BES Cyber Security Incident”.
No
The requirement in part 2.1 appears to apply to actual BES Cyber Security Incidents. However, the requirement states that deviations from tests should be recorded. Thus, “or test” needs to be struck. R2 Part 2.2 uses the phrase “initially upon the effective date of the standard.” It is not clear as to the meaning of this phrase. It could be interpreted that the BES Cyber Security Incident response plan(s)

would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not reasonable. If the intent of this requirement is to do an initial implementation within some time period of the standard becoming effective, then the requirement should state a time period for this to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.

No

R3 Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that a review of each BES Cyber Security Incident response plan would need to take place on the date the standard becomes effective. Because Requirement R1 compels the development of the response plan, it does not make any sense to compel review of the response the same day the requirement of the response plan becomes effective. Rather the response plan review should be required the following calendar year after its initial approval. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.

No

The stated rationale for Part 1.1 does not support the change and additional rationale needs to be provided. Paragraph 694 of Order 706 requires NERC to develop a specific requirement to implement the recovery plan. This requirement is not an implementation requirement but still a requirement for what to include in the plan. Thus, we do not see how the rationale supports the requirement. Part 1.2 should not require either names or titles. These are problematic in that the recovery plan has to change for every personnel move which includes transfers, terminations and promotions. A promotion of IT Analyst to Senior IT Analyst would necessitate an unnecessary change. A better approach would be to allow the use of generic roles such as analyst or even perhaps staff from department X. The requirement needs to allow some flexibility to avoid unnecessary paperwork that provides no reliability benefit. The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ.

No

Part 2.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the recovery plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not practical for many entities and especially for smaller entities. Part 2.2 of CIP-008-5 R2 already requires BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Many of the same staff involved in the BES Cyber Security Incident response plans will likely be heavily involved in the recovery plans. The important part is that the recovery plan will be in place on the effective date per CIP-008-5 R1 and will likely have been tested prior to the effective date. Thus, the requirement should simply state a reasonable time period that can be met by limited staff for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Part 2.2 has potentially has a similar issue to Part 2.1 but is less clear. Rather than use the full term “initially upon the effective date of the standard” it just states that the test must be conducted initially. We assume the drafting team meant for this to be conducted on the effective date similar to Part 2.1. This makes completing this part and other parts mentioned in the previous paragraph even more impractical. The requirement should simply state a reasonable time period for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Since Part 2.3 requires a full exercise in representative environment every 39 months and is required to be included per FERC directive, we recommend that it be limited to High Impact BES Cyber Systems. Conducting this test in a representative environment could get very expensive because responsible entities may have to purchase the appropriate equipment to set up a parallel environment. This is simply not practical or cost effective to do for every BES Cyber System. Is it really practically to set up a representative environment for every 500 kV substation or special protection system for testing?

No
Part 3.1 should be modified to require the first review of the recovery plan in the subsequent calendar year to the approval of the requirement. To accomplish this, the drafting team should strike “initially upon the effective date of the standard and”. CIP-009-5 R1 already compels the responsible entity to have a recovery plan and becomes effective on the same day as Part 3.1. Thus, the plan will already have been reviewed when it was developed and approved. Thus, it does not make sense to have a separate review in Part 3.1 on the effective date. For consistency with Part 3.3, R1.2 in Part 3.5 should be written as Requirement R1, Part 1.2.
No
The VSLs for Requirement R1 should include more gradations than two levels based on the number of parts missed. For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.
No
Part 1.1.6 could be redundant with CIP-007-5 Part 2.2. While CIP-007-5 Part 2.2 does not explicitly require documentation of the security-patch levels, demonstrating compliance with it ultimately will require such documentation. Thus, it becomes redundant with Part 1.1.6 of CIP-010-1 R1. If not redundant, it certainly sets up a high probability for double jeopardy because each compliance violation of CIP-007-5 Part 2.2 will likely result in a violation of Part 1.1.6. Part 1.2 is unclear. Is this intended to require the CIP Senior Manager or delegate to authorize the process to develop a baseline configuration or is it intended to require the CIP Senior Manager or delegate to authorize deviations to the baseline? As a result, Part 1.2 needs to be clarified. As it is written now, the only clear requirement from Part 1.2 is the need to document baseline configuration deviations. Part 1.4.1 requires the responsible entity to identify the cyber security controls that could be impacted by the change. This appears to be the first use of cyber security controls in the library of CIP standards. As a result, the intent and meaning of the term needs to be further clarified.
No
Comments: Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the security controls for every applicable BES Cyber System and BES Cyber Asset need to be assessed on the date the standard becomes effective. This is not practical particularly for smaller entities. Several other requirements including Part 2.1 of CIP-009-5 and Part 2.2 of CIP-008-5 R2 already require significant action on the effective date of the standards. Part 2.1 of CIP-009-5 requires recovery plans to be implemented on the effective date and Part 2.2 of CIP-008-5 R2 requires the BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Imagine the amount of personnel and effort necessary to complete all of these tasks on (not by) the effective date. Many of the same staff involved in the BES Cyber Security Incident response plans and recovery plans will likely be heavily involved in the vulnerability assessments. The requirement should simply state a reasonable time period for the vulnerability to be completed after the effective date of the standard or make it clear that the vulnerability assessment needs to be completed by the effective date and not on. Part 3.2 has a similar issue as Part 3.1 in that it appears to require a vulnerability assessment for all High Impact BES Cyber Systems on the effective date of the standard. We have the same issue with this requirement in that the same limited set of staff will likely be responsible for completing these assessments as the tasks compelled by several other requirements that must be complied with on the same effective date.
No
In general, the VSLs escalate violations to the higher end of the sanctions matrix too rapidly for minor violations. This could be fixed by writing VSLs for each level rather than just High and/or Severe VSLs in some cases. For example, if an entity fails to establish a single baseline on one applicable BES Cyber System or BES Cyber Asset per Requirement R1, it would be deemed a High VSL. If that is one out of one thousand BES Cyber Systems or BES Cyber Assets, this would seem excessive. Likewise, if an entity is one day late in updating their baseline configuration per Requirement R1, the violation would be deemed Moderate. This is not consistent with many other requirements in the CIP proposal which provide four VSL based on the number of days late.
No
The rationale for Requirement R1 indicates Requirement 4.1 was moved to the BES Cyber System Information definition. It does not reference which standards the requirement comes from. It needs to

for clarity. Part 1.1 needs to be clarified. We believe the requirement pertains to ensuring BES Cyber System Information is marked in some way to be clear it is BES Cyber System Information. However, we are concerned that requirement could be interpreted as needing to develop a method to ensure that all BES Cyber System Information has been found and there is no extraneous information. In other words, we are concerned the requirement could be interpreted as requiring the method to be some sort of search process. Use of the word identify is what causes us concern since it is what is used in CIP-002-5 regarding finding all of the BES Cyber Assets. We think this problem would be solved by changing "identify" to "mark" and providing some discussion of the intent of the requirement in the application guidelines. Part 1.3 needs to be modified. It requires the responsible entity to assess its adherence to its BES Cyber System Information protection process "upon the effective date of the standard". This does not make any sense since the responsible entity will have just then been required to utilize the BES Cyber System Information protection process. What will they assess? This requirement should not require this assessment until the process has been in use for a year. Part 1.3 uses a term "protection process" that was not used previously in the requirement. For consistency with other requirements and clarity, we suggest that either that term be used in Requirement R1 instead of just the term process or that "protection" be struck in Part 1.3 and replaced with a reference to the main requirement.

No

We agree with the implementation plan concept that essentially bypasses the effective dates of version 4 of the standards for version 5. This will significantly lessen the compliance burden for responsible entities to avoid two separate transitions and avoid the confusion of preparing for version 5 while still preparing for version 4. We believe that some requirements should have delayed implementations plans rather than become effective on the same date as the remaining requirements. Some requirements are dependent on the completion of other requirements and do not make sense to implement until the other requirements have been in effect for some time. Consider Part 1.3 of CIP-011-5. It requires the responsible entity to perform an assessment of its adherence to the BES Cyber System Information protection process. However, the protection process is only required to be in effect the same day. What sense does it make to assess adherence to a process that was just started? The drafting team should perform a complete review of all the requirements for dependencies and determine an appropriate staggered implementation for them. The first sentence in the "Proposed Effective Date for Version 5 CIP Cyber Security Standards" on page 2 should be modified. It states the responsible entities must comply with the definitions on the effective date. Definitions have no compliance obligations. They simply become effective and help explain the requirements.

Individual

Tracy Sliman

Tri-State G&T Inc.

Yes

BES Cyber System Definition – Change: "Maintenance Cyber Asset" To: "Transient Cyber Asset" Rationale: Consistency and no definition proposed for Maintenance Cyber Asset. BES Reliability Operating Services –AECI believes the following BES services should be removed from the BES Reliability Operating Services, because they fail to meet the "real-time reliable operation of the BES" 15-minute adverse-impact criteria: 1) Balancing Load and Generation, (other than ACE, nothing else in this category can have a 15-minutes or less impact, and ACE availability and integrity are addressed within the BAL Standard, so including here is double-jeopardy.) 2) Restoration of BES, remove, "but is not limited to", and list the aspects of the Restoration of BES Operating Service. 3) Situational Awareness – Frequency Monitoring – (While frequency monitoring is important, contrary to the underlying position within the CIP standards, redundancy of frequency monitors really does matter, and the standard should probably leave this one off, in order to avoid only a few instances of frequency-monitoring equipment being implemented. Also, the availability of a reliable Frequency Monitoring signal is subject to a strict BAL standard. Control Center Definition – Change: "BES generation facilities or transmission facilities", To: "BES generation facilities or BES transmission facilities", Rationale: Clarity of scope.

No

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 - Change: “at time of resignation or termination” To: “within 24 hours of resignation or termination” Rationale: Consistency with hard time-frames asserted with other sub-requirements, with reasonable delay for uncontrollable circumstances surrounding some separation of employment.
Yes
No
Low impact Cyber Systems should not be required to adhere to part 1.1 in the table.
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Measures required to show evidence of this requirement are unclear.
Yes
R4 part 4.5 – The requirement to review security event logs every two weeks is very onerous. Recommend the current practice of 90 day review or the ability to skip a manual review in favor of automated alerting on specific security events.
No
R5.5.1 Change: reword as “Minimum Password length of at least 8 characters, or maximum supported by the BES Cyber System if less than 8 characters is supported.” Rationale: Clarity R5.5.3 Change: “based on” To: “based upon” Rationale: grammatical
Yes
Yes
Yes
Yes
No
R1..R3 VSLs for Low Impact Assets - Change: High VSL To: Low VSL and Change: Severe VSL To: Moderate VSL. Rationale: align risk with severity. R3 VSL - Change: “30 calendar days” To: “60 calendar days” then Append: “within 60 calendar days” to last sentence. Rationale: Consistency and align timeframe with Severity. (Failure to review within 30 days might be considered High, and written into that column – see note on Low Impact Asset VSLs above.)
Yes
No
R2.3 Guidelines – Add: Guidelines! Rationale: Without some related guidelines, the phrase “in a representative environment that reflects the production environment” introduces too much ambiguity and opportunity for disagreement between Responsible Entities and Auditors. “SEE FAQS AND CIPC GUIDELINES” is inconsistent with the quality of product being produced in other CIP version 5 standards.
Yes
No
R3 VSL - Change: Severe VSL To: High VSL and Add: Severe VSL with 60 days violation. Rationale: align severity with risk.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Change: “18 months” To: “24 months”, including all other related wording Rationale: CIP Version 4 provides for 24 month implementation plan, yet CIP Version 5 is going to bring many more Responsible Entities into scope that have not formerly been acclimated to planning and accomplishing compliance with the NERC CIP Standards.
Individual
Bob Thomas
Illinois Municipal Electric Agency
Yes
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
Illinois Municipal Electric Agency (IMEA)appreciates the SDT's efforts to date. We emphasize that even though the comment (and balloting) period was longer than normal, it was stIll not enough time for small entities (in particular) to adequately review a proposed Reliability Standards development of this magnitude. IMEA's limited comments or lack of comments to questions in this comment form are due to this inadequate comment period. IMEA, therefore, would like to empahsize that it supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency; particularly those comments regarding the impact on small entities and the need for a fourth category of low impact without connectivity in order to accomplish a more realistic application of the CIP standards to small entities.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Recommend changing "upon" to by. Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
Yes
No
Recommend changing "upon" to by. Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.

Yes
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No comment.
Yes
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No comment.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments

submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
No
Illinois Municipal Electric Agency supports, and encourages SDT consideration of, comments submitted by American Public Power Association and Florida Municipal Power Agency.
Individual
Rich Vine
California ISO
Yes
1. Introducing ideas such as 'attempt to disrupt' into a definition requires a widely accepted and understood metric to define an attempt to disrupt. Recommend plagiarizing from NIST/ISO-27001/2 definitions to avoid these problems. 2. “Suspicious event” seems open to different interpretations. 3. Electronic Security Perimeter being defined as a “collection of Electronic Access Points” is an odd definition; a perimeter is not a set of objects, it is a line or boundary. 4. “Interactive Remote Access” is defined, yet “interactive access” is not, it would be helpful to have a definition for “interactive access”.
No
• Although stated that you do not need to keep a list of Low Impact BES Cyber Assets, you would still need to do a comprehensive inventory, as some requirements still apply to those assets.
No
• Measure 2 should include "or delegate".
No
• Seems like if you incorrectly categorized or missed 5% or fewer of your assets, by default you are automatically put into the Severe VSL range as it most likely will have been more than 60 days since the BES Cyber System was identified or categorized. If it only covers major changes to facilities and elements and not cyber systems, it would not be a concern – but this would need to spelled out.
Yes

Yes
• Would like to see some assurance that the auditors would focus only on the standard requirements, and not auditing against what is submitted into evidence. I believe there is some fear in the industry that the higher standards some entities hold themselves to could be held against them during the audit. This would help get rid of maintaining 2 different policies – one for CIP, and one for the non-CIP assets.
Yes
• Re-word the sentence - as written it is unclear whether we need to approve the CIP Senior Manager, or ensure that the policies are approved by the CIP Senior Manager.
No
• It appears to preclude an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems. This would be a more comprehensive way of ensuring that individuals who may have a job scope change in the future are not missed by having to track them and make sure they take another subset of the training pertinent to the new job function. Training and awareness is one of the most violated standards, and I believe it is the overhead associated with slicing up the base by roles, job functions and partitioned training that is causing this.
Yes
Yes
• M6 acceptable evidence should be the same as M5.
No
• Seems like the R1 VRF should be low as this does not directly affect the BES reliability, and is more administrative.
Yes
No
1. R2 appears to preclude an awareness and training program that covers all aspects of CIP for individuals who have access to BES Cyber Systems. This would be a more comprehensive way of ensuring that individuals who may have a job scope change in the future are not missed by having to track them and make sure they take another subset of the training pertinent to the new job function. Training and awareness is one of the most violated standards, and I believe it is the overhead associated with slicing up the base by roles, job functions and partitioned training that is causing this.
No
R3 implies that the training programs would be documented at the individual level as opposed to the program level. This suggests that showing that an individual received training may not be considered equivalent to a “documented training program for each individual….”
No
R4 seems to require an entity to document the criteria for pass/fail. While some general criteria could be described, each situation is fact-specific and it’s important that an entity have the ability to make a determination based on the facts and their perception of risk.
No
Disagree with the proposed modifications due to: 1. R6 specifies that “Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. Recently updated CAN-0007 (revised Dec. 9th, 2011) provides a better specification on what constitutes electronic (or logical) and physical access which should be included in this requirement to avoid any misinterpretation of intended requirements. Additionally, it is implied that if during review, a clerical error is identified in which access was provisioned incorrectly, it would be a violation of this requirement. Explicitly calling this out, if intended, is required to reduce unintended inference. 2. R6, 6.1 requirements should read “Identified Authorizers shall authorize electronic access, except for CIP Exceptional Circumstances, to BES Cyber Systems or systems enabling access to BES Cyber Systems (if this is required)." Most organizations have defined

processes for who can authorize this type of access. Adding the “CIP Senior Manager or delegate” increases administrative overhead to sign and maintain delegation letters. Can these requirements be reworded so that CIP Senior manager does not have to be involved in authorizing –either directly or through delegates?
No
Disagree with the proposed modifications due to: 1. In R7, the last paragraph in “Rationale for R7” should directly reference in accordance with the “Guidelines and Technical Basis” provided for CIP 004-5. The information provided in the “Guidelines and Technical Basis” is what is needed to ensure compliance with the requirements, and it should be blatantly obvious to avoid confusion. 2. In R7, 7.1, the requirement should read “. . .to BES Cyber Systems at the time of resignation or termination with verification of access removal and system-generated listing of user accounts showing such persons no longer have access with a maximum of x time”. There needs to be a defined threshold for acceptable maximum timeframe to complete and provide evidence for (such as 1 day, based on the maximum time required for system-based updates). 3. R7, 7.2 again the “Guidelines and Technical Basis” provide critical information for complying with the requirement, and information should be incorporated into the requirement directly. Given that the majority of job transfers require the user to essentially perform the current and prior job functions for some time, a review of permissions should be conducted, however, if permissions are still required, further review should occur during the next quarterly review. 4. R7, 7.3, again the “Guidelines and Technical Basis” should be included to reference the similar requirement indicated for 7.1 to remove unescorted physical access and Interactive Remote Access, with 30 days to remove all other local access permissions. 5. The drafting team should make it clear for reassignments or transfers that continued access should be allowed for a previous role for a period of time determined by an entity to be "necessary" to complete turnover and previous duties.
No
How does one document a technical implementation purchased from a vendor? How does one measure if that document proves sufficiency in impmentation? Highly recommend plagiarizing from NIST / ISO-27001/2 for appropriate control statements.
No
Most modern attacks originate using 'non-interactive' channels 'interactively.' Highly recommend plagiarizing from NIST / ISO-27001/2 for appropriate control statements.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with. Request Requirement 1.2 be updated to allow "escorted physical access." Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).

No
1. Need clarification on what disabling a physical port would entail. 2. A targeted audit of a static list in dynamic environment will almost always find a control failure.
Yes
No
3.4 Need clarification of the required/expected login and tracking process for a transient cyber asset.
No
• Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. • Request clarification on 4.3, does the failure need to be detected within a calendar day? • Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested two weeks.
Yes
Disagree with the proposed modifications due to: 1. In the “Guidelines and Technical Basis” section for R5, 5.3 should read “Where possible, any default accounts provided. . .”. This was simply missed. In 5.5, the sentence in the last paragraph on page 43 should read “Password complexity refers to . . . passwords to have the following types of characters:. . . “. If all four are required, as indicated by the “and” separating the four characteristics, then this sentence should be fixed to eliminate conflicting requirements. 2. For R5. 5.2, having a separate list or administrator, shared, default, and other generic accounts, signed by the CIP Senior Manager, creates more work. This requirement can be met during the quarterly access review of all BES Cyber System accounts reviewed by appropriate, designated Approvers. 3. Need clarification on 5.5.3 - not able to extract what is required under this standard.
Yes
Yes
Yes
Yes
• Applicability section in table seems to be mixed between All Responsible entities and High/Medium Impact BES Cyber Systems.
Yes
No
For 1.4, clarification is required. Is this a backup media verification process? If not what is the intent? Does this mean that for every backup (full/incremental) that a log is kept, and if so, for how long?
No
Request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current. What is the preferred sample size (all assets/system based) or a representative grouping (db/web/app)?
No
Does this mean a recovery test for each asset or a representative grouping of assets? Can I recover(drill or exercise) what is a full operational exercise in R2.1? Can I limit to an individual asset or sytem?
No
• Requirements – 1.1.6 – Clarify “security-patch” requirements. • Requirements – 1.2 - “Authorized” should be “Authorize”. • Requirements – 1.4.1 – Define “cyber security controls”. • Requirements - 1.5 – Some BES Cyber Systems may not have comparable test environments. Testing in non-CIP

production assets before implementing in CIP environment should be allowed.
Yes
2.1 – Measures – Clarify meaning of “records of investigation” (change record, incident record, e-mail).
No
Disagree with the proposed modifications due to: 1. R1 1.1 lacks specificity as to what is required. Verbiage should be clarified to express whether the sub requirement is requesting a documented process for identifying applicable BES Cyber System Information, or that there is an information classification process in place and being followed to label applicable BES Cyber System Information. 2. The evidence examples provided in 1.2 are nebulous, and in some cases difficult to provide (e.g “hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals”). It should be clearly stated, if required, that approvals must include attestation that user access to BES Cyber System Information was granted based on a “need to know” basis.
No
Disagree with the proposed modifications due to: 1. As currently stated, 2.1 speaks only to BES Cyber Asset media, however BES Cyber System Information may reside on devices that are not BES Cyber Asset media (such as in printer memory, email servers, etc.). Given that CIP-011-1 R1 assumptions directly references “Information handling procedures should detail access, sharing, copying, transmittal. . .”, clarification that specifies any system that contains BES Cyber System Information should have media cleared, purged or destroyed prior to reuse or disposal should be specified, if that is the intention of the requirement. 2. The Standard (applicability) is sufficient, but not wide spread enough as it should cover all computer processing and storage assets (Cyber Assets) within the BES. The data contained on servers in a well-constructed infrastructure is stored on secured disk arrays. Individual processing units or storage devices connecting to these resources or attain data through a secondary transfer can collect confidential data. If the asset falls outside the standard, the data contained on the device can move beyond the established security perimeter. Any asset that provides a data storage capability that is within the security perimeter or enters the security should fall within the standard. 3. Requirement R2 “Guidelines and Technical Basis” information requires clarification to state whether strong encryption used on media besides a SAN is considered acceptable. 4. The standard states “Media Reuse and Disposal” is a requirement, but does not provide guidance of what is required for reporting “Evidence”. This leaves the method of what information or actions required open for interpretation. Specific definitions and requirements would allow Vendors to the BES provide solutions to meet destruction requirements provided for reporting and improve internal processes to meet this standard.
Yes
Group
NRG Energy Inc.
Patricia Lynch
Yes
1) The control center definition is in conflict with the requirements in Medium Impact Rating of CIP-002 Attachment I as it does not fully address or delineate those generation facilities that control small remote units on a different footprint from the centralized control room. . These units collectively may be significantly under the 300 MW threshold as indicated in 2.13 and present no risk to the BES, yet can be defined as control centers at medium impact as they are physically located on a different footprint. 2) The definition of BES Reliability Operating Services does not address whether read-only operating data which is displayed for situational analysis and decision making through voice communication needs to be protected under the CIP standards (ex. PI, RIG displays, Historian)
Yes
1) Although the BES cyber systems have been explained in detail, the allocation of impact for various BES cyber systems is not written clearly that classification of these systems is based upon

categorization of devices based upon site characteristics per Attachment I. It is not clear if BES cyber systems at a facility can have numerous levels of impact. 2) For facilities that control blackstart resources, it is not clear in Attachment 1 if all BES cyber systems within the confines of the control room would be considered for inclusion in CIP security, and if so, if they are considered medium impact. 3) In Attachment I-2.1, there are two different resulting interpretations as to how the 1500 MW threshold is applied. One is that if BES cyber systems in a facility are tied together and control more than 1500 MWs collectively, they would be in scope. The other interpretation is that all BES cyber systems are in scope for a facility of multiple generators that collectively produces 1500 MWs, whether the BES Cyber systems are tied together or not. This ambiguity should be removed.3) Under Attachment I 2.6, Transmission facilities operating at 500 KV or higher are included. Would this address facilities that essentially are radial leads with no load flow through? 4) For generation facilities that require notification from the Planning Coordinator or Transmission Planner for inclusion under medium impact, this must be placed on a frequency for notification and provide ample time for remediation 5) Since the aspect of qualifying connectivity has been removed in this set of standards, is it assumed that all relevant requirements need to be included for the various impact levels regardless if the devices are isolated? This needs to be explicit.
Yes
No
This should be stated clearly that this initial and annual review applies to all BES Cyber assets impact levels, regardless if the entity has not identified High or Medium BES Cyber Assets or BES Cyber Systems.
Yes
Yes
Yes
Yes
No
This requirement should state that training on relevant policies associated with job function are required.
No
The authority for subsequent delegations may result in reduced oversight and control.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
In Table R6, the Senior manager or delegate may be too far removed from the actual access control

process to authorize individuals and provide access permissions.
No
In large organizations that cross many regions, revocation under R7.1 concurrent with termination may not be possible if there are numerous BES systems that require coordination of revocation at that time
Yes
No
R1.1 does not clearly explain that an electronic security perimeter or technical controls is required for all low impact BES Cyber systems
Yes
No
R1.3 requires use of two or more complementary physical access controls appears to be excessive whereas one robust physical control can avoid unauthorized access.
No
Under this requirement, there are less restrictions for visitors than required for employees.
Yes
Yes
Yes
No
1) Security patch management does not spell out the required level of patching requirements. Should third party application be included? And what about parsing programs or scripts written for data collection, DVD drives, etc. which do not impact the functionality of the BES system? Please delineate all levels of required patching. 2) Patching that cannot be supported by devices will still require TFEs at medium and high impact levels. 3) Assessments on Vulnerability notices may take more than 30 day period. 4) What is the CIP Exceptional Circumstance definition? It is not listed.
No
TFEs would still be required under the medium or high impact levels unless these systems are upgraded or replaced.
No
If an high or medium impact system is required to alert in real time for events that necessitate a real time event in R4.2, why is necessary to review a sampling every two weeks under R4.5?
No
1) Under R5.2, The senior manager or delegate may be too far removed from the actual access control process to authorize individuals and provide access permissions for various accounts. 2) CAN-0017 is in direct conflict with R5.5 which allows either technical or procedural controls for enforcement of password parameters. CAN-0017 forces TFEs unnecessarily.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Authorization under R1.2 by the CIP Senior Manager or delegate to document changes to the BES system that deviate from the baseline configuration may be considerably out of scope for these individuals. This includes maintenance activities such as patching.
Yes
Yes
No
Labelling of all devices and associated information is excessive and at the level of nuclear grade security.
Yes
Yes
No
There is a direct conflict with Version 4 and version 5 of the standards concerning overlap of time for implementation, if version 4 is not immediately approved. Secondly, if this was to occur, there may be conflicting requirements-ie CIP-002 R2.13 does not exist in V4 for same level of impact and remediation
Group
Imperial Irrigation District (IID)
Jesus Sammy Alcaraz
No
No
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Depending on the criticality of the device in question the VRL & VSL should be classified. Not all assets are the same and the language does not provide any room for type of assets
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
No
Part 3.2; 3.3, 3.4, 3.5 Due to limited resource, IID would like to change the response with additional 60 calendar days to current propose.
No
IID suggested the VRFs and VSLs should be at lower risk or moderate risk.
Yes
Yes
Yes
Yes
Yes
Yes
No
IID'S position does not agree with the combining of these two vulnerability assessments. IID feels that they should be kept separate.
Yes
Yes
Yes
Yes
Yes
Group
Western Area Power Administration
Brandy A. Dunn
Yes
1) “Transient Cyber Assets” are defined as directly connected devices. However, external cyber assets used for transient remote access are not addressed and no security controls are required for such devices. Since CAN-0005 asks if system operator laptops are CCAs (or …”are system operator laptops parts of the BES system?”) and this CAN is still outstanding, we recommend revising this definition to address direct and remote transient devices in CIP version 5 so CAN-0005 will be retired. 2) Add clear definitions of “physical access revocation” and “cyber access revocation” so CAN-0007 – Revocation of Access may be retired.
Yes
a) General - Study based exceptions should be allowed. Given that a substation may fall into the

medium category under the bright line criteria, an entity should be able to show through study work that loss of the substation does not lead to voltage collapse or cascading outages, and thus exclude its inclusion in the medium category through studies. b) General - The method used to determine classification of facilities is too proscriptive. Use of Short Circuit MVA coupled with study work showing that loss of the bus(es) at a substation do not lead to cascading or voltage collapse should be sufficient to show that the facilities should be classified as low. c) General - CIP-002-4 changes the risk based assessments to a more proscriptive method. The industry does not have a good measure of what those changes will lead to, yet is expected to accept additional changes in this version 5. The industry should be allowed to gauge the changes from version 3 to version 4 and operate under the new version before being asked to vote on acceptance of version 5. d) General - The "Guidelines and Technical Basis" section of the standard is problematic. It basically states that any element or system of elements that has an adverse impact on BES services should be listed. This is an issue because elements incorporated into the BES will always have an impact, otherwise they would not exist. This section of the standard goes on to define conditions that will always skew the impact toward adverse, and the impact is not quantified, so the reader is left with the implication that any adverse impact requires listing of the asset. Perhaps this is the intent, and if so why have the pretense of the "bright line" criteria? Simply declare all BES transmission elements as Medium and be done with it. Otherwise, the level of impact needs to be defined such as "additional elements which, upon loss, will lead to voltage collapse or cascading outages" in addition to or instead of the specific "bright line" criteria defined in Attachment 1 of the standard. e) General - Attachment 1 is written in the context that Version 4 is in effect and the entity has already performed the "bright line criteria" assessment of its facilities and has a completed list of CAs and CCAs. But if Version 4 is skipped (as described in the Version 5 implementation plan) then the Attachment-1 assessment process will require revision. It is not logical to assess cyber asset and cyber system impact on ROS impact as the first step. This approach would require the assessment of every single asset at all facilities to determine high/medium/low rankings, versus assessing & ranking facilities first, then assessing devices only at the high and medium ranked facilities. As described in the Version 4 Attachment 1, facilities supporting ROSs should first be determined, and then the cyber assets supporting those facilities and services can be assessed. f) Attachment 1, 2.4 and 2.5: The fact that a facility is identified in the TO's restoration plan does not imply that the facility is crucial to the plan. Given that multiple Blackstart Resources are available, then using the logic applied in the Application Guidelines, all these resources should not be deemed critical, and in fact none should be for these criteria. g) Attachment 1, 2.7: The "weight value per line" used to determine total weighted aggregate value does not allow for variations in various owners' systems. Many owners have 230 kV lines that are not capable of carrying 700 MVA as detailed in the Application Guideline. Provisions should be made to exclude facilities that can be shown to not lead to cascading or voltage collapse upon their loss. h) Attachment 1, 2.8 and 2.9: The standard is placing a burden upon the TO for actions of others, that the TO has no control over, with no allowance for coordination or negotiations for potential changes in the determination of IROLs. Previously stated in this standard, the TO has 30 days to place the facility on the Critical list, yet nowhere in this standard is there a requirement for the outside entity to communicate its proposed inclusion of the impacted TO's facility as a potentially higher rated facility. This would be problematic for the TO because if a new IROL was unilaterally declared by the outside entity, the 30 day clock may start before the TO is aware of the issue, in which case the standard could be violated by the TO for actions outside the TO's control. i) Attachment 1, 2.11: Given that the SPS could have an impact on IROLs, this standard implies that all components of the SPS are designated as medium without regard to whether loss of those elements of the SPS system would lead to the referenced IROL violation. The SPS can be designed so that incorrect readings or misoperation of a given element of the system has either no impact or acts to run the SPS in the "safest" manner. If this is the case, the individual elements of the SPS should not require a medium designation, and should be allowed for in the standard. j) Attachment 1, 2.12: The standard and the Application Guidelines do not indicate whether the 300 MW limit is a system limit or an entity limit. Discussion in the application guidelines started to define the load shed discussion to a single location, but then fogged it up again when the discussion brought in the term "system", and thus spread out the load again. This area needs to be more clearly defined. This could be done by inserting "aggregate" if the net potential load shed is the trigger or "discrete" if only concerned about loads at specific sites over 300 MW. k) Attachment 1, 2.12: Given that a system results in load shedding over 300 MW, if the system is a set of relays set to work on observation of a system variable such as frequency or voltage, independent of the other elements of the load shedding system (ie relays at substations distributed across the TO's system, set

to trip for various under voltage or frequency levels, but not in communications with each other), it is not necessary to declare each of the relays and therefore each substation as medium assets. l) The discussion in the Application Guidelines under transmission part 2.7 (page 28): This section claims that the average MVA line loading used in a report used as a reference for quantifying risk is 700 MVA for 230 kV lines, and 1300 MVA for 345 kV lines. It is not clear where this averaging took place, but at least one TO is outside the norm, with emergency ratings of the highest rated line of each voltage class under 72% of those values, let alone the average line loading. This goes directly to the greatest weakness of this revision of CIP-002-5, and that is that the standard does not allow for systems that are different than the model system used to baseline the standard, nor does it allow study-based exceptions.
No
1) See above comments on Attachment-1 – if Version 4 is skipped, then CIP-002-5, R1 is out of context; it prescribes a required process backward to what would logically be done to determine BES-CAs and BES-CSs. 2) R1-1.1 requires the identification and categorization of changes from lower to higher within 30 days. Does requirement 1.1 refer to inclusion of the element or facility on the BES Cyber Assets and Cyber System list, or does this requirement include the entire scope of CIP-002 actions including the signature of the CIP senior officer?
Yes
No
Under the Table of Compliance Elements is included the phrase “Operations Planning” under the “time horizon” column. The industry cannot predict with certainty future upgrades and additions to the system, yet the standard appears to state that VSL apply to the planning time horizon under the “time horizon” column. It may be that the standard intends to apply to operations only, but this is not clear in the text since both “Operations” and “Planning” are capitalized. Please clarify.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
CAN-0048 is in development to clarify acceptable sources of ID verification. CIP-004-5 R4.1 requires identity verification but does not address what is acceptable. NIST Special Publication 800-63 has an acceptable description of Identity Proofing Requirements by Assurance Level, where assurance levels are Level 1 (low) through Level 4 (high). Please identify acceptable ID verification methods, for instance by identifying High Impact BES Cyber Systems as needing Level 4 Identity Proofing Requirements, and Medium Impact BES Cyber Systems as needing Level 3 Identity Proofing Requirements, as documented in NIST Special Publication 800-63.

Yes
No
Table R6, Part 6.3 includes the requirement that access to BES Cyber system Information be controlled to the degree that “Access permissions shall be the minimum necessary for performing assigned work functions.” This requirement will place undue, onerous, and unmanageable restrictions on drawings, diagrams, etc. This requirement could result in hundreds of information categories; feasibly one category for each employee. It is reasonable to protect this information from public release, but unreasonable to require that an entity classify information down to the “assigned work functions” level. We recommend removing the words “Access permissions shall be the minimum necessary for performing assigned work functions.” from CIP-004-5, Table R6, Part 6.3. Also please remove the words, “and the minimum necessary for performing assigned work functions” from CIP-004-5, Table R6, Part 6.6.
Yes
No
Too highly ranked VSL for information protection violations
Yes
No
Project 2009-26 is an interpretation asking whether indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access shall be considered supervision of electronic access. This has not been adequately addressed in CIP-005-5, or CIP-007-5. The drafting team should either require that entities have documented procedures for supervised electronic access or the drafting team should specifically state that no supervised electronic access is allowed.
No
CAN-0031 – Acceptable physical opening dimensions. The six-wall border is eliminated. Does that mean that opening dimensions are also immaterial? CAN-0031 is in response to a request to define the entry point metric definition of the access points on the perimeter. NERC also received a request for clarification for an acceptable entry point into a Physical Security Perimeter (PSP) as well as acceptable opening dimensions. Recommend including the wording from CAN-0031, “That any opening that does not have physical preventative measures in place is less than 96 square inches. That any opening greater than 96 square inches, with its shortest side greater than 6 inches in length, is protected against entry by the use of bars, wire mesh or other permanently installed barrier that leaves no opening greater than 6 inches on its shortest side.”
Yes
No
Testing of these systems every three years is sufficient. There will be too many systems to test on a two year schedule. Also – if monitoring of the access control systems is required and use of the system proves it is functioning, the two year cycle becomes highly redundant.
No
CAN-0019 is in development to answer the question, “What is the acceptable time to install a software patch before a TFE is required?” CIP-007-5 R2 states that a remediation plan must be developed within 30 days, but does not answer the question. Please identify an acceptable interval for completion of the remediation plan. Is one year too long? Can a remediation plan state that implementation will start after 6 years?
No
R3.5 requires the logging of “each transient cyber asset connection”. This is not only a large burden

for Maintenance staff performing daily operations, but difficult (or impossible) to audit accurately.
Yes
No
Project 2009-26 is an interpretation asking whether indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access shall be considered supervision of electronic access. This has not been adequately addressed in CIP-005, or CIP-007. The drafting team should either require that entities have documented procedures for supervised electronic access or the drafting team should specifically state that no supervised electronic access is allowed.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Version 4 must pass to get the ‘bright-line criteria’ in place first or Version 5 will be too large of a leap in the assessment process, cause confusion, and be very difficult to audit. Western recommends NOT skipping version 4.
Individual
Richard Salgo
NV Energy
Yes
BES Reliability Operating Services – Dynamic Response to BES Conditions: Please provide clarity as to the intent of the term “sensors” as used to describe SPS, UFLS, and UVLS. Does this refer to instrument transformers, and if so, isn’t this overly expansive? Also the “breakers” included in these items are not cyber systems and should be deleted. BES Reliability Operating Services – Managing Constraints: The inclusion of ATC and unit re-dispatch/unit commitment appears to be outside the

realm of “real-time” (15 minute threshold). Rather, these considerations are most typically hour-ahead and day-ahead in nature. Suggest deletion of these two items or re-write to emphasize that the scope is limited to real-time functions in these areas. BES Reliability Operating Services – Situational Awareness: The inclusion of “Current Day and Next Day Planning” is outside the realm of the stated 15-minute threshold for real-time. This should be removed.
Yes
TO/TOP Control Centers in 1.3 are contingent on controlling one or more of the assets listed at the end of 1.3. This list includes 2.12, which is UVLS and UFLS. Suggest deletion of this item 2.12 from the list in 1.3, as Control Centers cannot and do not manipulate the operation of UVLS or UFLS. UVLS/UFLS are discrete relay systems typically located in distribution systems distributed throughout the BA or TOP area, and have no linkage to particular control centers. GOP Control Centers in 1.4 similarly are qualified by control of assets identified including 2.12 (UVLS/UFLS). Again, the inclusion of UVLS and UFLS for a control center, and more particularly, a GOP control center, is inappropriate. Transmission Facilities 500kV or higher, 2.6: This should be qualified as “networked” 500kV, so as to exclude radial 500kV facilities, which are performing a distribution function. Transmission Facilities 200-500kV, 2.7: This item should be changed to specifically exclude radial and local network (see Project 2010-17 BES Definition) facilities from consideration in the weighting calculation. UVLS/UFLS 2.12: As a matter of principle, UVLS and UFLS should not be included; this item should be deleted. UVLS and UFLS are deployed at the distribution level and are not controlled via any common control system. Inclusion of these sorts of distributed discrete relay elements is extremely expansive, and does not appear to offer any benefit to cyber security of the BES. Version 0-3 only included such schemes if they were under “common control” and shedding 300MW or greater. If deletion is not agreed to by the SDT, then it may be acceptable to add a qualifier of “under common control” to this item. Also, it is not clear whether the phrase “as required by its regional load shedding program” modifies both UVLS and UFLS or simply UFLS. Generator Control Centers, 2.13: It is unclear what is the definition of the generation control center as used in 2.13. If this item is retained, the SDT should clarify the definition of a generation control center and specify that the 300MW generation threshold is limited to BES generation only.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
From the structure of the table in R2, it appears that the Requirement calls for training on all ten aspects 2.1 through 2.10 for all individuals having access to medium or high impact BES cyber systems. This would not allow the appropriate degree of role-based training differentiation and will

therefore require unnecessary training for many individuals.
No
The statement of R3 indicates that the entity shall implement its documented training program for individuals needing access that includes each of the applicable items in Table R3, but Table R3 doesn't contain any "applicable items". Does this reference really belong to Table R2?
Yes
Yes
Yes
Please clarify in Part 6.5 whether the intent is that there be a review conducted on an individual by individual basis that their access is appropriate, or does this call for a review of the access rights for each type of "role"?
No
Concurrent revocation required in Part 7.1 will be virtually impossible to comply with. As with any task that requires human intervention and consideration, there will necessarily be a time lag between the action of termination and the steps that are taken to revoke certain elements of access.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Individual
John Martinsen
Public Utility District No. 1 of Snohomish County
Yes
Comments: Refer to additional comments submitted for Question 49. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
Comments: Recommend that 2.8, 2.9 and 2.11 start with “Applies to all Regions except…” For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
Comments: For clarity, request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days when a change to BES Elements and Facilities is placed into operation”. For clarity and consistency with the previous change, request changing M1 from “as required in R1 and list of changes to the BES (” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards

Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation "requirements" in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.

No

Comments: Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation "requirements" in a guidance document rather than in the requirements in the standard.

No

Comments: The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4's making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.

Yes

No

Comments: The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from "Changes to the CIP Senior Manager and" to "Changes to the CIP Senior Manager or".

No

Comments: Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This

question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
Comments: For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
Comments: For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
Comments: For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Comments: Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
Comments: Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point

or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Comments: Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Comments: Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in

Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Comments: Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Comments: Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
Comments: Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
Comments: For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
No
Comments: Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be

at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: 2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.

No

Comments: Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .

No

Comments: For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new

requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
Comments: For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
Comments: Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Comments: Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.
No
Comments: For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.
No
Comments: Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-

002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Comments: Request that footnote 2 in 2.1 be moved into that Requirement.

No

Comments: The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.

Group

NESCOR/NESCO

Annabelle Lee

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Definitions: Clarify definition of Electronic Access Point Electronic Security Perimeter – definition does not say clearly that this has to include ALL interfaces from outside the BES(s) being protected. Suggest change to: “The collection of all EAPs that permit communications to a BES system from a device not in that system.” Note that existing definition of EAP says “restricts” rather than "permits.” Unsure of the specific meaning of “restricts". As stated in the document, "...from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities." Redundancy is not an appropriate mitigation for all vulnerabilities, but it is a mitigation for some. NERC may want to consider revising the sentence and being more specific when redundancy is not appropriate. As stated in the Table of Compliance elements, "100 High and Medium Impact BES Cyber Assets." Why are only cyber assets listed and cyber systems excluded? As stated, "The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” The term element is not defined nor related to cyber assets/systems. NERC may want to consider adding a definition for element. NERC may want to consider adding iteration/feedback loops to the use case CIP process flow diagram. BES Cyber System mentions the phrase Maintenance Cyber Asset. This phrase has no

associated definition. There is no explicit reference to generator control rooms in the definition a Control Center. It should be made clear if a generator control room is included or not.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Attachment I, Medium Impact Rating (M): This is of particular concern given that there is a push from FERC and congress that more generation be inclusive in the application of cybersecurity controls. The wording of this measurement has had much debate over the last several months and there isconflicting understanding on what this actually entails. Based on the latest information, the SDT has stated that this would be 1500 MW attached to a single DCS (for example). As currently written, this means that a single facility with multiple generation units at 1499 MW or less that are attached to separate DCS' would not reach the category of medium. An aggregation of generation capacity per facility should be considered. Attachment 1: Text before 2.1, 2.2 does not read correctly in connection to those items. We are unsure how it should be corrected. Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. The SDT may want to consider criteria 2.4 be modified to read “Each Blackstart Resource identified in its Transmission Operator’s restoration plan used to provide power for remote start of another generation unit(s)”. Attachment 1: Blackstart plans for resources used for load restoration purposes may be inadvertently included in the existing definition, specifically criteria 2.4. The Cranking Path diagram on Page 26 implies that Blackstart resources are only included where used to start a unit. The SDT may want to consider criteria 2.4 be modified to read “Each Blackstart Resource identified in its Transmission Operator’s restoration plan used to provide power for remote start of another generation unit(s)”. Attachment 1: Criteria 2.11 contains the words “…if destroyed, degraded, misused”. (Twice). This appears to be a carryover from version 4, but it now is redundant and perhaps conflicting with the “15 minutes” qualification as defined at the top of the Medium Impact Rating section. Attachment 1: Criteria 2.12 refers to a “system” – as in “Each system or Facility…” – that implies something of a cyber nature. The rest of the bright-line criteria refer to or describe hard assets, not cyber assets. This seems like an odd exception. The SDT may want to consider removing “Each system or”. Attachment 1: Page 30 of the draft standard contains an example methodology or process flow for categorizing BES Cyber Assets and BES Cyber Systems. This graphically illustrates the overall intent of the SDT for CIP-002-5. However, when you boil down all the security controls in CIP-003-5 through CIP-011-5, there really isn’t any appreciable difference between High and Medium requirements. The SDT may want to consider modifying items 1.1 through 2.13 on Attachment I to be “All these assets have a Critical Impact Rating”. Requirement 1 would therefore be “For all cyber assets including associated physical and electronic access control and/or monitoring systems and associated protected cyber assets, that support one or more BES reliability operating services at a Critical facility, apply the controls as specified in CIP-003 through CIP-011”. If there are cases (like CIP-010-5-R3.2) where specific “High Impact” systems are intended, then the SDT could consider stating so in the requirement; “For Control Centers, perform an active vulnerability assessment every 39 months…”. Although the addition of "within 15 minutes" does lend itself to a "bright-line" criteria, it may be arbitrary in the event that a BES Cyber Asset or BES Cyber System is unavailable, degraded or misused and one or more BES Reliability Operating Service becomes "adversely impacted" at the 16 minute mark or longer. Why is an adverse impact happening within 15 minutes any less important to the BES than one happening in 20 minutes? Attachment 1: The term "adversely impact" is not clearly defined. Attachment 1: A concern with the 15-minute time limit is that it is really related to the ability to make generation with the contingency reserve available within 10 minutes of a disturbance and then allow the Transmission Operator/Balancing Authority to restore firm load within 15 minutes of a disturbance. The methodolgy does not equate on the security side. The security side is that you are attempting to reduce the risk that you have to recover within 15 minutes. A possible approach is to prescribe protective measures by facility type, system type, and device type. Attachment 1 is a good start, but it could be rewritten to be specifically based on preventing the need to restore. Attachment 1: Suggest changing wording “would, within 15 minutes, adversely impact” to “could adversely impact.” There is a significant difference between would and could. A more specific definition of “adversely impact” would be useful, but it is unclear whether this is practical given the number of BES reliability operating services and the utility circumstances. Multifunctional devices as high impact assets: Attachment 1: Handling of multifunctional devices identified as high impact assets, for example, protection relays may be addressed through sets of restrictive non-functional requirements. Besides of its protection function, digital protective relays typically provide monitoring

and reporting functions. CIP may be too restrictive or lacking guidance on how to approach accessing the protective devices and other multifunctional devices to allow for data and report retrieval. This is considered a significant problem by power utilities and currently they are restricted on how to retrieve and use recorded data and reports remotely.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Clarify – is each cyber asset categorized EITHER alone OR as part of a BES system? Since the BES system concept is a major change for v5, a bit more explanation would be useful. What constitutes a “change to BES Elements…” per part 1.1? The SDT may want to consider modifying this language to simply state that new or retired assets be added or removed from the list within 30 days of commission or decommission. For M1, we believe the intention is that entities are not specifically required to list their Low Impact systems. Therefore, the SDT may want to consider modifying the last sentence to “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems is not required, but instead may be demonstrated by the application of the required controls”. (New words are “is not required, but”)
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months…”, this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year..." Similarly for “every 39 months…”. To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc. This wording precludes attempts to extendthe word "annual" to mean longer than one year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z". The SDT may want to consider that this requirement and all others that use the words “…initially upon the effective date of the standard…” have this phrase stricken. The implementation plan that accompanies the final approved draft should include the requirements for first time iteration of periodic activities. It’s not reasonable to assume that every entity is capable of executing all procedures “upon the effective date”. Minor point, but this is the first time “CIP Senior Manager” is used in the standards. Perhaps add a cross-reference to the appropriate requirement in CIP-003-5. In section “B. Compliance”, under sub-section “1.2 Evidence Retention”, there is a typo in the second to last line. Please change “complaint” to “compliant”.
Yes
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The need for cyber security policies that address the BES Cyber Systems is prudent; however, it appears that the required topics to be addressed may not be holistic and/or fully appreciated without more description. For example, does Personnel Security include Training and Awareness policies? Would an entity know to include policies addressing Monitoring & Logging in the topic System Security? There does not appear to be specific policy requirements to address Application Security, provisioning, forensics or cryptography. The list of topics does not include such items as: access control, training and awareness, audit and accountability, I&A, planning, risk management, information system and information integrity, continuity of operations, information system development and maintenance. Please consider looking at the full list of families included in NISTIR 7628 and consider augmenting the topics list. As stated, "BES Cyber Systems." This does not include BES cyber assets or facilities. Please clarify. Application Guidelines for R2: There are a number of technical issues raised here that, in some cases, can be technically enforced, and not just required by policy. Consider moving and/or adding these to other CIPs where they are more appropriate. Also many of these issues go beyond the scope of the standards and are not required for compliance. This may cause confusion as to what is required for compliance. Organization stance on use of wireless networks (this would be optimally addressed in CIP005) Monitoring and logging of ingress and egress

at Electronic Access Points (this is in CIP007 R4.1.1) Maintaining up-to-date anti-malware software before initiating interactive remote access (is in CIP007 R3.4) Maintaining up-to-date patch levels for operating system and applications used to initiate the interactive remote access before initiating interactive remote access (this would be optimally addressed in CIP007 R2.x) Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access (this would be optimally addressed in CIP005) For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s interactive remote access controls (this would be optimally addressed in CIP011 R1.x) Monitoring and logging of physical ingress and egress (this would be optimally addressed in CIP006 R1.x, noting that egress logging / monitoring in not in the current CIP standards) Availability of spare components (this was in CIP v1-v4, but doesn’t appear to be in CIP v5) Break- fix processes (this would be optimally addressed in CIP010 R1.x)
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This rule states "...individuals who have access to BES Cyber Systems..." This could be emphasized to state that the "access to BES Cyber Systems" means logical and/or physical access. Even techs without cyber access to equipment in substations, for instance, should nevertheless be aware of the cyber security policies governing that equipment, such as, for example, no use of thumb drives.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Are the measures listed under M5 meant to be prescriptive? These are very specific and imply requirements. Throughout the standards, measurements are now tightly tied to requirements and are much more prominent. However, examples should be stated as examples, so that “measures” do not become “requirements” . The SDT may want to consider stating (somewhere) the compliance applicability of Measures. In the second bullet under M5, CIP-002-5 R3 is mentioned. There is no R3 in CIP-002-5. In the last sentence in the last bullet under M5, the bullet is one huge run-on sentence, confusing, and should be redrafted for clarity.
Yes
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R1.1: If awareness is provided only to personnel with authorized electronic access and/or authorized unescorted physical access, it could still be possible for personnel without appropriate awareness doing unrelated work on systems in other networks such as the enterprise network to infect systems in those networks. This malware might then be used to stage attacks against electronic security perimeters protecting BES cyber systems. The Rationale for R1 indicates that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems are to maintain awareness of best security practices. Neither the R1 requirement language nor the R1.1 table requirement make mention of best security practices rather the requirement states security concepts. Also, It would seem that if the expectation is for those personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems are to be the recipients of such awareness then the requirement should be explicit in that regard. It was noted that the Change Rationale for R1.1 states "Changed to remove the need to ensure everyone with authorized access receives this awareness" which appears to be counter to the Rationale of R1. Responsible Entities does not appear to include operators, specifically, those who operate the BES cyber system and/or BEST cyber assets. Operators should also receive training.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Parts 2.2 and 2.4 seem somewhat redundant. If there was a specific distinction intended by the SDT, please consider rewriting to make this clearer. For example, 2.2 could be reworded to add the clause “including electronic access controls” OR 2.4 could be reworded to say “The training

required under 2.2 shall include training on electronic access controls."
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Users of low impact BES cyber systems/assets also need basic cyber security training. Consider revising the training requirement to include basic cyber security training for all individuals. One potential oversight in all versions of the CIP-004 standard is guidance on the training requirements for "transient" workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R3 (or Part 3.2) to make clear the requirements for this category of worker.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R4.1: Without requiring verification of credentials, e.g., government issued photo ID, how is the utility able to trust an employee's identity? R4.2: The requirement only states criminal record checks and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries and reasonable for both cyber security and safety. There should be consideration in this requirement to include drug and alcohol testing within the constraints of state laws and collective bargaining agreements. R4.2: The criminal check record is private confidential information and, therefore, needs to be stored securely. R4.4: It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). In many cases, these contractors and/or vendors, have been working for utilities for many years without any background or criminal check. What if the utility cannot get all that information? What if a utility finds something from the criminal record of a contractor who has been with them for several years? In these cases, what should the utility do? R4.4: Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIPs? R4.4: Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similiar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. One potential oversight in all versions of the CIP-004 standard is guidance on the PRA requirements for "transient" workers. By transient, we mean persons whose access is either temporary, or perhaps is granted and revoked on a periodic basis due to project work. The SDT may want to consider adding some words to R4 to make clear the requirements for this category of worker. The Applicability sections of R4 and R5 are different and it doesn't make sense to design a PRA process for one set of assets, but implement it for a different set.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Parts 6.1, 6.2, and 6.3 state that "access permissions shall be the minimum necessary…" This appears to be a goal and the SDT may want to consider moving this sentence to the Rationale or Guidelines section. Part 6.3 should include a cross-reference to CIP-011-1-R1.2, as in "…as documented in the entities information protection access control procedures in CIP-011-1-R1.2." Parts 6.1, 6.2, and 6.3 include the qualifier "…except for CIP Exceptional Circumstances". For consistency, this language could either be stricken, or amended to include a reference back to the entities CIP Exceptional Circumstances policy per CIP-003-5-R2. Please clarify whether Part 6.5 applies to cyber access or physical access, or both. The notion of "groups" can theoretically apply to physical access to control systems as well as cyber access. Part 6.6 appears to be redundant to the annual information protection review performed per CIP-011-1-R1.3. Per an earlier comment, the "minimum necessary" language throughout R6 may be difficult for entities to prove and the SDT should consider moving it to the Rationale or Guidelines section.

No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Extended leave situations - such as a sabbatical, employee behavior/performance suspensions or maternal/paternal leave - are not identified as a reason for revoking or suspending access. Given the criticality of the environment being protected, reducing the privileges to only those who have a need for access as a part of current job duties should be maintained. These specific role changes perhaps could follow the requirements for transferred or reassigned personnel; however, it should be made clear in the requirement or Guidelines and Technical Basis section how to manage these common personnel situations. In the Guidelines and Technical Basis, there is a table that identifies that no action is required for death. The SDT may want to reconsider this requirement. Revocation of access privileges for the deceased is an important action. Dormant accounts with privileges could be misused. By removing such privileges, the entity is reducing their overall attack surface as well.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. In the Guidelines section of CIP-004-5, the last sentence under Requirement R3 (and again under R4) states “…by the single senior management official identified in Requirement R1”. This should be re-written to say “…by the CIP Senior Manager or delegate identified in CIP-003-5-R1”. In the Requirement R4 section of the Guidelines, the reference to CIP-011 is a typo and should state CIP-004. In the Requirement R6 section of the Guidelines, the last sentence of the first paragraph could be modified to state “Best practice recommends that access authorization and provisioning should not be performed by the same individual”. Some entities are too small for strict separation of duties to be feasible.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have the integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. Cyber assets associated with data networks and data communications links between discrete ESPs, rather than being exempt from CIP requirements, could be specifically included, and exempt only when all communications between those ESPs are encrypted and have their integrity assured. IPSec VPNs have been a mature technology for many years, as are SSL VPNs. Given that these technologies are widely used in other industries, and that devices implementing them are available in industrial- and substation-grade form factors, we recommend that all routable communications, not just remote access connections, be protected with strong encryption and integrity (message authentication), using encryption technologies such as site-to-site secure VPNs. Secure VPNs should not be confused with technologies such as MPLS and GRE that can segregate traffic, but do not encrypt, and are therefore only secure if every intermediate device in the traffic path is secure. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. If communications assets are exempt from the CIPs as the draft currently states and communications are not encrypted and integrity verified, then every radio, modem, hub, communications device, wire, and fiber can provide an attacker with access to and the ability to falsify critical control system communications. This particularly applies to most private WANs leased from communications service providers: if communications over private WANs are not encrypted, then compromise of the service provider via mis-configuration, vulnerabilities in equipment, or insider collusion by employees of the service provider, could lead to compromise of multiple utility communications networks. This particularly applies to communications across the public Internet. Fully addressing security of communications links may require more than just removal of the A 4.2.4.2 exception. This topic seems sufficiently important to merit its own CIP section covering appropriate requirements for end-to-end protection of communications (encryption, integrity verification, key management, etc.). A comment in the summary of changes for R1 states that "the non-routable protocol exclusion no longer exists". However, R1.1, R1.2, R1.3, and R1.5 all provide

exclusions for non-routable protocols. Of these, R1.5 is the only requirement for which there might be limited choices of technical solutions currently available on the market. There are also exclusions in CIP 007 R1 and R4. We recommend removing all non-routable protocol exclusions, as the summary of changes claims. R1.5: This requirements states that the entity needs to establish a documented method for detecting malicious communications at each EAP. There is no additional comments in the Guidelines and Technical Basis section to clarify this requirement; however, the responsible entity could infer expectations from the measures column. Perhaps a better phrasing would be: "At each EAP, the entity shall document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity." How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? Please consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. Please provide a technical basis for the requirement that outbound access permissions are necessary per Part 1.3. If no technical basis can be defined that can be uniformly applicable to all BES entities, then please consider qualifying “outbound” to be “…inbound and, where implemented by the entity, outbound access permissions”. In Part 1.5, the term “malicious communications” is too vague. The SDT could consider changing 1.5 to say “A documented method for malicious traffic inspection at each EAP”. The third paragraph states “This requirement applies only to communications for which ‘deny by default’ type requirements can by universally applied…”. This sort of language, while useful, should more properly be included in the requirements. The SDT could consider making clear the intent of the Guidelines and Technical Basis section of the standards, and the expectations of the entity - and of the compliance enforcement authority – on how this information should be used. As stated, "A documented method for detecting malicious communications at each EAP." Does this include both inbound and outbound communications? Malicious communications can also be sent from the BES through the EAP. R1 Guidelines: Regarding dialup connections to a specific BES Cyber Asset, the guidelines state "... examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use". Dial-back modems are easily defeated as revealed by a simple google search. Caller-id spoofing services make reliance on caller-id tags questionable. Remote enable or powerup leaves a window of vulnerability unless combined with other defenses, such as modem BES cyber asset passwords. Policy requiring disabling after use is error prone. R1 Guidelines: Problems with dialup modems and methods of securing them are discussed in some detail in"Securing Control Systems Modems" from Idaho National Lab: www.inl.gov/technicalpublications/Documents/3874574.pdf Products and technical solutions to secure dialup connections exist at reasonable cost, and NERC could consider requiring stronger measures to protect dialup connections. R1 Guidelines: Products and technical solutions to secure dialup connections exist at reasonable cost, and NERC could consider requiring stronger measures to protect dialup connections. R1 Guidelines: This sentence is unclear: "Since low impact BES Cyber Systems can impact BES Reliability Operating Services in real time, they should not be located directly on public networks or other networks of lesser trust." Does that mean networks of lesser trust to public networks and, if so, what are those networks? Or is this saying that one should not place low impact BES Cyber Systems on public networks or networks of lesser trust to a corporate network or a network behind an EAP? It is not clear that Security Event Monitoring as called out in CIP 007 is required of all EAPs. NERC could consider security event monitoring be required of all EAPs, regardless of impact level. This requirement could also apply to Associated Electronic Access Control Systems and perhaps also Associated Protected Cyber Assets, since where authentication servers are used separately from the EAP devices, they need to be at least as strongly secured as the EAP devices themselves.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. R2.2: As stated, “Requires encryption for all interactive Remote Access sessions to protect the confidentiality and integrity of each interactive Remote Access session.” However, this statement does not address end-to-end encryption. Sometimes vendors access SCADA systems remotely via a third party remote access service, such as "logmein". Such sites may establish a secure tunnel between the vendor and the remote access service, and then another secure tunnel between the utility and the remote access service. In such a case, the remote access service has access to all the remote access traffic; that is, the encryption between the utility and the vendor is not end-to-end. R2.2: Connections between initiating Cyber Asset and Intermediate Device can be encrypted most

times using 3rd party applications, however the connections between the Intermediate Device and Remote gateway or end device (IED) is often not technically feasible. R2.2: It does not state anything about "Authenticating based on certificates". R2.2: There have been a significant number of CAs compromised recently, and recent versions of Firefox trust approximately 50 CAs located at organizations all over the world. Secure authentication is necessary to ensure that encryption is useful. Relying on CAs outside of the US to authenticate remote access to critical national infrastructure may need to further assessment. As stated, "Require encryption for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session." Please consider replacing "encryption" with cryptographic techniques. Cryptographic techniques includes encryption, integrity, and non-repudiation. As stated, "Require multi-factor authentication for all Interactive Remote Access sessions." Why would multi-factor authentication be required for device to device remote access? As technology evolves, there could be more interactive device to device remote access sessions. R2.3: There is a discrepancy on the usage of multi-factor authentication. In this rule, it states that for High and Medium Impact BES Cyber Systems, as well as the Associated Protected Cyber Assets "REQUIRES" multi-factor authentication. However, in CIP-007 R5.1, it states to "validate credentials before granting electronic access to each BES Cyber System" which does not state the need for multi-factor authentication. A reference for the definition for strong (two-factor) authentication in the RSA information security glossary at http://www.rsa.com/glossary/default.asp?id=1080 R2.3: Multi-factor authentication needs to be carefully defined. US banks have been required to use two-factor authentication since 2006, but while the meaning of the term is clear to security professionals, it has been interpreted in some cases by the banking industry to mean "mother's maiden name plus last 4 of social security number", which is far weaker than the generally acknowledged concept. Without clearly defining what is intended by multi-factor authentication, significantly weaker interpretations may be chosen. NERC could consider that the different factors involved in a multi-factor authentication be drawn from at least two different classes of authenticator, the classes being something you know (e.g., password, userid), something you have (e.g., badge, smartphone, token, physical key), or something about you (e.g., fingerprint, retina scan, voice print). Also some requirement for liveness should be included to prevent, for example, a physical key (as in a metal thing with notches) acting as one factor being left permanently installed/attached to a reader.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This CIP standard no longer has a statement related to "All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter." The language could guide physical security measures through a description of acceptable construction materials, construction practices, and based on facility type. Specification on vegetation management, lighting requirements, stand off distances, periodic patrol, etc., should be included. The key point is that we are drafting physical security standards for the electric industry. It is important to write down a "standard" that people know how to follow for the sake of consistency and achieving the goal of protecting the BES Cyber Assets and BES Cyber Systems. For example, tell them they need an 8ft tall mesh fence with shakers and motion detection if that is needed to establish physical security perimeter. This is also necessary to help in making this requirement auditable. Without more description and additional security control specific the plans generated by the responsible entities may only identify the minimum stated requirement which can leave gapping holes. ASIS physical security standards could be considered as one source of generally accepted good practices that could be leveraged to help make CIP-006-5 a more robust and adequate security standard. As stated, "Define operational or procedural controls to restrict physical access." How is this consistent with the little or no security requirements for low impact systems? Also, as stated, low impact systems do not have to be uniquely identified. As stated, "Utilize two or more different and complementary physical access controls to..." Examples are provided – but they are not mandatory. What if the associated protected cyber asset is a laptop? Requirement 1.6 references only systems. Early CIPs also reference assets and facilities. How does an entity demonstrate compliance to Part 1.1 if CIP-002-5 does not require that entities document their Low Impact cyber assets? The SDT may want to consider revising the Measures section to provide clear guidance on recommended artifacts for compliance that do not pre-suppose lists of Low Impact cyber assets. R1.2/R1.3: The requirement statements in R1.2 and R1.3

address ingress controls; however, the associated measures state egress and ingress. If egress controls are an expectation then the requirement should make it clear as to what the responsible entity is required to do. R1.5: The control as documented is to issue alerts for un-authorized physical access, however there is no control to document results of followup. We propose that events (from alerts) and findings are documented, or even that a summary of findings per period (daily / weekly, etc) are documented. For consideration: “Issue real-time / immediate alerts in response to unauthorized physical access attempts, and investigate and respond to alerts before the end of the next calendar day, and document outcome.”

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Continuous monitoring should be defined with a maximum time frame of escort, communication mechanisms, minimum communications capability during escort, required periodic communications, maximum distance between escort and visitor, visitor identification mechanisms, escort qualifications.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Testing could be at least daily operational checks by security staff using the equipment. This can be simple camera pans, alarm testing, etc. Physical maintenance could be performed based on the environment, e.g., Gen plants are dirty so the condition may warrant a high frequency of checks due to carbon and dust build up, control centers are typically well enclosed, so lower frequencies are needed. NERC could consider adding a requirement to retest if the system fails.

Yes

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Table R1 is referred to as Ports & Services, but the controls are all about Ports, and there are no controls about services. NERC could consider either removing the reference to services or introduce a control to require an analysis of which services are running, and to disable or remove any services that are not necessary. For Part 1.1, SDT could consider acknowledging the use of dynamic ports/ranges used by a wide variety of cyber systems. The documentation requirement seems a bit redundant to the configuration management documentation requirements of CIP-010-1-R1.1. Under the Guidelines and Technical Basis for Requirement R1, 1.1 the draft states “. . . therefore it is the intent that the control be on the device itself; blocking ports at the perimeter does not satisfy this requirement”. This seems to exclude the use of an intermediate device immediately preceding/inline with the device, thereby removing a valid security defense mechanism. Inline security mechanisms where no path around them exists enable security functionality to be placed in a manner to ensure they are engaged and also allow multiple solutions to be used where existing systems lack protection. An example would be a dedicated firewall and IPS system placed directly between a critical system and all connections, ensuring they are in the path of all traffic and allowing specialized security functions not available on some systems. A rewording of the quote above would add the option of providing non-bypassable security controls. “. . . therefore it is the intent that the control be on the device itself, or positioned inline in a non-bypassable manner; blocking ports at the perimeter does not satisfy this requirement”.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The SDT may want to consider revising Part 2.2 to say “Identify applicable security-related patches or security-related updates…” As written, a person could interpret “updates” to mean security-related or not. The words “…that addresses the vulnerabilities within a defined timeframe” could be separated from the end of the sentence and rewritten as its own sentence for clarity. Part 2.3 is not clear on what is actually required. The requirement talks about a process, yet the Measures suggest evidence that the remediation took place. Should Part 2.3 say “Execute the remediation plan documented in Part 2.2”? Patch management could also be considered for low impact systems. If the same operating system or application is used on low and medium/high impact BES systems, the patch should be applied to all the systems to mitigate the vulnerability. As stated, "A process for remediation, including any exceptions for CIP Exceptional Circumstances." This is vague – and could be more specific. Also, this should be linked to configuration management requirements and incident

response requirements, as applicable. R2.1: This requirement states the need to identify the source or sources to be monitored for security patches, updates, etc. However, there is no mention of how frequent the responsible entity should be conducting this activity. It can be inferred from R2.2 that this activity must be conducted, at a minimum, every 29 days or less; however, as written, compliance is limited to identifying a source or sources and does not account for how often monitoring is to be conducted. If the intent is to have the responsible entity frequently monitor the identified sources so security patches, updates, etc. are discovered within 30 days of their release then the requirement should be more clear as to the monitoring expectations.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "Deploy method(s) to deter, detect, or prevent malicious code." This does not address remediation if the malicious code impacts a BES system. How does this requirement specifically relate to separate boundary protections? This requirement appears to be mandatory for every system, rather than to different systems at the boundary. As such, the requirement drives a specific architecture. At what level of the system is this required? Does this include the boot code/kernel, the OS, the applications, etc.? How does this apply to embedded systems? As stated, "Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." This requirement is specific to profiles. There are other techniques that address anomaly-based behavior analysis and heuristics based analysis/detection. NERC could consider revising the requirement to address other types of malicious code detection. R3.3: 30 days is a lifetime when considering updating signatures/pattern files to malicious-code protection tools. Consider shortening this to a lesser period of time that is commensurate to the risk. R3.4: There does not appear to be any consideration for the possibility of the introduction of malicious code through a cyber asset or network-media device connected to the same network (within an ESP or behind the same EAP) as a BES Cyber Asset or BES Cyber System. The definition of a Transient Cyber Asset states that it is a: "A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System." Consider changing the definition of a Transient Cyber Asset to include assets connecting to the same network where a BES Cyber Asset or BES Cyber System is connected.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. A comment in the summary of changes for CIP 005 R1 states that "the non-routable protocol exclusion no longer exists". However, R4.2 and 4.3 provide exclusions for non-routable protocols. We recommend removing these exclusions, as the summary of changes claims. There is a requirement to log events (4.1), a requirement to generate alerts for certain important events (4.2), and a requirement to detect and activate a response to event logging failures within one day (4.3). There is no requirement to activate a response to events important enough to raise an alert within any time period. Dealing with the actual alerts is at least as important as dealing with logging failure. As stated, "4.1.4. Any detected potential malicious activity." How will "a potential malicious activity" be determined? This can be wide open to interpretation as what is “potentially malicious.” Why log every successful logon? NERC could consider logging all events related to privileged accounts. As stated, "Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert." This is not specific to cyber security. Is that the intent? As stated, "(i) dated event logging failures and screen-shots showing how real-time alerts were configured." Configured real-time alerts are not directly related to event logging failures. These are different events. NERC could consider clarifying the requirement or developing two requirements. As stated, "potential event logging failures." Logging failures are typically due to a full log or other basic problem. How is a bi-weekly review going to address this problem? A summarization may miss certain events. As stated, "Activate a response to rectify any deficiency identified from the review before the end of the next calendar day." It is not always possible to rectify a deficiency within a short period of time. This requirement may need to be split into two requirements – one addressing logging failures and a second addressing security incidents. R4.2: The Measures and Change Description/Justification indicated that analysis is expected; however the requirement states that necessary alerts need to be established. Consider rewording the requirement to make analysis of the alert a clear objective. There is no requirement within the set of CIP standards 002-5 through 011-5 that make it clear that trained, knowledgeable

and aware people are essential to making a security logging system fully functional. CIP-004-5 training requirements mention role-based training but without specific descriptions a responsible entity could have the alert analysis (and the R4.5 summary review) accomplished by an administrator who has no training or skills to perform such activity. Effective security log management requires aware and skilled personnel watching the log systems and output. If an entity does not have expertise to understand what alerts are possible, and what the alerts may indicate, then the alert generation exercise called out in the Measures is not effective. Furthermore, a utility might simply decide that no alerts need a real-time alert. We recommend that unauthorized access attempts, at a minimum, be considered to require real-time alerts. R4.5: As written, R4.5 requires log review exactly every two weeks. Since the intent of this rule is to require a review at least every two weeks, we recommend adopting wording for this requirement that is similar to what was recommended earlier to fix the definition of the term "annual". Specifically, we recommend something like " an entity is out of compliance with R4.5 unless, within the preceding 14 calendar days, it has reviewed a summarization or sampling of logged events".
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types." How do you implement least privilege and other security controls if they are not defined in policy? This does not restrict the use of administrator, shared, etc. account types. These should be limited based on least privilege and need to know. As stated, "Identify individuals who have authorized access to shared accounts." Why only shared accounts? Consider identifying individuals with privileges – particularly those with access to administrator accounts. As stated, "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required." Consider changing default passwords on devices. Because a default password is unique to a device does not imply that it is secure. As stated, "A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts." Consider adding an exception for emergency situations. Also, this is a potential method for launching a denial of service attack. The decision to limit the number of unsuccessful authentication attempts should be based on the potential risk. Consider adding more details in the requirement related to the potential risk. Part 5.2 implies, but does not state, that a signed and approved list of delegates is required. Please clarify. Also, this requirement talks about the “use of” shared accounts. This could be interpreted as either the initial creation of, or day to day use of, those ID’s. We believe the SDT meant the former, but we request that you please clarify. Parts 5.2 and 5.3 imply, but do not explicitly state, that there must be a procedure to authorize individuals having access to shared/administrative accounts. Please clarify. For Part 5.4, please simplify by stating “Procedural controls for initially changing default passwords, where technically feasible”. All the rest may be stricken, and the asset types moved to the Applicability column. R5.5: Long passwords are primarily required to defend against offline password attacks. Increasing the minimum password length from 6 to 8 characters is not adequate to address offline password cracking attacks, in the face of modern GPUs offering significant hardware parallelism and available on cloud computing services such as Amazon's EC2. All possible 6-character passwords can be tested on a supercomputer such as the Tianhe-1A in approximately 1 second, or on a distributed EC2 cluster in approximately 15 seconds at a cost of 50 cents. Raising the minimum length from 6 to 8 characters only requires an attacker to spend 96*96 times longer to try all passwords, which is still less than a day using cloud-based distributed computing. Furthermore, on Windows systems that store LM hashes, any password of any length is easily cracked in minutes on a conventional CPU. This applies to all Window systems prior to Windows Server 2008 and Windows 7. We recommend that NERC consider increasing the minimum password length to no fewer than 12 characters on Windows systems and no fewer than 10 characters on Unix-based systems that use SHA-512, salt, and key stretching. We recommend that NERC consider disabling LM hashes on all Windows servers, clients, and domain controllers. Third, we recommend that NERC consider guidance accompanying the CIPs that point out that using long passwords, even those that satisfy the complexity metrics of 5.5.2, does not automatically result in strong passwords. For a real-world example, The Tech Herald reports that of the 860,160 Stratfor passwords leaked late 2011, they were able to crack roughly 10% of them in a little over 4 hours using a CPU-based (ie. no GPU acceleration) cracking tool. Many of these were longer than 8

characters. There is supporting document "NESCO Common TFE Analysis: CIP-007 R5.3 Password Complexity".
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library R1.2: Even though the R1 rationale states that reportable incidents would follow the EOP 4 actions and timelines, the requirement language cow;d be more specific regarding that expectation. R1.3.1: What happens if there is a third-party IT company that handles the utility's cyber security incidents? Who should be doing what and who has the ultimate responsibility? For example, should the IT company handle everything from the beginning to the notification of the incident?
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library Part 2.1 the words "…when incidents occur" is redundant. The requirement is a bit contradictory in that the incident response plans MUST be used, yet deviations are allowed. Recommend rewording this requirement to say "When a suspected BES Cyber Security Incident occurs, the incident response plans shall be executed. Should deviations from the plan be necessary, those shall be documented for later review". As stated, "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." Consider making testing cyber security incident plans a separate requirement. Part 2.2 does not address new vulnerabilities or threats. Consider adding a requirement that the plan be revised based on new threats/vulnerabilities. As stated, "Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years." Is this sufficient for law enforcement, state, and federal requirements? Also, if the documentation is in electronic form, consider storing it in encrypted form and signed to ensure confidentiality, non-repudiation, and integrity.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library The Change Description field mentions "DHS Controls". What are these? Also, due to the complexity of the testing and review of the BES Cyber Security incident response plans, consider including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan. As stated, "Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary." Consider revising the plan if there are incidents, new vulnerabilities, new threats, and modified security configurations. As stated, "Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." Consider modifying other relevant documentation, e.g., configuration management plan, access control policies, audit policies, etc. As stated, "Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan." Consider updating the plan based on new threats and vulnerabilities.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position

of DOE. For Part 1.4, what does “verified initially” mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets. As stated, "Conditions for activation of the recovery plan(s)." The terms “response plans” and “recovery plans” are not adequately defined. It is not clear what the differences are between the two types of plans. As stated, "Roles and responsibilities of responders, including identification of the individuals, either by name or by title, responsible for recovery efforts." The definition of roles and responsibilities and the names of specific individuals assuming those roles are two different areas. Roles and responsibilities may not change significantly over time, unless there is a new vulnerability or threat. The identity of individuals may change – based on people moving, terminating, etc. Consider having the list of specific individuals in a separate document. R1.3: Protection of backup media and backed up information is only lightly mentioned in this rule. Consider adding greater emphasis on the protection of backups, such as off-site storage and other physical protection, so that sensitive information in backup files (network configurations, device configurations, passwords, etc.) is protected. Is the intent of the standard the recovery of the function of an asset or system, or the recovery of the actual asset itself? This would be a good opportunity to clarify.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Consider revising part 2.1 to read “Test the Recovery Plans at least once every calendar year”, and include the three bullets. It also needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Need to also allow for the fact that not all cyber assets can be “backed up” in a traditional IT sense. As stated, "...initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment." The other components are tested every 15 months – why is this 39 months? This assumes that a utility has a complete representative environment. This may not be realistic for all the BES associated systems. If there is a significant cyber security incident, the plan could be tested once the system is made operational. This will ensure the revised plan is accurate.

No

These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. As stated, "or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned." Consider revising the plan after a significant cyber security incident to ensure that it is accurate. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures. As stated, "Update recovery plan(s) to address any organizational or technology changes within thirty calendar days of such change." As discussed earlier, the basic recovery plan should not be linked to specific individuals in an organization. The list of POCs should be kept separate from the plan and updated regularly – based on personnel changes. “Technology changes” is a vague term and could refer to software, hardware, firmware and may or may not be security relevant. Consider clarifying the definition to focus on security relevant changes. Due to the complexity of the testing and review of the BES Cyber Security incident response plans, NERC could consider including a timeline/graphic in the Guidelines section to visually demonstrate the lifecycle of the plan. For Part 2.2, the same question on scope applies. The language needs to be made clear whether ALL cyber assets need to be included in the annual test, or a subset, or representative sampling, or entity defined. Also, not all cyber assets can be “backed up” in a traditional IT sense. R3.2: For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both. R3.3: Consider updating the Measures in Part 3.3 of CIP-009-5 Table R3 to include identification and documentation of the date of any event or lesson learned that results in an update to the recovery plan. R3.4: Table CIP-009-5 R3 parts 3.4 and 3.5 need the sub-headers titled Part Part Part

Part updated to Part Applicability Requirements Measures. R3.5: NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library For Part 1.1.4, the word “scripts” is generic and thereby difficult to address. Scripts that are used for key functionality of the system would make sense to include in the baseline, but scripts for administration, backups, maintenance or troubleshooting, for instance, may be too dynamic by nature to be included in the baseline. Please either clarify or revise the words “and scripts”. As stated, "Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels." This is not a comprehensive list of what could be included for each cyber asset. It is not clear how this list applies if the device is hardware only. Also consider adding communication protocols. R1.1: The baseline configuration requirements is missing "Network Topology" – "Network Topology" is suggested in NIST SP800-53 CM-2 "Configuration Management" ---> "Baseline Configuration". R1.1: NERC could consider adding a requirement to include in the baseline any non-standard configurations of the BIOS, operating system, services, etc. For example, BIOS version, BIOS boot disk order, BIOS password, changes to Windows registry entries, changes to service/task scheduling priorities, addition of periodic processes via modifications of tools like crontab, etc. R1.1: NERC could consider adding a requirement to explicitly include in the baseline any remote access services, eg. RDP, VNC, PCanywhere, etc. R1.1: NERC could consider adding firmware and programmable device load versioning to the list of items in the configuration baseline. This could include any executable or loadable image that can be modified without requiring physical access to BES Cyber System component internals.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. NERC could consider adding protections to the process for modifying cyber assets, in addition to monitoring for unexpected changes. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Vulnerability analysis looks for any weaknesses - it is more than an audit of implementation against design. There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library. There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all

requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. R3.1: This requirement does not compel an entity to take any action based on the results of the assessment to correct vulnerabilities, and is weaker than the language in R8.4 of CIP-007-3 currently in force. R3.2 calls for vulnerability assessments every three years. CIP 007-3 R8 requires vulnerability assessments annually. No rationale is given for weakening this requirement. As of January 2 2012, the National Vulnerability Database contains 49053 CVE vulnerabilities, with 11 being added per day. Even without likely acceleration of this growth rate, this implies 4000 new vulnerabilities will be discovered each year. Even if only a small percentage of these apply to BES cyber assets, this could mean a significant number of KNOWN vulnerabilities in BES cyber assets by the time a vulnerability assessment comes due. Because of the constant change and introduction of new vulnerabilities, revising the time frame to three years seems inconsistent with this constantly changing vulnerability environment. Consider modifying the time frame to annually, or less. R3.2: For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where “test” systems just aren’t economically feasible. What is the acceptable deviation between test and production? R3.3: For Part 3.3, please clarify whether “new Cyber Asset” means literally that or, more reasonably, could mean “new Cyber Asset category” or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it may not make sense. R3.2:
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com. General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. This CIP does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information. Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access. The measures column in R1.1 talks about "training materials that ... to recognize BES Cyber Security Information." but does not contain information about having training materials for handling BES Cyber System information. Table CIP-011-1 R1 parts 1.2 and 1.3 need the sub-headers titled Part Part Part Part updated to Part Applicability Requirements Measures.
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The statement, "...the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media." does not clearly address secure sanitization of media. It is recommended that NIST SP800-88 is followed by the utilities to safely sanitize the information in the media. Some examples of safe sanitization methods according to NIST SP800-88 are: Clearing information in a media using an overwriting software or hardware, Purging using degaussing tool for magnetic media, Destroying by shredding, Disintegration, Incineration, Pulverization, and Melting. Also, another reference for clearing and sanitization is: http://www.oregon.gov/DAS/OP/docs/policy/state/107-009-005_Exhibit_B.pdf?ga=t For Part 2.1, please consider adding language that allows for re-use or redeployment within a similar BES Cyber System.
Yes
No
These comments were developed by NESCOR/NESCO/EPRI and may not represent the official position of DOE. The implementation plan calls for CIPv5 to come into effect January 1, 2015. Given that this draft has already been in the works for nearly two years, it is not clear why the effective date is three years in the future.
Individual
Bo Jones

Westar Energy
Yes
Westar Energy supports EEI comments as submitted.
Yes
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No

Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
The current practice is to restrict access to only those ports and services needed with a business justification for each.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Yes
Yes
Information pertaining to Associated Protected Cyber Assets could potentially contain protected information. Associated Protected Cyber Assets likely reside on a protected network therefore the information should be protected similar to High Impact BES Cyber Systems, Medium, Impact BES Cyber Systems, Associated Physical Access Control Systems, and Associated Electronic Access Control

or Monitoring Systems.
Yes
Information pertaining to Associated Protected Cyber Assets could potentially contain protected information. Associated Protected Cyber Assets likely reside on a protected network therefore the information should be protected similar to High Impact BES Cyber Systems, Medium, Impact BES Cyber Systems, Associated Physical Access Control Systems, and Associated Electronic Access Control or Monitoring Systems.
No
Westar Energy supports EEI comments as submitted.
No
Westar Energy supports EEI comments as submitted.
Individual
Bruce Metruck
New York Power Authority
Yes
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: A definition for a 'Control Center' would be helpful. i.e. Change 'two or more locations' to 'two or more separate locations', not including the facility where the BES Cyber Systems are located. In certain situations the control of an adjacent BES facility may be provided at a generating plant – which should not classify that plant control room to be classified as a Control Center.
Yes
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: It would help if section 1.4 clearly defined what level of control of generation would require classification as a 'High' impact. In some case a control center may have limited 'base point' setting capability for assets under section 2.1.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: The word 'owns' is used in two places – this should be changed to operates or utilize – ownership may not be the determining factor based on outstanding operating agreements over time – also a single asset may be used by more than one entity.
No
NYPA concurs with the response provided by NPCC for this question.
Yes
NYPA does NOT concur with NPCC in leaving this question unanswered.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Last bullet of M4 should not be there – covered in CIP-004 (possible double jeopardy). Wording should be focused on 'Available' rather than 'Aware'. In general, we believe that all measures should be what the auditors will accept, or they should be removed (for all standards).
Yes
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: The footnote should be embedded in the actual requirement wording, re-word or move into a guidance.
No
NYPA concurs with the response provided by NPCC for this question.

No
NYPA concurs with the response provided by NPCC for this question.
Yes
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: In 1.1 “Applicability” add the ‘Medium Impact Cyber Assets with no external connectivity’ (see below for rationale)
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: In 1.2 “Applicability” replace the “Medium impact BES Cyber Systems’ to ‘Medium Impact Cyber Assets with external connectivity’. The rationale for this change is that stand alone devices such as protective relays cannot be controlled via defined electronic access points as defined in Part 1,2 without increasing their vulnerability by connecting them to such points.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R2 Part 2.1, as set forth in the table, from “Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets” to “Identify any available, active source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets.” Many older cyber assets may exist that may not have active vendor support or the vendor may have gone out of business. The requirement should provide for such situations. Recommend changing the language in Section R2 Part 2.2, as set forth in the table, from “Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe” to “Identify, document and initiate review procedures for patches, updates and vendor security notices within 30 days of release from the identified source. Procedures shall review for applicability to the entities BES Cyber Systems and Assets, identify a level of security/operational risk and provide a plan with defined responsibilities to address any identified vulnerabilities.” The majority of patches and updates provided by vendors are not necessarily security related but may include bug fixes, enhancements and upgrades. In many cases, patches are issued against an Operating System that may not be applicable to a system that has been hardened. In addition,

utilities may be dependent on third parties (e.g. system integration vendors) to review and test the impact of patches on operating software. The time frame for planning the implementation of the patches, or any alternate mitigating measures is highly variable.
Yes
NYPA does not agree with the NPCC response for this question, the original wording is sufficient.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R4 Part 4.1, as set forth in the table, from “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: …” to “Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, where available, each of the following types of events: …”. The intent is to provide leeway for additional log information. It should be noted that many “Medium Impact Cyber Assets” such as protective relays, metering, etc., may have minimal event log capability. Here the standard will require that whatever is available should be preserved. Recommend clarification of the terms “alert” and “real-time alert” in Section R4 Part 4.2, as set forth in the table.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Recommend changing the language in Section R5 Part 5.1, as set forth in the table, from “Validate credentials before granting electronic access to each BES Cyber System” to “Validate credentials before granting functional electronic access to each BES Cyber System.” Functional access is defined as capability to affect the operation of the BES System/Asset or of any of the BES Reliability Functions of the System. Many cyber devices, such as protective relays, meters or IED display terminals have some level of “Read Only” capability. It is not practical to provide individual log in capability to perform functions such as viewing equipment status while walking by or reading relay targets. Similarly some HMI systems are provided with auto-boot to non-privileged accounts from which users may only start up a BES Reliability Application that provides for or requires authentication. Note also that some level of control is provided for these non-privileged accounts in that they will need to be listed in Section 5.2.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Deletion of the second sentence in the NPCC comment - 'Is this integrity, availability or other information protection such as access controls, encryption?' - , the original wording is sufficient. In addition, this wording should clearly focus on ‘Loss Prevention’ or ‘availability’ rather than ‘protection of information’, and 1.4, should be verified ‘upon’ the actual backup to ensure backup success.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: It is unclear where the line occurs between the ‘Implementation’ covered by 2.1 and the ‘Testing’ covered by 2.3 – please clarify.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Should use wording ‘When technology changes’, and should refer to only ‘Applicable’ organizational change, and Technology Changes should be only BES Systems.

No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Change sub-requirement 1.1.4 from 'any custom software or script …' to 'any compiled software or script that affects system startup, external communication or application program operation'. Some scripts such as macros for a spreadsheet or an application script do not merit full change control.
No
NYPA concurs with the response provided by NPCC for this question, with the following addition/change: Requirement 2.1 should be replaced – i.e. 'Implement technical or procedural controls to detect unauthorized changes to the baseline configuration'. The existing wording appears to require additional technical controls beyond those stipulated in CIP-007 R3.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question.
No
NYPA concurs with the response provided by NPCC for this question, including the additional general comments that NPCC added to the comment since there was no other place to indicate such.
Individual
Edward Bedder
Orange and Rockland Utilities Inc.
No
Comments: Minor correction should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.
No
Comments: 4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.

No
1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices. (R7.5).
No
Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.
No
Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No
The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.

No
R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
No
CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should include language indicating that the registered entity identifies the “authorized individuals”.
CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.
No
General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only

that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Individual

Thad Ness

American Electric Power

Yes

The definitions are inconsistent on the use of singular versus plural. For example, “Cyber Assets” versus “BES Cyber Asset” and “Protected Cyber Asset.” AEP recommends the use of singular. In “BES Cyber Asset” the second sentence appears to be somewhat at odds with the first and third sentences and does not add any further clarity. AEP recommends considering deletion of the second sentence. In “BES Cyber Asset” should “cyber security event or incident” actually be “BES Cyber Security Incident”? AEP recommends using the defined term “BES Cyber Security Incident” if possible. In “BES Cyber Asset” it says “Redundancy shall not be considered when determining availability.” Does that redundancy refer to BES redundancy, or Cyber Asset redundancy? Is BES redundancy sufficient to eliminate a Cyber Asset from consideration as a BES Cyber Asset? For example, if multiple path options exist from a generating facility, do all path options have to be considered? AEP recommends changing the definition to read “Cyber Asset redundancy shall not be considered when determining availability” if that was the drafting team’s intention. Are all BES Cyber Assets part of BES Cyber Systems? Can BES Cyber Assets reside “outside” of a BES Cyber System? Or do all BES Cyber Assets necessarily have an associated BES Cyber System? If a BES Cyber System is required for all BES Cyber Assets, AEP recommends clarifying that in the definition. “BES Cyber System” definition includes “typically” – which is not well defined. AEP suggests removing the term “typically.” “BES Cyber System” definition still includes “Maintenance Cyber Asset” which is not a defined term. Does “Transient Cyber Asset” replace “Maintenance Cyber Asset”? “BES Cyber System Information” definition is not crisp. AEP recommends the definition should use the following construct to identify BES Cyber System Information. The information must explicitly indicate *something* about 1) the BES Cyber Assets themselves (such as information to uniquely identify a BES Cyber Asset), and 2) their impact on the BES (information to indicate the significance of its role in the BES). If both tests aren’t met, it isn’t “BES Cyber System Information” itself. “BES Cyber System Information” contains a lot of detailed information. Why include specific requirements for types of information in the definition? Can’t the requirements be included in a “Requirements” section? These are not examples – these are requirements. AEP recommends they be moved to the requirements. “BES Cyber System Information” should say “recovery plans” not “disaster recovery plans.” “BES Cyber System Information” says “BES Cyber System incident” but “incident” should be capitalized. “BES Cyber System Information” says “network topology” – which is not a defined term. It doesn’t appear that “network topology” refers to anything to do with the electrical system network (but it could be confused that way). AEP recommends this be changed to “communications network topology.” “BES Cyber System Information” says “Electronic Access Control System” but should say “Electronic Access Control or Monitoring Systems" to be consistent with the rest of the standards. “BES Cyber System

Information" uses the term "BES Cyber System Impact" which is not defined. AEP recommends defining the term or removing it from the definition. "BES Reliability Operating Services" uses lots of abbreviations and colloquial, casual language: "x-former" "&" "etc" "auto" "Know generation status & capability & restrictions". AEP recommends using very formal language for this important definition. In "BES Reliability Operating Services" "Monitoring & Control" should "BES Elements" be a NERC-defined term? "BES Cyber System" combined with "Situational Awareness" from BES Reliability Operating Service is unbounded – it could include a wide variety of internal and external inputs that arrive via Cyber Asset (Internet access, CNN, AM radio, etc.). It would be difficult to demonstrate that a system does NOT impact situational awareness. In this instance, AEP recommends removing the "but are not limited to" phrase. In "BES Reliability Operating Services" "Inter-Entity Real-Time Coordination and Communication" appears unbounded. How do you limit the systems which are subject to this criterion? Could this include public telephone systems, public communications networks, satellite telephone systems, or even amateur radios? In this instance, AEP recommends removing the "but are not limited to" phrase. In "CIP Exceptional Circumstances" "Cyber Security Incident" should be changed to "BES Cyber Security Incident." "CIP Exceptional Circumstances" – could a reliability crisis be considered a CIP Exceptional Circumstances? AEP recommends that be added. In the definition of "Control Center" the bullet "Coordination of BES restoration activities" could be problematic. Could temporary facilities be considered a Control Center? Or would the absence of BES Cyber Assets prevent that? Or would phones, radios, laptops, etc. that might be considered BES Cyber Assets pull those Control Centers in to scope? AEP recommends dropping "Coordination of BES restoration activities" from this definition – the other functions should be adequate. Can the drafting team provide a definition of "Control Room" in addition to "Control Center"? AEP recommends the drafting team leverage the definitions posited in the Critical Asset identification guideline. The definition of "Cyber Assets" includes the term "programmable" – which is not well defined. Is a device with DIP switches considered programmable? Is a device that is loaded with a non-modifiable, non-configurable firmware (such as a USB drive) considered programmable? Is a differential pressure transmitter programmable if it can be "programmed" via a HART protocol handheld? AEP recommends the term "programmable" be defined, or an alternative term ("configurable"?) be chosen. "Defined Physical Boundary" seems to be a low-value name change. Awareness and training materials will have to be updated, documentation will have to be changed, programmed systems will have to be re-written, etc. Why not continue to use the term "PSP"? Or at least leave both defined? At a minimum, AEP recommends the SDT should keep the term PSP (6-wall perimeter?) defined, so that legacy documentation is still "correct." "Dee-Pee-Bee" seems to be an awkward combination of letters. It's difficult to distinguish the letters when said quickly. Is there another word or phrase to describe a physical limit that is not a complete, six-wall enclosure? AEP recommends the drafting team consider alternative terms with different abbreviations. In "Electronic Security Perimeter" is "protect" subject to the qualifiers ("routable or dial-up data communications") in the definition of "Electronic Access Point"? That is, do non-routable or non-dial-up connections need to pass through an Electronic Access Point? AEP recommends that the drafting team clarify that this is not required. "External Routable Connectivity" and "External Connectivity" definitions vary. And "External Connectivity" does not appear to be used in the standards. Should "External Connectivity" have been deleted? AEP recommends deleting "External Connectivity" unless it is used somewhere in the standards. "External Routable Connectivity" implies inbound only. Is that the intention? Why have requirements in CIP-005-5 for outbound access when it's not governed by "External Routable Connectivity"? BES Cyber Systems / BES Cyber Assets that have access outbound only are not addressed by the standards. AEP recommends "External Routable Connectivity" have "is accessible from" changed to "is accessible from or has access to" if that was the drafting team's intention. Alternatively, should "External Routable Connectivity" be replaced with "Remotely Accessible"? Is it correct that "Interactive Remote Access" does not include client-server or "process" based communications in to the ESP? AEP recommends clarifying that in the definition. In "Interactive Remote Access" the term "network-based" appears to replace "routable" – can "routable" be used for consistency? AEP recommends replacing "network-based" with "routable." In "Intermediate Device" the term "Interactive Remote Access" should be capitalized. AEP recommends the definition of "Physical Access Control Systems" be extended to exclude logging systems that are merely used as a replacement for paper log book. This definition should only refer to systems that "programmatically" participate in the logging transaction, rather than those that are used as "offline" logging systems. Does a "Reportable BES Cyber Security Incident" that compromises one part (but not all) of the BES Reliability Operating Service really qualify as a Reportable BES Cyber Security Incident? If so, AEP

recommends the drafting team add “any part” to “compromised or disrupted a BES Reliability Operating Service” in that definition. Does “Transient Cyber Asset” include removable media such as USB drives, CD-ROMs, etc.? AEP recommends that the drafting team clarify this type of removable media would not qualify as a “Transient Cyber Asset.” The definition of “Transient Cyber Asset” includes the term “directly connected” – which is not well defined. Does this infer “locally connected” or “physical attachment”? Does it include USB, serial and 2-wire signaling? Is wireless included in the phrase “directly connected”? AEP recommends the drafting team replace “directly connected” with something more descriptive. AEP would like to see the language from CAN-0005 appear somewhere in the definitions, so that CAN-0005 can be retired in favor of an appropriate definition. AEP recommends the drafting team address the issue in the definition of “Transient Cyber Asset” by clarifying that “system operator laptops with the capability and purpose of controlling BES Cyber Systems remotely (either in normal operations or in emergencies) are not Transient Cyber Assets and must be considered BES Cyber Assets.” Alternatively, the term “System Operator Laptop” could be defined separately using CAN-0005. AEP is concerned that the process for maintaining and revising the definitions proposed in this project is not clear. Obviously, changes to any one of these definitions could have cascading implications to a variety of requirements. AEP recommends that this process be explicitly stated – that the definitions can only be changed by a SAR authorized SDT.

Yes

Due to the wording changes, AEP believes it’s not accurate to say “Most of these criteria are similar to those already approved by the industry as part of Version 4” – there have been small but significant changes. AEP recommends any future questions or statements on this topic make this clear. Does an entity have to maintain evidence of 15 minute impact? Is a 15 minute “test” applied for Cyber Assets included as BES Cyber Assets, or just Cyber Assets NOT included as BES Cyber Assets? And for Cyber Assets NOT included, will there be an expectation of evidence demonstrating why (or “how long”) a system could be down without impacting the BES? AEP recommends the drafting team explicitly answer this question in the Requirement / Measures. AEP believes the Attachment 1 “bright line” criterion regarding load shedding systems (“300 MW”) should be included in the Section 4.1.2 Distribution Provider Applicability section. Otherwise, all distribution providers may be obligated to demonstrate that their UFLS / UVLS / SPS / RAS equipment was not responsible for IROL violation / 300 MW – where they may not even be aware of the full scope. Alternatively, could the Distribution Provider Applicability section (4.1.2) be clarified that it is subject to the criteria in Attachment 1? AEP observed that 1.10 in CIP-002-4 has been removed. While there may not be many Transmission facilities that meet this criterion, it seems like a logical (and essential) criterion for the Transmission connection of Generation meeting Criterion 2.1, etc. AEP recommends it be reinstated in Attachment 1. AEP encourages the drafting team to consider whether BES Cyber Assets without routable or dial-up connectivity really are Medium Impact BES Cyber Assets. Due to the isolation of these systems, they simply don’t have the risk to the BES that a non-isolated Cyber Asset would, and shouldn’t have to meet the requirements for Medium Impact BES Cyber Assets. AEP noted that applicability sections throughout the standards include references to “Medium Impact BES Cyber Systems with External Routable Connectivity” – could the drafting team simplify its work by treating these isolated BES Cyber Asses / BES Cyber Systems as Low Impact BES Cyber Assets? The heading of “Attachment I” appears to use a Roman numeral. Why not use “1” for “Attachment I”? Why use a Roman numeral? AEP recommends consistent use of the Arabic numeral “1”.

No

AEP could not find a good place to insert this comment in the question form as it applies to all of the requirements in all of the standards in this project. It has come to AEP’s attention that elements, such as measures, that are bulleted lists infer that any individual or multiple items can be considered; however, if it is a numerical list then every element is in scope and must be applied. If this assumption is correct, AEP recommends that each standard have that direction explicitly stated. Otherwise, it is extremely likely that some individuals and/or entities will overlook this important distinction. AEP further recommends that the use of “or” and “and” be used with these lists to be explicitly clear to the readers. AEP is concerned that the sentence “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls” is not clear. AEP understands this to mean that an entity does NOT have to maintain a list of Low Impact BES Cyber Assets, but must simply apply the controls outlined in CIP-003-5 through CIP-011-5 for Low Impact BES Cyber Assets. If that’s the drafting team’s intent, can that be said more clearly? AEP recommends simply explicitly stating that a list of Low Impact BES

Cyber Assets is not required, but that entities must meet applicable requirements for Low Impact BES Cyber Assets. AEP is concerned that an entity has to maintain a list of Cyber Assets not identified as BES Cyber Assets. Again, AEP recommends explicitly stating that this is not required. On page 7 the diagram uses the term “Associated Protected Cyber Assets.” Should the term “Associated” be removed? On page 7 the diagram uses the term “Associated Electronic and Physical Access Control and Monitoring Systems.” Should the term “Associated” be removed? On page 10, “Evidence Retention” states “until found compliant.” As far as AEP understands, regional entity auditors will not deem an entity compliant; they will merely report “No Finding.” AEP recommends re-writing or striking the second bullet. On page 18, in the “Guidelines and Technical Basis” the description of the BES Reliability Operating Services varies between this section and the glossary of terms. The examples provided between the two vary as well. If the BES Reliability Operating Functions are going to be referenced their description and examples should be consistent between CIP-002 and the glossary of terms. AEP recommends deferring to the glossary of terms. On page 21, in the “Guidelines and Technical Basis” the term “Substation automation” is used. This is a term with widely varying meaning throughout the industry, and is not defined in the NERC Glossary. AEP recommends the drafting team think carefully about whether to include this term, or whether to remove it altogether.
No
The requirement says “delegate” but should say “delegate(s).” The measure does not reference “delegate(s)” despite the requirement referencing “delegate.” AEP believes R2 should say “initially prior to or upon the effective date of the standard…” Without that, it would seem the CIP Senior Manager or delegate(s) would need to approve the lists precisely on the effective date.
No
The VSL table doesn’t appear to address BES Cyber Systems. The VSL table seems to favor small entities, since the “percentage” of BES Cyber Assets would be lower. AEP recommends using a percentage for everyone.
Yes
No feedback to SDT.
No
The Rationale for R2 should be restated to include the word “cyber” before security policy (“One or more cyber security policies”). AEP believes the inclusion of the word "implement" in Requirement R2 may open entities up to double jeopardy with CIP-004 – CIP-011. The security controls for 1.1 – 1.9 are implemented as part of CIP-004 – CIP-011. If the implementation of the cyber security policy is audited then would it not be an audit of the CIP-004 – CIP-011 requirements? AEP recommends removing the word “implement” in this instance. AEP is also concerned that a Registered Entity with only Low Impact BES Cyber Systems would be unable to “implement” their cyber security policy since some of these areas are not applicable to them. Are those entities expected to go beyond the standards requirements and provide evidence they have done so? Again, AEP recommends removing the word “implement” in this instance. In item 1.10 in Requirement R2, AEP noted that provisions for “responding to” CIP Exceptional Circumstances are identified here, but are not covered anywhere else in the CIP standards. This might bring into scope (for example) Business Continuity, Disaster Planning, and Emergency Medical Response plans that have no bearing on cyber security. At a minimum, AEP recommends removing the words “and responding to” from item 1.10 in R2. In Measure M2 the standard states “Records that indicate the required ten topics were implemented.” This measure should not be required, as the actual implementation of the policy is addressed in the implementation of the requirements of CIP-004 through CIP-011. If you have a non-compliance issue with a requirement in CIP-006 would the entity be non-compliant with the policy in CIP-003-5 R2? AEP recommends striking item #2 from Measure M2.
No
AEP recommends that “initially upon the effective date…” should be phrased as “initially on or before the effective date…” or something similar. In Measure M3, this should be restated as “A dated approval by the CIP Senior Manager for each cyber security policy that indicates annual approval.” Approvals can occur via a variety of methods including but not limited to “wet ink” signature.
No
AEP believes it would be beneficial to consolidate this requirement with the training requirement in CIP-004.

No
AEP understands the desire for a filter-down effect of the approvals and authorizations; however, for larger companies the documentation and updates as part of this requirement would be a significant burden without a corresponding increase in cyber security or reliability. AEP recommends that entities should be required to develop a program for approvals and authorizations that demonstrates engagement of the CIP Senior Manager, without requiring numerous explicit, documented layers of delegation. At a bare minimum, AEP strongly recommends striking the last sentence of Requirement R5. AEP suggests the wording like the current version be used "R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager." The requirement that all approvals and authorizations be performed by the CIP Senior Manager (or an explicit delegate) will require a tremendous amount of paperwork, with no commensurate increase in security or reliability. “Cyber Security Policy” is lower case in other sections of the standard, and is not defined in the definitions. AEP does not believe it should be treated as a proper noun in CIP-003-5 R5. AEP believes the reference to CIP-003-5 R3 in CIP-003-5 R5 should be to be CIP-003-5 R2. In Measure M5 the requirement allows delegation by position or name of delegate, but the measures reference individuals. This appears to be inconsistent and if this requirement is going to remain in CIP-003-5 largely “as-is” AEP strongly recommends the measure be modified to reflect that delegates can be named by position. AEP believes the last bullet in Measure M5 is too complex and recommends it be restated to be clearer if possible. AEP suggests that the use of sub-bullets or additional bullets may make this bullet point clearer.
No
Please see AEP’s comments relating to Requirement R5. The footnote indication “2” should be in superscript.
No
VRFs: AEP believes the VRF for Requirements R1 and R2 should be Lower. These requirements are documentation and administrative based requirements. VSLs: Requirement R2: The implementation of the policy is a function of implementing the remainder of the requirements in CIP-004 through CIP-011. There should not be a requirement to implement the elements of policy as an instance of non-compliance of a specific requirement will result in “double jeopardy.” As such, there should be no associated VSL. Requirements R5 and R6: The numbers in the VSL are arbitrary and do not account for the size of the company, the number of BES Cyber Assets/Systems, number of employees or number of individuals delegated for the approvals. These number stated in the VSL would be acceptable for a smaller organization, but for larger organizations this would not be appropriate. AEP suggests more Levels to be defined in the VSL to account for a wider range and urge the SDT to incorporate a percentage (in addition to an absolute number) as has been done in other standards.
No
R1.1 is applicable to “All Responsible Entities” but the section called “Rationale for R1” (not the “Change Rationale”) only discusses “personnel who have authorized…access.” AEP suggests updating the “Rationale for R1” to reflect the more general applicability of the requirement.
No
AEP is uncertain if all roles need to be trained on all items in R2.2 through R2.10, but believes that not all roles may need each of the different types of training. AEP recommends the drafting team explicitly state this R2.1. R2.2 – R2.10: AEP is concerned that a Registered Entity could create a training program with one level of detail but that an auditor will expect a greater level of detail, and deem the program insufficient. AEP recommends attempting to offer greater specificity about the minimum requirements for each of these topics. While AEP does not have a specific recommendation for the drafting team, ideas might include a minimum number of minutes, a minimum number of “quiz” questions, or a minimum number of “slides.” R2.10: AEP is concerned this topic is well beyond the scope for most users. The few personnel who have this knowledge do so because they are involved in the day to day operation, engineering, design, and maintenance of the BES Cyber Systems, not because they have received training on them. Depending on what detail is included in the training the training itself would need to be updated every time there is a change to a BES Cyber System – undoubtedly by the experts on those systems, who are likely the only people to ever receive the training. This seems like an extremely inefficient use of scarce resources. Furthermore,

AEP is concerned that all of this "interconnectivity" would need to be documented for each BES Cyber System to ensure it is covered in training. AEP recommends re-wording Requirement R2.10 to specifically address the topic of concern, or to set a minimum “level of depth” so that if this topic was covered at a cursory level in the training course, it would be deemed acceptable during a Regional Entity audit.
Yes
No comments for SDT recorded.
No
R4.1: AEP is uncertain if users with existing access to existing BES Cyber Systems are considered “grandfathered”? Or do they need to have a new initial personnel risk assessment? AEP recommends clarifying that existing personnel risk assessments are sufficient until their regular seven year expiration. Is “Social Security Number verification” still sufficient for compliance? Or is the requirement intended to require matching photo identification to name to Social Security Number? AEP suggests the drafting team clarify what is meant by “identity verification.” AEP recommends continuing to explicitly allow “Social Security Number verification” in the requirement. Again, if photo identification matching is required (in addition to SSN verification as per CIP-004-3), is it required for only new personnel? AEP recommends that the drafting team clarify that existing personnel risk assessments are sufficient until their regular seven-year update. Finally, if evidence of photo identification matching is required, it will put large, widely distributed entities like AEP at significant risk of inadvertent disclosure of Personally Identifiable Information (PII). Like many companies, AEP has worked very hard to strictly limit the collection and storage of this information – but if this evidence is required to be produced at the time of the audit, it will require personnel from outside of an entity’s HR department to have access to extremely sensitive PII. As per above, AEP strongly encourages the drafting team to explicitly allow “Social Security Number verification” in the requirement. R4.2: AEP is extremely concerned that the requirement to perform a personnel risk assessment for each location where a person has “…been employed, and / or attended school for six months or more” is very difficult to do programmatically. The location of an employer or a school is not necessarily available from the Social Security Administration or other on-line databases. It requires a subject to provide a truthful statement, and then manual processing of that statement to order the correct criminal history check. This can no longer be done programmatically, and will be enormously labor intensive. And it will still be totally dependent on a truthful and complete statement from a person who could easily “forget” certain locations. For example, many modern “schools” of higher education are virtual, and do not have a single geographic location. AEP believes this is another reason that demonstrating compliance with Requirement R4.2 as written is totally unachievable for a large entity. AEP strongly recommends narrowly on the location of residence, or returning to previous language in the requirement. R4.3: No comments for SDT recorded. R4.4: AEP believes that the combination of requirements R4.1, R4.2 and R4.4 discourages AEP from handling contractors like employees – which could weaken an entity’s program. Using an entity’s own internal “employee” program for contractor personnel risk assessments is the best possible option, but having to maintain evidence of photo id matching / identity verification for widely distributed contract personnel is an unreasonable distribution of Personally Identifiable Information (PII) – something that AEP (and other entities) must work very hard to protect. AEP believes that it is particularly difficult to validate the information provided by contractors for compliance with R4.2. Again, this combination of requirements has the effect of discouraging entities from subjecting contractors to internal programs for entity employees because the burden of collecting, validating, and protecting information for non-employees is so overwhelming.
Yes
No comments for SDT recorded.
No
R6.1: “Delegate” should be “delegate(s)”. R6.1: Somewhat duplicative of CIP-003-5, R5. R6.1: How is (i) in the “Measures” aligned with the Requirement? Why wouldn’t one of the measures be process documentation approved by the senior manager or delegate? R6.1: Aren’t (i) and (ii) and more closely aligned with R6.4? R6.1: The measures (especially (i) and (ii)) appear to expand the requirement, and add confusion about how to demonstrate evidence. R6.1: Is it reasonable to have the CIP Senior Manager or delegate(s) authorizing access in this fashion? Is that scalable? Can the CIP Senior Manager or delegate(s) authorize low level authorizers for access? AEP recommends both

re-writing the Measures, and reconsidering whether this type of authorization is scalable for a large responsible entity. (R6.2 and R6.3 are similar to R6.1, and the same comments apply) R6.2: AEP recommends "BES Cyber Systems" be replaced with "Defined Physical Boundary." R6.4: "physical or electronic" should be "physical and/or electronic" R6.4: AEP recommends the use of "are authorized" instead of "were authorized"? As long as the workflow can be produced that authorized access ("were authorized"), they can keep the access forever. As written, this requirement appears to be more paperwork and produce less security than the current requirement to (essentially) re-authorize access quarterly. R6.5: Does this requirement require assessment of the connection of accounts to groups or privileges provided to a group? Measure (i) is the former, while measure (ii) is the latter. AEP recommends re-writing the Measure to specify one or the other. (R6.6 is similar to R6.5, and the same comment applies)
No
R7.1: AEP recommends the drafting team clarify that "time of the resignation" does not refer to when they've announced their resignation ("notice"), but refers to the time when their resignation is effective – which could be two weeks (or more!) later. R7.2: AEP recommends the drafting team change this to seven days. Or, at a minimum, the next business day (instead of the next calendar day). For large organizations, with a large number of transfers, it isn't reasonable to revoke all unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day. AEP is unsure why the strict time limit is imposed on "reassignments or transfers." These are "friendly" transactions with known personnel. AEP strongly recommends a more realistic time boundary on "reassignments or transfers." R7.2: AEP suggests inserting "unescorted" in front of "physical access" to maintain consistency with other standards. R7.3: Can this be changed to seven days? Or, at a minimum, the next business day? Revoking information access on a Saturday or holiday could be very problematic.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1.1: AEP observed that Requirement R1 states "shall implement" while Requirement R1.1 only requires entities to "define technical or procedural controls." AEP recommends the drafting team make these consistent. R1.2: No feedback to the SDT. R1.3: What does "explicit" mean in this context? Does that mean that rules cannot be grouped together, or that systems cannot be grouped together in a single rule? AEP recommends that the drafting team clarify the use of "explicit." R1.3: In the phrase "…including explicit criteria for…" AEP recommends replacing the word "criteria" with "justification". The use of "criteria" implies that you need criteria to assess the quality of the justification – where the Measures seem to suggest the justification alone is sufficient. R1.3: Use of "Medium Impact BES Cyber Systems with External Routable Connectivity" in the Applicability section implies that BES Cyber Systems without External Routable Connectivity do not need explicit outbound permissions. AEP recommends the SDT should consider whether this was the intention – AEP believes all Medium Impact BES Cyber Systems should require outbound permissions. R1.4: No feedback to SDT. R1.5: AEP believes there may be other technical solutions that address FERC's desire for "two distinct security measures." For example, would two firewalls (in series, not in parallel) achieve FERC's request? Or would the Intermediate Device (Requirement 2) be sufficient? There simply may be situations where IDS / IPS can't be used, and that other solutions must be acceptable (or the requirement must be subject to TFE). AEP recommends the drafting team take another careful look at both FERC's guidance, and this requirement. If this is to remain "as is" AEP strongly recommends permitting TFEs for this requirement.
No
R2: AEP recommends the drafting team consider making this requirement (and associated sub-requirements) eligible for TFE. While TFEs are undoubtedly cumbersome, requiring an Intermediate System may result in eliminating Interactive Remote Access to certain BES Cyber Systems – and may result in lower BES reliability. While these TFEs would have to be subject to scrutiny, AEP believes the drafting team should at least consider making the mechanism available to entities. R2.1: "Intermediate Device" is defined by the services it provides. If the services described in the "Intermediate Device" definition can be provided in an alternative device(s), why is an Intermediate Device required? Could this requirement simply articulate the services that must be provided, and the definition of "Intermediate Device" be removed? R2.2: Requirement R2.2 appears to conflict with R1.5

in certain instances due to the definition of Intermediate Device. Is there a point of having “IDS”-type systems at EAP if the traffic to the Intermediate Device is encrypted? The Intermediate Device is permitted to be inside the EAP – so the traffic crossing the EAP could be encrypted. Common sense would suggest that the Intermediate Device should go outside of the EAP or be part of the EAP itself, but that’s not required by the definition of Intermediate Device. In fact, the definition explicitly allows the opposite. R2.3: No feedback to SDT.
No
R1 VSLs: It seems like Lower / Moderate / High VSLs should be described for instances where an EAP fails, or is implemented incorrectly. “All or nothing” VSLs seem unreasonable, and different types of failure should be accounted for. R2 VSLs: It seems like Lower / Moderate / High VSLs should be described for instances where an Intermediate Device fails, or is implemented incorrectly. “All or nothing” VSLs seem unreasonable, and different types of failure should be accounted for.
No
R1: AEP has a general concern with the specific inclusion of “egress” in the measures for R1.2 and R1.3. If “access” is intended to mean both ingress and egress, the requirements themselves should be specific. R1.1 uses the term “access” yet the associated measures makes no mention of either ingress or egress. A reasonable person would assume that “access” refers to the common definition of access; “a means of approaching or entering a place. “ If access to the space within the Defined Physical Boundary is what is being protected, egress controls in this context simply do not make sense. AEP recommends the drafting team remove “egress” from the Measures. R1: If implementation is going to be included in R1 then a list of all Low BES Cyber Systems will be required to demonstrate to an Auditor that the defined technical or procedural controls have been implemented. R1: AEP had hoped to see accommodation in CIP-006-5 for entities to rely on other entities’ Defined Physical Boundary for their own BES Cyber Systems. With increasing numbers of jointly located BES Cyber Assets, AEP recommends a provision for allowing “shared” or “delegated” DPB’s somewhere in Requirement R1. This will avoid a situation where a DPB must be created within a DPB. R1.1: AEP is concerned that “Associated Physical Access Control Systems” do not need to be inside a DPB. Why not have those systems inside a DPB? With (apparently) less strenuous controls for a DPB then a PSP, why not require a DPB? R1.2: Is the implication that “access” includes both ingress and egress? Why is “egress” in the Measures? What is the requirement for controlling egress? Is that for visitors? Or for those with authorized access? R1.2: If FERC hasn’t mandated a change to controlling egress, why is it in the Measures? Again, to be clear, it doesn’t appear in the Requirements. R1.3: Same comment as R1.2 regarding egress. Is it a requirement? It’s especially concerning that this appears to require “…egress is controlled by two or more methods…” R1.3: “Requiring” (via the Measures) two methods (card / bio / PIN) for egress is not reasonable. R1.2 and R1.3: Both of these requirements use “Associated” in the Applicability. AEP believes this term should have been removed. AEP recommends the drafting team determine how to apply the term “Associated” consistently throughout CIP-002 through CIP-011. R1.4: “access point” is not defined. Would a window, hatch, etc. count as an access point? Can the term “Physical Access Point” (similar to “Electronic Access Point”) be defined? R1.4: Suggest rewording:"Issue real-time alerts to individuals responsible for responding to unauthorized physical access through access points in a Defined Physical Boundary." R1.5: Suggest rewording:"Issue real-time alerts to individuals responsible for responding to unauthorized physical access through access points in a Defined Physical Boundary."
No
R2.1: “Continuous escort” is still not defined. AEP would recommend the standards drafting team emphasize the need to prevent tampering with BES Cyber Assets. As long as the escort can prevent the escortee from tampering with BES Cyber Assets, that should be sufficient. R2.2: No comments back to SDT.
No
R3.1: Why not use the same approach for “annual” events here? AEP would recommend consistency. For example, “every other calendar year, not to exceed 27 months” or something similar. R3.2: Where did the term “Associated Physical Access Control or Monitoring Systems” come from? Is “or Monitoring” a typo? AEP recommends using the defined term where possible.
No
R1 (High): This includes a “15 minute” time limit for response – apparently a requirement. This both

requires 1) response, and 2) response within 15 minutes. Neither of which are explicitly required by R1.4. Should requirements like this be introduced in the VSLs? And how do you measure compliance? R2 (Moderate): Should this say “daily” or “per 24-hour basis” similar to the requirement? And the requirement does not say “each” – should that be removed from the VSL? R2 (High): “Continuous escort” is still not defined.
No
R1.1: AEP recommends the SDT explicitly state that only enabled “listening” ports be documented. It is not always technically feasible to collect the enabled ports on a system. Is it permissible to document enabled listening network ports as “unknown” or “under investigation”? R1.1: There is no longer a technical feasible exception process for ports and services. Previous versions of this requirement were eligible for a TFE, will that be permitted or required under this version? Two approaches to identifying enabled ports and services, as well as their drawbacks are described below: 1. Port scanning of listening ports. TCP and UDP port scanning can be technically performed to enumerate listening ports, but it doesn’t address “disabling” unused ports. This approach does not appear to be fully compliant. Port scanning is not always reliable nor feasible in every situation. 2. Positive control by reviewing / modifying device configuration which is not always technically feasible. AEP recommends the drafting team be as explicit as possible about the results (and approach) expected from entities. R1.1: the measure says “and” screen shots. Producing screen shots for a large number of BES Cyber Assets could be extremely difficult. R1.2: Again, apparently no TFE allowed for this sub-requirement. This will require the use of “administrative” controls such as signs. Should this be “Disable, restrict or discourage”? AEP recommends removing this sub-requirement as the effectiveness and quality of this control will vary wildly based on a variety of factors such as environment, device type, and usage.
No
R2.1: The comma should be removed. The word “Security” should refer to “patches”, “software” and “firmware”. Not all software and firmware updates are related to security. R2.2: Can a responsible entity develop a pro-forma remediation plan to “apply all future Windows patches” or something similar? Or does a responsible entity need a patch-by-patch remediation plan? What information is required to be included in a remediation plan? Without a minimum set of required data points, responsible entities and compliance enforcement staff may disagree on the quality of the plan. R2.2: Are there limitations to the management and execution of a remediation plan such that revisions to the plan are limited? R2.3: “A process for remediation”? Could that be clearer? Perhaps, something like “execute the remediation plan developed for R2.2” or “implement the remediation plan developed for R2.2.” Can the remediation plan be condition based, such as based on the timing of a planned outage? R2.3: The 30 day window was apparently removed from this requirement, and should be removed from the “Change Rationale” as well.
No
R3: TFEs not permitted for R3 or any of its sub-requirements. This implies that either controls may be external to the systems being protected or that each discrete device is required to have dedicated controls locally installed. R3.1: Will all systems be required to “deter, detect, or prevent malicious code” locally or can external network based controls be documented and employed? R3.2: The measure suggesting “white-listing applications” can “disarm or remove identified malicious code” is incorrect. Application white-listing technology is a preventative control, not a corrective control or measure. This measure should be moved to the measures for R3.1. R3.3: What is the appropriate means to document that a malicious code protection does not use “signatures”? R3.5: There is nothing in the “Measures” column addressing how to prove the negative. Is an attestation acceptable to prove the there were no Transient Cyber Assets attached? Is the expectation that the logs are electronically generated? If so, should this be a requirement subject to a TFE? R3.5: AEP encourages the drafting team to clarify the language in this requirement. Instead of “Log each Transient Cyber Asset connection” AEP suggests something like “Log each time a Transient Cyber Asset is connected to a BES Cyber Assets or Protected Cyber Assets.” As written, the Requirement could be interpreted to mean a log is required for each connection originated from the Transient Cyber Asset.
No
R4.1: Many devices cannot be configured to alert on these events. How should an entity demonstrate compliance for devices that cannot be compliant with this requirement? Can this be addressed in the Measures? For example, in the Measures state: “For BES Cyber Systems capable of generating logs of

events, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs." R4.1.1, R4.1.2: AEP recommends striking the word "Any" in these two requirements. "Any" is unnecessary and unreasonable. R4.1.3: Appears to be duplicative with R3. AEP recommends striking this requirement. R4.1.4: This requirement is too general. AEP recommends striking this requirement. R4.3: If this Requirement is meant to address the failure of the security event monitoring and alerting system, should the Applicability be limited to "(Associated) Electronic Access Control or Monitoring Systems"? Or, conversely, if the "Applicability" is correct, can the Requirement be made more realistic? Demonstrating compliance for all BES Cyber Systems would be extremely difficult. R4.3: In the Requirements, AEP recommends this be "next business day" especially if the Applicability really is all referenced BES Cyber Systems. R4.3: In the Measures, how does "dated event logging failures and screen-shots showing how real-time alerts were configured" address event logging failures? This is ambiguous. Please clarify. Is it meant to refer to collecting before and after logs to demonstrate how long the system was out of service? R4.4: R4.4 specifies log retention periods for a subset of the Cyber Systems described in R4.1. Should the Applicability be the same for both requirements? If not, are undocumented retention period requirements to be decided by the Responsible Entity? R4.5: AEP recommends replacing "unanticipated BES Cyber Security Incidents" with "events that are not configured to alert, but should possibly be considered BES Cyber Security Incidents" if that was the intent of the standards drafting team. R4.5: "potential event logging failures" is addressed in R4.3, and should be removed from R4.5. R4.5: What guidelines or practices are acceptable for determining an acceptable summarization or sampling method?
No
R5.1: The "Measures" section says "internal and remote paths" but doesn't define those terms. R5.2: "delegate" should be "delegate(s)." R5.2: "administrator" is an attribute of a shared, default or user-specific account. It is not a generic account type. R5.2: The "Measures" section isn't well aligned with the "Requirements." Is a list of accounts required? It's in the "Measures" but not the "Requirements". Furthermore, the list of accounts should be adequately addressed by R5.3. Suggest deleting it from the "Measures." R5.4: The "Measures" section isn't well aligned with the "Requirements". The Requirements indicate that a procedure or TFE should be sufficient to demonstrate compliance. Why doesn't the "Measures" section say that? R5.5.3: Why not just go with calendar year within 15 months where technically feasible? R5.5.3: Who will determine if a time frame is acceptable?
Yes
"Medium" is appropriate as a VRF for each CIP-007-5 requirement.
No
R1.1: "…dated copies of…" seems unusual. Why is this phrase introduced here in the measures for CIP-008-5? R1.2: "…dated documentation of…" seems unusual. Why is this phrase introduced here in the measures for CIP-008-5? R1.3.3: Can "internal staff" include groups rather than individual names? Can "internal staff" be clarified to something like "internal groups or individuals"?
No
R2.1: The phrase "when incidents occur" appears twice in the Requirement. The second use should be struck. R2.2: AEP recommends changing "initially upon the effective date of the standard" to "prior to or on the effective date of the standard" if that's the standards drafting team's intention. R2.2: Should "implement" be "execute or exercise"? R2.3: No feedback to SDT.
No
R3.1: AEP recommends changing "initially upon the effective date of the standard" to "prior to or on the effective date of the standard" if that's the standards drafting team's intention. R3.2: No feedback to SDT. R3.3: No feedback to SDT. R3.4: Renaming organizations shouldn't count as "organizational…changes that impact that plan." For large organizations, updating an incident response plan within 30 calendar days of any organizational change (department name change, for example) is not reasonable. Recommend adding something like "organizational change or technology changes that would impede the execution of the plan." R3.5: AEP recommends that "each person" should be "each person or group" or "each person within a group" who could fill the defined role.
No
AEP recommends that the VRF should be higher than "Lower" – it seems this should be at least "Medium." R2: The VSLs should be more granular. Failing to follow a single part of the plan when an incident occurs is not a "Severe VSL." Perhaps this should be a "Medium VSL"?

No
R1.1: AEP recommends that the requirement make clear the plan itself can contain the conditions for activation (e.g., based upon an event classification). R1.2: AEP recommends that “individuals” should be “individuals or groups”. Titles might refer to a single person, where several people with similar (but unique) titles might be eligible for a particular role in the recovery plan. R1.3: “…and protection of information…” appears to create double jeopardy with CIP-011-1, R1. Can that clause be removed? R1.4: Compliance with R2 should be sufficient. It is very difficult to demonstrate initial verification of this information after the backup. Compliance with R2 should adequately test this process. AEP recommends merging this with R2. R1.4: Appears to create double jeopardy with R2.2. R1.5: This seems like a “nice to have” but could be an unnecessary distraction during a stressful time where SMEs should be focused on recovery. Worse still, this could cause double jeopardy with CIP-008. AEP recommends moving this to CIP-008, or making this a guideline. R1.5: AEP notes this requirement says “where technically feasible.” How would you create a TFE for this situation? Would it be created “retroactively”? Is this compliant with the NERC Rules of Procedure?
No
R2: FERC wanted to see Responsible Entities actually implement the recovery plans when conditions for activation actually occur. Not implement a “different” recovery plan when the “real life” situation occurs. Did the drafting team adequately address FERC’s comment? R2: Are exercises "Operational" or "Functional"? R2 uses both “Functional Exercises” and “Operational Exercises”. AEP suggests change to "Operational" for both the std/requirement and the Rationale. R2: What is the rationale for not requiring testing on Medium Impact BES Cyber Systems outside of the Control Centers? Perhaps these BES Cyber Systems should be excluded from R2.3, but not R2.1 and R2.2? R2.1: Use of “operational exercise” is confusing. As AEP understands it, this is not an “operational exercise” of BES operations. This is an “operational exercise” restore of a BES Cyber Asset / BES Cyber System. For example, rebuilding an actual PC – not moving BES operations to a backup site. Is there a different term that can be used for “operational exercise”? Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner. Is this a simulated event in a simulated environment or a simulated event in a fully operational environment? R2.1: Exercises in a simulated operational environment. AEP suggests change to "Exercises in a simulated or fully operational backup environment." R2.1: "Full operational exercise." Strike the word "full." (It appears to conflict with the language of the Rationale: "Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup)." R2.1: AEP disagrees that this is “essentially unchanged.” Permitting an “operational exercise” (depending on its meaning) is significantly different than what is permitted for CIP-009-3, R2 today. R2.2: Appears to duplicate CIP-009-5, R1.4. Can they be consolidated? R2.3: Use of “initially upon the effective date” is confusing. Does it have to be done prior to the effective date? Can that be clarified? R2.3: What does “representative environment” mean? Can you use “on-line” “secondary” “hot” system instead of requiring a “tertiary” system for recovery plan testing?
No
R3.1: Unless conducting an actual exercise, there’s little difference between R2.1 and R3.1. R3.1: This needs to exclude like-for-like replacement of BES Cyber Assets. Also, does vendor equipment replacement invoke this requirement? How many BES Cyber Assets within the BES Cyber System need to be replaced before this requirement is invoked? R3.2: No comments back to SDT. R3.3: No comments back to SDT. R3.4: For large organizations, updating a recovery plan within 30 calendar days of any organizational change (department name change, for example) is not reasonable. Recommend adding something like “organizational change or technology changes that would impede the execution of the plan”. R3.5: Could this say “individual or group”? In large organizations, several individuals might be included in an email distribution group, and the group would be notified – not the individuals. “Personnel” (old term) is preferred over “individual or group”.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R1.1: Could recording software “hashes” be used as an alternative to recording version

levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset? AEP recommends this be added to the requirement. R1.1.3: Need to figure out how to put boundaries on software installed on BES Cyber Assets. Are individual “applications” subject to this? Which “utility applications” are subject to this? Is the version “product level” or “executable level”? R1.1.4: “scripts” is problematic. Very small scripts may be used for a multitude of purposes, including one-time activities such as software installation. Can the word “scripts” be struck from this requirement? R1.1.5: Can you further define “logical network accessible ports”? R1.2: Suggest rewording: "Changes to the BES Cyber System that deviate from the existing baseline configuration must be authorized by the CIP Senior Manager or delegate(s) and documented." R1.3: Some of the changes for R1.2 may not be baseline changes for all BES Cyber Assets within a BES Cyber System. While the change in R1.2 may require a baseline change to an individual BES Cyber Asset – it would not necessarily require a baseline change to all BES Cyber Assets within a BES Cyber System. R1.3: There is not good alignment between Requirements and Measures. The Measures do not address the first part of the requirement: “updating the baseline configuration.” R1.4: There is no explicit measure for R1.4.1 (“determining the controls”). If compliance with R1.4.1 is going to be “measured”, a “Measure” should be created. Alternatively, the requirement to determine the controls prior to the change should be removed. R1.5: The applicability to Control Center BES Cyber Systems should be captured in the “Applicability” section rather than the “Requirements” section. R1.5: In the Measures, “descriptions of how any differences were accounted for” is (unreasonably) challenging. Unless this description is boring, uniform, useless boiler plate documentation, it simply isn’t possible to scale this to any large number of BES Cyber Assets. R1.5: In the Measures, it is unclear as to what “including of the date of the test” applies to. Is the measure simply stating the evidence must include the date of the test, or is it stating that any differences in the date of the test must be accounted for?
No
R2: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R2.1: How frequently must changes to the baseline configuration be monitored for or must it be done continuously? There is no defined time frame for the detection. What is the acceptable detection window? If the change monitoring cannot be done in an automated manner, does it need to be done manually? R2.1: In the Change Rationale section, text “DHS Catalog & addresses FERC Order 706, paragraph 397” is duplicated.
No
R3.1: The applicability includes “or Monitoring” for Electronic Access Control Systems. Is this intentional? R3.2: Difficult to articulate (and account for) all of the differences in the test environment. While Responsible Entities can endeavor to make their test environment as similar as possible, creating the documentation required seems like burdensome busywork. R3.3: AEP recommends the measure say “of any tools used to perform the assessment” or something similar, since “tools” may not be used in this active vulnerability assessment. R3.3: Applicability does not include Medium Impact BES Cyber Systems, or Associated Protected Cyber Assets. Is the implication that a new, but non-essential (?) Cyber Asset becomes an Associated Protected Cyber Assets after being added to the BES Cyber System? AEP recommends that the applicability of R3.3 be extended to include at least Associated Protected Cyber Assets. R3.4: If security controls tested in the assessment are found to be deficient, would that not be a violation of the CIP standards requirement for that security control? That would require a self report. Could the self report mitigation plan be used as the action plan for 3.4? Guidelines and Technical Basis: Includes sections on “Wireless Review” and “Wireless Scanning” which seems unrelated to the requirements.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
R1.1: Should “a documented program” be listed in the Measures? The existing Measures appear be the results of a documented program and it seems only logical that the documented program itself should be a measure of compliance. R1.2: “Part” / “Part” / “Part” should say “Applicability” / “Requirement” / “Measure” R1.2: Should “a documented program” be listed in the Measures? The existing Measures appear be the results of a documented program and it seems only logical that the documented program itself should be a measure of compliance. R1.2: How do you prove that “hardcopies of information stored in a locked file cabinet…” exists? Are you expected to show the cabinet itself? R1.2: Why isn’t a “PSP” or other access restricted boundary listed as a Measure for

controlling access to Information? “Locked file cabinet” seems needlessly specific. R1.2: Why isn’t a locked office listed as a Measure for controlling access to Information? “Locked file cabinet” seems needlessly specific. R1.3: “Process” should be listed as potentially plural; “process(es)” since the requirement permits more than one process.
No
R2: This still doesn’t address the issue that BES Cyber System Information is not typically contained on the BES Cyber Assets themselves. R2: Can this require a documented program for disposal and redeployment? And allow you to write your own program for disposal and redeployment? R2: Can this require the “assessment of adherence” that’s found in R1.3? It seems appropriate for this type of program. R2.1: Can this say “Prior to the…of media containing BES Cyber System Information…” rather than “Prior to the…of BES Cyber Asset media”? R2.1: “cleared” appears to just be a different word for “erase.” “Prevent the unauthorized retrieval” in the Requirement is much closer to the actual intent. Can that phrase be used in the Measure as well? R2.1: It does not always make sense to clear the entire media if the Cyber Asset is going to be reused, especially if it is to remain as a component of the same BES Cyber System. Simply clear the “BES Cyber System Information” from the media – not the entire media. R2.1: “Reuse” may not be the most appropriate term in the measure. “Release” may be more appropriate, or “release to non-Responsible Entity personnel” or something similar. R2.2: No feedback to SDT.
Yes
VRFs / VSLs: Not yet reviewed by AEP.
No
AEP is still concerned about the impact of version 4 on version 5. Implementing “version 4” on a “bright line” set of assets and then implementing “version 5” on those assets shortly afterwards is unnecessarily difficult. Could these new standards be accompanied by a series of “readiness” audits or something similar? There is concern that with an abrupt transition from Critical Assets / Critical Cyber Assets to BES Cyber Assets, etc. there will be uncertainty about whether the compliance program includes the “right” assets. This type of “break in” period would be essential to understanding how the standards are going to be interpreted “in real life.”
Group
MRO NSRF
Will Smith
Yes
The NSRF is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The NSRF does agree that CIP-003-5 through CIP-011-5 be moved forward. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. If the SDT does not take this recommendation then the following comments are submitted concerning Version 5 CIP Standards. Significant work needs to be performed on the definitions. Many times new definitions are proposed in version 5 that aren’t an absolute necessity. This would require entities to unnecessarily revise documentation and drawings just to meet new wording in a definition when the old definition or a change to the definition itself, rather than the term/phrase, would suffice. For example, instead of changing Critical Cyber Asset to BES Cyber Asset, retain the term Critical Cyber Asset and change the definition of Critical Cyber Asset to include “within 15 minutes”. Definitions may also confuse and unnecessarily expand the scope of compliance. This will likely generate the need for Compliance Application Notices and Standard Interpretations. The CIP Rev 5 definitions and requirements are confusing in that they require entities to carefully align separate definitions and requirements to understand the full impact. They also

unnecessarily expand the compliance scope into assets not currently covered by CIP Rev 4. This expansion will increase the burden on almost all entities. One example is, a BES Cyber Asset is defined as a "Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, adversely impact one or more BES Reliability Operating Services". The use of adversely impact is ambiguous and will lead to people applying their own interpretation to what adversely impact means. An entity may have generation connected at the distribution level that when unavailable may adversely impact any one of a number of items listed in the definition of BES Reliability Operating Services. Recommend that the SDT update BES Cyber Asset to be: "A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its operation, mis-operation or non-operation, when required, would impact the reliable operation of the BES within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance". This recommend definition is based Section 215, Electric Reliability, (a), (4) of the Federal Powers Act. The above recommended definition would also allow for the definition of BES Reliability Operating Services to be deleted, since BES Cyber Asset is clearly identified. The definition of BES Reliability Operating Services includes several items that a non BES user or owner does in real-time. Other examples of errors: BES Cyber Asset: Contains multiple references to other definitions. It is unclear as to the "within 15 minutes of its operation" inclusion. The redundancy of devices should be taken into consideration if there is a totally isolated redundant system providing the same functions or in a supervisory role. In protection schemes, there are primary and secondary relays which protect the same lines and a good practice recommends the relays have different logic/hardware to avoid common mode failures (totally independent of each other). BES Cyber System: Need to correct reference to Maintenance Cyber Asset BES Cyber System Information: Need to define "BES Cyber System Impact" (is this based on section 215 of the Federal powers Act?). Situational Awareness: Definition includes the term "Situation Awareness Operating Service" that is not defined. The Current day and Next Day Planning functions can typically be performed on a corporate PC, does this bring the entire corporate network into scope? Control Center: Based on this definition, a Control Center could be a building at a substation with 2 RTU's that monitor a 345 KV substation with multiple transmission facilities (lines) and a 115 KV substation with multiple transmission facilities (lines) in two different yards (locations) but geographically adjacent. Need to clarify that the two or more locations refers to some type of geographical separation. Otherwise the control building could meet the bulleted items under the Control Center definition. Transient Cyber Asset: Need to break up the 3rd qualifier based on the intention of the SDT as such: "3) capable of altering the configuration, or (and) 4) capable of introducing malicious code to the BES Cyber System." A second example of where definitions may also confuse and unnecessarily expand the scope of compliance is shown just below: CIP-002-4 requires cyber controls on: 1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection. (Emphasis added) Whereas: CIP-002-5 requires cyber controls on: Control Center One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations: • Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, • Inter-utility exchange of BES reliability or operability data, • Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES, • Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function, • Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES • Coordination of BES restoration activities. 2. Medium Impact Rating (M) Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: 2.13. Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners; or (2) generation control centers that control 300 MW or more of generation (emphasis added) The concern here is that every Distributed Control System (DCS) that control two or more generators or substations with a total output of more than 300 MW will now be subject to the CIP standards. Even if the DCS is not externally connected by serial or routable protocols it will be subject to the CIP

standards.
Yes
The NSRF is recommending that since CIP version 4 has been approved by the NERC BOT and is awaiting approval from FERC, that CIP-002-5 be placed on hold. Our industry has approved CIP-002-4 and the terms Critical Assets and Critical Cyber Assets are well known terms within our current cyber security plans. The NSRF does agree that CIP-003-5 through CIP-011-5 be moved forward. The following supporting information outlines a superior solution to the proposed version 5 standards that meets the main FERC goal of including more critical assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. The proposed solution below allows entities to start from a firm industry approved base (CIP-002 version 4) and modify its controls CIP-003 through CIP-011. This approach also appropriately maintains an ultimate focus on protecting the electric grid elements which is the fundamental reason all NERC standards exist. The proposed CIP version 5 approach inappropriately drifts towards an Information Technology based approach. While this is understandable, given the fact cyber security is involved, any solution must remain focused on protecting the Bulk Electric System from instability, uncontrolled separation, and cascading as a whole from a relatively large coordinated attack. Issue: As currently drafted Version 5 of the CIP standards: • Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. • Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. • Exceeds FERC's 706 order without justification. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: • Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed by the drafting team in Rev 5 • Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. ¶253-258, 270-273 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. ¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. ¶294-297 • Not exceed FERC Order 706: o ¶284: "… there is no formally accepted method for identifying critical cyber assets before us at this time … we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o ¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access … We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: • That identifies which assets in CIP-004-2 are High Impact and • Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. • Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described in this paper and meet FERC Directives in order 706. If the SDT does not take this recommendation of maintain CIP-002-4, then the following comments are submitted. Keep the "bright-line" criteria thresholds defined in CIP-002-4 in the CIP-002-5 standard. There was much industry input into developing these thresholds and it does not seem appropriate to modify them again. It is difficult for utilities to keep up with the changing thresholds in the changing CIP versions and associated implementation plans, with no BES reliability improvement Issue - 1 high Impact, bullet 1.2, states: Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority. The NSRF does not understand how this can be applied to every BA, regardless of size. Upon review bullet 1.2 has qualifiers for a TOP in order to be a High Impact category (notwithstanding that a TO should not be included since TO's are not required to have primary or backup control centers). Recommend the similar qualifiers contained bullets 2.1, 2.3, 2.4, and 2.12 be written for a BA to be in the High Impact category. We can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of lines, Blackstart Resources, etc, for being considered High Impact or Medium

Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, we want to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the High Impact Rating? Issue - Criterion 2.7 in Attachment I describes the "weight value" to be applied to transmission lines. There is no guidance given for transformers. Many entities may treat a facility that has multiple voltages as separate substations, with separate control houses, and may be assessing the independent Impact Level of each voltage as separate facilities. Therefore, there must be some guidance on how to deal with transformers. Furthermore, it is suggested that the weight value given a transformer (if transformers are to be included in the calculation) be the weight value of the secondary, not primary side. For example, a 345kV substation may have a single 345kV transmission line out of it, weighted at 1300. That same substation may then have two 345kV/230kV transformers. It is not obvious from criterion 2.7 what the total weight of the substation would be. It is suggested that the secondary voltage be used (if transformers are to receive a weighting value) making each of these transformers valued at 700, for a total of 2700 at this substation, making it Low Impact. However, if the primary voltage level was used to determine the weight, the transformers would each count for 1300, making the total weight value of this substation 3900, and a Medium Impact facility. It is suggested, if transformers are to be included, that the secondary voltage be used because, from the 345kV bus in this example, its two additional outlets (the transformers) are only capable of 230kV outlet flows, even though they are connected to the 345kV bus. Issue - Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Issue - Criterion 2.11 in Attachment I states "Each SPS, RAS or automated switching scheme that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations." It is unclear whether the phrase "that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROL violations" refers to the SPS itself or the BES elements that the SPS operates. It is possible (and likely) for an SPS to be a higher Impact Level than the BES elements that it operates. Assuming the phrase is meant to apply to the SPS, a suggested re-wording of this phrase is the following. "Each SPS, RAS or automated switching scheme that operates BES Elements and is capable of causing one or more IROL violations if the SPS is destroyed, degraded, misused or otherwise rendered unavailable. We propose the following: Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency.
No
Issue - What is the NERC basis for 30 days. Many reviews are performed annually. NERC has not provided any technical justification for a 30 day update. An annual update is sufficient based upon the low probability of a serious cyber or physical attack. Issue - The text "all other BES Cyber Assets and BES Cyber Systems … shall be deemed to be Low Impact." This text appears to include all BES Cyber Assets in CIP scope, which was not directed by FERC Order 706.
Yes
Issue - With recent guidance on the term "annual" provided by NERC, it may be prudent to replace the phrase "and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals" with the word "annually".
No
Issue – We believes that the VSLs recognize the fact that entities of different sizes are taken into account in the severity levels and associated impacts to the BES.
No

Issue - Most of the changes made to CIP-003, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, but do result in increased bureaucracy and implementation costs for 241 entities with existing programs. We suggests the FERC directives be addressed within the structure and language of CIP version 4. We propose the following requirements for CIP003-5: R1: Cyber Security R2: Leadership R3: Exceptions R4: Information Protection
No
This is an administrative task and once written does not add to BES security.
Yes
Issue - With recent guidance on the term “annual” provided by NERC, it may be prudent to replace the phrase “and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals” with the word “annually”. Issue - suggest changing to annual “review” and NOT approval. Entities need not “approve” the same security policy if there are no changes or updates.
Yes
Yes
Yes
No
Issue - Many of the changes made to CIP-004, in general, were not directed by FERC Order 706. These changes do not result in improvements to security, and they increase implementation costs for 241 entities with existing programs. We suggests the FERC directives be addressed within a structure and language that is more in line with CIP version 4. We propose the following requirements for CIP-004-5: R1: Awareness R2: Training R3: Personnel Risk Assessment R4: Access
Yes
Yes
No
Issue - Add clarification to R4.4 in terms of vendor support from foreign companies. Please clarify when an Entity or contractor is initially in the CIP Standards then they are removed (for some reason) then they are brought back into CIP compliance. Is the risk assessment previously obtained in it is still within 7 years?
Yes
No
Issue - In FERC Order 706, paragraph 381, the Commission stated its intent is to ensure there is a clear line of authority. Order 706 did not direct making the senior manager authorize every individual change down to the account level. The version 5 draft is an additional administrative burden that does not commensurately improve security of the Bulk Electric System and creates a disproportionate amount of bureaucratic work.
No
Issue - For reassignments requiring a different level of access, there may be the need for a large amount of work in setting up new user accounts, modifying user accounts, changing firewall and router rules, etc… that cannot be accomplished by the end of the next calendar day without jeopardizing reliability. This is also an issue for BES Cyber System information for entities which are using document management systems with individual accounts to restrict access to information. It is usually easier to “remove” an account than it is to “modify” an account, yet the modification of these accounts is subject to a single calendar day while the removal of these accounts is allowed for 30 calendar days. Due to the amount of reconfiguration needed for these types of changes, it is suggested to allow at least 7 calendar days for modifications in access levels. Issue - FERC Order 706 did not direct a change. We recommend retaining CIP-004-4 where revocation already is covered.

Issue - The time requirements are too restrictive for Medium Impact BES Cyber Systems. Allowing 7 calendar days for R7.1 and R7.2 would be more acceptable and practical for systems that may not be controlled centrally. Issue - We appreciate how the SDT tried to give treatment to the “immediate revocation” requirement of the FERC order in Part 7.1. However, we feel the current language is too open for interpretation. Even with the footnote qualification, an auditor could still interpret “at the time” to mean literally “to the minute”. Complicating matters is the fact that there is often no way to measure specifically when a person resigned or is terminated. Our suggestion for Part 7.1 is to restate as: “Develop and implement a program to revoke an individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of resignation or termination”. This way, the entity is measured for compliance to their own program and not struggling to provide time-stamped comparisons that may not exist. For Part 7.5, it is possible that entities use shared accounts for remote access. Suggest adding “...if shared accounts are used for Interactive Remote Access to BES Cyber Systems, passwords must be changed at the time of resignation or termination per Part 7.1”.
Yes
No
Issue - R1.1. Appears to require that you document Low Impact Cyber Systems. This requirement should not be required for Low Impact BES Cyber Systems; otherwise we have to prove to auditors that external routable connectivity is not used at EVERY Low Impact BES Cyber System.
No
Issue - The requirements ignore the fact that some utilities have their own (unique) communication network from the Control Centers to the substations. Adding encryption devices and additional devices adds additional points of failure without increasing security. Exceptions should be made for interactive remote access across company owned and operated communication links.
Yes
No
Issue - In the “Measures” column of Table R1, Part 1.1, it states the need for documented “operational and procedures controls”, while the requirement is “operational or procedural controls”. Please correct the Measures column to be consistent. If the error was in the Requirements column, we disagree that operational physical access control systems should be required for Low Impact BES Cyber Systems. Issue - The Requirement in Table R1, Part 1.2 and Part 1.3, should define whether or not these physical access controls are to be operational, procedural, either, or both for Medium Impact and high Impact Cyber Systems as was done in Part 1.1 for Low Impact Cyber Systems. If operational controls are required, is a separate operational physical access control system needed to monitor the primary physical access control system or is it allowed for a system to monitor access to itself? Issue - For CIP-006, in general, we disagrees with changing the definition name from Physical Security Perimeter to Defined Physical Boundaries because it unnecessarily creates the need to update numerous procedure documents and physical security drawings, etc. Changing the term does not improve security, but increases confusion and costs for 241 entities that have Physical Security Perimeters.
No
Issue - R2.2 does not seem applicable to Medium Impact Substations. The logging of entry and exit of visitors will be tedious without much value. R2.2. should only be applicable to Medium Impact Control Centers.
No
Issue - R3.1 and R3.2 will be troublesome for Low Impact Facilities that may use procedural controls for Physical Access Control. What hardware or devices will be included? R3.1 and R3.2 should only be for applicable electronic physical access control systems
Yes
Yes

No
Issue - Suggest changing the term “remediation” to “mitigation”. R2.3 appears to require the installation of the patches, where some utilities may mitigate the vulnerability through procedural controls.
No
Issue - R3.1. Allows the Responsible Entity to choose which approach they want to take “deter, detect, or prevent”. If a Responsible Entity chooses to deter or prevent malicious code by procedural controls on isolated control systems (i.e. non-routable serial links), requirement R3.2 and R3.3 are impossible to achieve. Additionally, R3.3 requires modifying a tested and working control system at a substation with the possibility of inadvertently introducing malicious software with manual updates (e.g. using thumb drives to install signature updates on non-networked systems.) Recommend excluding Medium Impact BES Cyber Systems that do not have external routable connectivity. (Most AV or malicious code software cannot recognize new malicious code such as Stuxnet until the signatures are discovered anyway).
No
Issue - FERC Order 706 didn’t direct changes. CIP-007-5 R4.1 - The enumerated list is too prescriptive for the requirement. Add to guidelines. CIP-007-5 R4.2 – Some assets can log, but not alert. Remove “real-time”. CIP-007-5 R4.3 – Clarify timing. We propose revised text, “Activate a response to event logging or alerting failures before the end of the next calendar day after identification. Issue - It is great to see how the SDT allowed entities to develop their own system events related to cyber security, but this leaves an open door for auditors to apply their own approach (and interpretations) to what the auditors believe is acceptable. R4.1. will be troublesome for entities to prove compliance with Medium Impact BES Cyber Systems with no external routable connectivity, unless the auditors accept the configuration files and not the actual logs. Issue - R4.2. Also leaves a large audit hole for the entity determining what events necessitate a real-time alert and the auditors having differing opinions of what they feel the entity should include. Issue - R4.3. Additional information should be provided for the requirement on how it will be possible to detect an event logging failure for a failed physical contact/sensor before the end of the next calendar day (e.g. door alarm contacts). Suggestion: This should be rewritten to only include “the event logging system failure, not to include sensors).
No
Issue - Delete R5.2 because it replicates the CIP-004 access authorization requirements and could create double jeopardy. Issue - R5.5.1 – FERC Order 706 did not direct a change to password length. Although an increase in password length from six to eight characters improves security, an increase to ten would improve it more and so on. Where does one stop? Not all assets have capability for longer passwords. We recommend retaining the six-character password. Issue - R5.4. Should be limited to Entities having a policy in place that all default passwords should be changed. Proving compliance at a sampled location basis opens up the door in an audit to have entities having to prove compliance on all their BES cyber systems if there is 1 finding. The 1 finding would require the entity to have to inventory all Low Impact Cyber Systems and show that every system had the default password changed. The requirement also leaves open the auditor’s interpretation of what is considered a Low Impact Cyber System at a sampled location, since there is not an inventory required by the standard.
Yes
No
Issue – The SDT should coordinate more closely with EOP-004-2, SDT
Yes
Yes
Yes
No

Issue - R1.5 states, “Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.” As FERC Order 706, paragraph 708 states, “should not impede or restrict system restoration”, we recommend this proposed revised text: “Preserve data, when it does not impede or restrict system restoration, if necessary to determine the cause of any event that triggers activation of the recovery plan(s) as required by Requirement R1.
No
Issue - The wording in the Requirement Column of Table R2, Part 2.2, implies that all backup media must be tested annually. If an entity, for example, has 25 Windows Servers – that entity should be able to annually test a Windows backup without having to test the backup for each system, especially if the same backup system is being used for all Servers. This is even more extreme in the case of substation cyber assets, such as protective relays. Recommend changing the language “Test any information used in the recovery …” to “Test information, for each type of Cyber Asset, used in the recovery …”.
No
Issue - In Table R3, Part 3.4, the language “Update recovery plan(s) to address any organization or technology changes…” is too vague in regards to technology changes. Recommend wording as “Update recovery plan(s) to address any organization or implemented technology changes…” Issue - R3.1. Is not clear on how soon the recovery plan has to be updated “when BES Cyber Systems are replaced”. Suggestion: Include “or within 30 days of when BES Cyber Systems are replaced.” Recommend that “Update recovery plan(s) to address any organization or implemented technology changes that would prevent a successful implementation of the recovery plan”
Yes
No
Issue - The draft requirement is too prescriptive, which was not directed by FERC. Move the details to guidelines. Recommend limiting the applicability to High Impact Critical Cyber Assets, which will allow entities to focus security improvement efforts on the highest priorities. Issue - R1.1. Will be time-consuming for Medium Impact BES Cyber Systems at substations/plants. The number of IED’s and programmable devices are very large and some of these devices may have multiple modules or add-on boards with different software versions. Issue - R1.2. and R1.4. Will create problems when making emergency repairs in the field that require replacing a “card” or “module” with different software versions and obtaining CIP Senior Manager approval. Suggestion: Provide a separate requirement for Medium Impact Control Centers and Medium Impact Systems excluding Control Centers which allow more flexibility for the type of environments and equipment. For Medium Impact BES Cyber Systems excluding Control Centers could require documenting baseline configurations on only a subset of the cyber assets (e.g. HMI’s, EAP’s, etc.) not including meters, gauges, battery chargers, electronic programmable thermostats, relays, modules, PLC’s, etc
No
Issue - We recommend that the applicability of Table R2, Part 2.1 include only “Medium Impact BES Cyber Systems with Routable Connectivity”. By requiring baseline monitoring of a system, the existence of a routable connection would be required. If an entity feels that a Medium Impact BES Cyber System should not have routable connectivity out of the perimeter (for example, a substation), then it should not be required to automatically detect baseline configuration changes since the implementation of such a system would require a routable connection from the system server to the Cyber System. Furthermore, some entities may have Medium Impact Cyber Systems at locations where the only means of communication is a low-quality analog microwave system, which may not be able to accommodate the traffic of a baseline configuration system. Issue - FERC Order 706 did not direct authorization by the senior manager or delegate, but to “express acknowledgement of the need for change control.” We recommend this can be achieved with revised text, “Authorize changes to hardware and software components of Critical Cyber Assets.” Issue - R2 does not provide any benefits and any changes should already be covered under R1.3. of CIP-010. Recommend to remove this requirement. Issue - Requirement R2 needs a lot of work and justification. Perhaps unintentionally, this requirement as written will result in another massive filing of TFE’s, since we can’t install a “Tripwire” on my Router. While the purpose of the requirement is well-intentioned, with good reference to best practices, the application doesn’t work outside traditional IT server-based cyber

assets. This is a net-new requirement within CIP that, if retained, will require major initial and ongoing investment by entities for little reliability benefit. We recommend striking R2, or vastly limiting its scope (Server-type assets at Control Centers, for instance).
No
Issue - Annual vulnerability assessments on Medium Impact Cyber Systems will prove to be very costly and resource intensive for utilities with multiple substations in this category that are geographically dispersed. We recommend allowing Medium Impact Cyber Systems to have 2 years between vulnerability assessments. Issue - Though FERC directed guidance for Vulnerability Assessments, the rewritten standard's general reference to "security controls" could result in varying interpretations and likely expansion of assessment scope. Issue - R3.1. Needs to be reworded to more clearly define if the assessment is a vulnerability assessment or only an "assessment of the security controls", such as the EAP and Physical Access Controls. Issue - R3.2. Should allow entities to perform an active vulnerability assessment on either the production system or the test environment to meet the requirement. This will allow entities to make the choice on which environment to use and not require the documentation of differences between the test environments and production environments that leave entities open for interpretation of differences by auditors. Issue - For Part 3.2, please clarify whether all cyber assets need to be included in the assessment, or a subset, or representative sampling, or entity defined. There are certain cyber asset categories where "test" systems just aren't economically feasible. What is the acceptable deviation between test and production the auditors will allow? As written, and without explicit language in the requirement, our entity fears this will be a topic of a CAN later. Issue - For Part 3.3, please clarify whether "new Cyber Asset" means literally that or, more reasonably, could mean "new Cyber Asset category" or a new make/model, or a new function. It would be reasonable to test something that brings net-new functionality to a BES Cyber System, but if when replacing an end-of-life or failed component, it wouldn't make sense.
Yes
No
No
Issue - R2.1. Needs to include additional clarification of devices that are included. Where do protective relays or devices that have flash memory or other on-board memory media fall? Does this apply when reusing the device from a Medium Impact BES Cyber System to a Low Impact BES Cyber System? The application guideline does not distinguish if there is a difference between impact levels and only refers to reuse outside of a BES Cyber System (e.g. could go from High-Medium-Low without being erased).
Yes
No
Issue - It is imperative for the industry to know whether or not Version 5 will supersede Version 4 well in advance of any implementation plan. If Version 4 has a short implementation period before Version 5 is in effect, entities will view their efforts to comply with Version 4 as "wasted" in many cases because the infrastructure required for a Version 4 Critical Asset is more than that of a Version 5 Medium Impact facility. It would be irresponsible to ask entities to "over-protect" facilities that will not be High Impact with Version 5 right around the corner. In addition, this could also have a drastic impact on decreasing reliability as many entities may elect to remove all routable protocols and dialup access to cyber assets within Version 4 "Critical Assets", to bide them time until Version 5 becomes effective. During this time, engineers would not have access to troubleshoot protection systems, retrieve fault data, and perform multiple other duties without having to travel to a remote site – this could result in prolonged customer outages, and possible instability with known defects in design taking longer to correct. Entities realize that NERC has made an effort to do this, however, there is still risk associated with version 5 not passing in time to supersede version 4. This could be catastrophic to the standards development process.
Individual
Chris de Graffenried
Consolidated Edison Co. of NY, Inc.

No
Minor corrections should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.
No
4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.
No
1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices (R7.5).
No
Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.
No
Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to

alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No
No
The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.
No
R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence

could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should include language indicating that the registered entity identifies the “authorized individuals”.

No

CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.

No

General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Individual

David Burke

Orange and Rockland Utilities, Inc.

No
Comments: Minor correction should be made to list of topics under R2. They are listed as 1.1, 1.2, 1.3 etc. They should either be labeled as 1 through 10, or 2.1, 2.2 through 2.10.
No
Comments: 4.1 and 4.2 do not clearly indicated whether an entity current PRA policy covers full identify verification and documentation of any PRA that could not go back a full 7 years. It should be made clear whether either of these requirements is retroactive or whether any PRA prior to the effective date of the standard are grandfathered. It is recommended that the committee not require previously completed PRA to be updated.
No
1. R7.1 is unclear even with the footnote description of what the desired time frame is for “at the time” of resignation or termination. The phrase “at the time” needs to be defined as simply same day, before COB or end of day. The requirement also appears to apply to any reason for departure from the company. An individual leaving for retirement or termination due to unethical behavior would be treated the same. We feel there needs to be a differentiation between an individual being “fired” and an individual leaving for other reasons. It is recommended that same day revocation be required to termination for cause, and a two day revocation for any other departure. 2. The revocation periods for R 7.2 and 7.3 should be subsequently changed to match the recommended two day revocation mentioned above. 3. For environments that do not have external connections and maintain physical security access, such as individual non networked microprocessor relays, the risk to system reliability associated with frequently accessing the relay for purposes of changing the password outweighs the benefit achieved through this password change. It is recommended to alter this requirement to allow periodic (twice per year) password changes on these types of devices. (R7.5).
No
Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table.
No
Comments: Amend the VSL table to remove the 15 minute response requirement for issuing real-time alerts (R1.4). R1.4 requires issuing alerts in real time, but the related VSL table requires responding to alerts in 15 minutes. There is a disconnect between the requirement and the VSL table. Also reference to part 1.6 appears to be incorrect, should be 1.4.
No

Comments: The change to R2.2 goes beyond the stated rationale of requiring the current assessment to include the identification of what/who the source of the patch is so the time of availably can be determined. The new requirement now also requires a plan vs. assessment and requires including in the plan a defined timeframe; each of which is beyond the rationale. It is recommended that the word “plan” be replaced by “assessment” as is the current requirement, and that the additional requirement to include in the plan a defined time period be removed as it is in the current requirement. If a time frame is desired, we recommend that the timeframe be a planned timeframe and not a fixed timeframe. It is also recommend that a “plan” not be required as it implies a more extensive documentation of the patch reviews which will require additional paperwork that will not add value to the patch process.
No
Comments: R4.5 requires a manual review of a sampling of logged events every two weeks. The frequency is excessive, requiring 2-3 days per review, and will provide minimal value. We recommend once per month (R4.5). R4.3 – The requirement as written can be interpreted very broadly. It is not clear whether the intent is to detect a device has stopped sending log or the logs have stopped being accumulated by the receiving end (Syslog for example) is vague. If it requires detecting something is not sending logging within 24 hours this can be an issue, as some devices do not send logs every day. Some UPS devices , KVMs, and network switches only send a log if something occurs. There may several days without use and therefore no logs. Also, every time someone shuts down a workstation logs will not be sent. If action needs to be taken each of these times that would require documenting on a daily basis numerous events. This requirement should only address that action if the log repository has stopped recording incoming logs.
No
Comments: R5.4 is not clear as to whether unique default passwords applies to application level passwords only or includes default vendor user passwords also. The language needs to be clarified.
No
Comments: R3.2 requires active scanning in an environment that models baseline configuration. This may be impractical to replicate, the replication will need to be maintained and the some systems may have issues with active scans. Recommendation: A complete active scan should not be required (R3.2).
No
Comments: CIP-011-1 Requirement 1.1: The Measures associated with R1.1 indicate that evidence may include indications on information (e.g., labels) that identify it as BES Cyber System Information. It is suggested that the SDT expand on what types of repository would require labeling. For example, it may not be reasonable to label micrographic media, but rather label the cabinets or a room where the media is stored. Recommendation: We recommend allowing the entity appropriate discretion when applying labeling. CIP-011-1 Requirement 1.2: Measures associated with R1.2 indicate that evidence could be provided that shows user access is implemented on a “need to know basis”. The Measure should state that “need to know” personnel are determined by the registered entity. Similarly there is a suggested Measure that hardcopies of information be stored in a locked file cabinet with keys provided to only “authorized individuals”. Recommendation: The Measure should

include language indicating that the registered entity identifies the “authorized individuals”.

No

Comments: CIP-011-1 Requirement 2.1: “Evidence may include, but is not limited to, records that indicate that BES Cyber Asset media was cleared prior to its reuse.” Recommendation: SDT should define what “cleared” means. The language in footnote #2 should be included in the wording of R2.1, to ensure it becomes part of the Requirement.

No

General Comments: 1. Applicability sections of CIP-002-5 through CIP-011-5: the Applicability sections should be consistent. Note that in CIP-005-5 and CIP-006-5 the Applicability sections 4.2.2 are different from the other CIP standards. We recommend that the drafting team adopt consistent Applicability language across all Version 5 CIPs. Alternatively, the drafting team should explain any Applicability variances between the various Version 5 CIPs. 2. CIP-006-5 Requirement 1, Guidance section on pp. 22 and 23 (Guidelines and Technical Basis): “While the focus is shifted from the definition and management of a completely enclosed “six-wall” boundary, it is expected in many instances this will remain a primary control for controlling, alerting and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems. … Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.” Comment: In reviewing CIP-006 – 5 we have seen that the “enclosed 6 wall” wording is removed, but it appears as though six walls are still required. The guidance section mentions that the Defined Physical Boundaries are allowed to have openings less than 96 square inches but does not exclude the need for 6 walls, only that they are not required to be completely enclosed (excerpt above). Is this correct? Would a window be considered an “opening,” to be protected by a barrier as noted in the guidance? The CIP wording could be read as requiring a ‘ceiling’ over open air substations in order to preclude exceeding the 96 sq. in. and 6-inch limits. We do not believe that this was the drafting team’s intent. What was the drafting team’s intent? Recommendations: We suggest that this matter be clarified by the addition of wording specifically allowing an exception from this requirement for open air substations, such as, “This requirement does not apply to open air substations” or “This wording is not intended to require placement of a roof over open air substations.” Alternatively, if it was the drafting teams’ intend to apply this requirement to open air substations, then would surrounding all BES Cyber Systems in six-walled enclosures within an open air substations meet the objective of this requirement? Clearly, a roof should not be required for and physically cannot be installed over all open air substations. 3. The use of the “Measures” column for each requirement is beneficial as are the guidelines of each CIP standard. Providing these as part of the standards can imply that they are part of the requirements. By this one could see that by meeting the measures for each requirement that will be in compliance. Also the guidelines provide much more information than the requirements. The requirements tell you to perform an assessment without specifics while the guidelines provide specifics. Are the guidelines to be read as requirements? For example, A Defined Physical Boundary is required, but it is not until the user reads the guidelines is there mention to it needing to be enclosed completely with limitations on the openings. The requirements call for a active vulnerability assessment and it is not until the guidelines that what should be in an assessment is provided.

Group

Salt River Project

Cynthia Oder

Yes

No

SRP agrees with the proposed criteria.

Yes

Please specify implementation timeline for the compliance of the newly identified and categorized BES Cyber Asset(s) and/or BES Cyber System(s).

Yes
Yes
Yes
Yes
Yes
SRP suggest removing "between reviews and" tp be consistent with the language in CIP-002-5 R2 and clarify that the time requirement is lined to the approval only.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
A clear definition of where encryption is needed for Remote Access needs to be provided, in particular where encryption needs to take place; e.g. at the source, from the source and the network to the access point, from the source to the network to the ESP, from the source all the way to the end-point, etc.
Yes
Yes
Yes
Yes

Yes
No
SRP suggests including language to specify this requirement is applicable only when technically feasible, consistent with the language in CIP-005-5 R2.
Yes
No
SRP suggests modifying the requirement to clarify if running antivirus on the transient device itself satisfies the requirement of malware protection and to specify this is required only when technically feasible (similar to language in CIP-005-5 R2).
No
SRP suggest modifying the requirement to allow for automated alerts to replace manual reviews or at least for the use of automated alerts to lengthen the time between manual sampling of the logs.
No
SRP suggests modifying the requirement to indicate that the implementation of all numeric two-factor authentication is acceptable.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
SRP suggests modifying the requirement to include the signoff from the Asset Owner and allow the Asset Owner to delegate this authority to the appropriate Manager.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Group
Luminant
Rick Terrill
Yes
The BES Cyber Asset definition states that “Redundancy shall not be considered when determining availability. Recommend clarifying as follows “Redundancy shall not be considered when determining classification as a BES Cyber Asset”..
Yes
The current Version 5 draft of the NERC CIP Cyber Security Standards will have a significant negative impact on the reliability of the ERCOT Bulk Electric System (BES). In particular, the Version 5 CIP Cyber Security Standards would severely inhibit the ability to restore the ERCOT grid in the event of a complete or partial system blackout. While Blackstart Resources in ERCOT today may be classified as Critical Assets, many do not have external Routable Protocol or Dial-up connections. Thus, they are not required to implement the current CIP-003-3 through CIP-009-3 requirements. The Medium Impact ranking proposed in the Version 5 draft of CIP-002 for Blackstart Resources would require implementation of a majority of the CIP Version 5 requirements for all Blackstart Resources regardless of the external routable connectivity considerations, and represents a step change in CIP compliance activities and costs. Typically, Blackstart Resources in ERCOT are older, smaller units with very low capacity factors and limited revenues. The application of the Medium Level CIP requirements will result in significant CIP investment and increased on-going operational costs as well as increased compliance risks. This will result in Generator Owners/Generator Operators not offering units for Blackstart service in the competitive ERCOT market. It would also likely result in Blackstart Resources not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart services. With fewer units being offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. Luminant recommends one of the following options for changing CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: 1) “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” This is the preferred option. Blackstart Resources with External Connectivity would still be in the Medium Impact category; however, those Blackstart Resources without External Connectivity would have less cyber risk and move to the Low Impact category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through the Electronic Access Point. Thus, many ERCOT Blackstart Resources would not fit in the Medium Impact category. 2) Include a Regional Variance for ERCOT in CIP-002-5 similar to option 1 described above. This would limit the variance only to ERCOT and not be a comprehensive application to the industry. Also Attachment 1, section 2.13, creates ambiguity regarding the type of control center to which the rating applies. Recommend capitalizing Control Center to clarifiy that this applies to centralized command centers rather than plant operation control rooms.
No
The timeframe for updating should be changed to 60 days to allow for entities to train their staff to ensure common understanding, validate the modifications including basis, obtain reviews and approvals of documentation changes, and coordinate changes with third party entities.
Yes
No
The VSL table should refer to BES Cyber Assets and BES Cyber Systems (not just BES Cyber Assets) as does Requirement R1 for consistency with terminologies used in R.1 & R.2.

Yes
Yes
Yes
Yes
No
The Requirement and Measure are inconsistent in that the Requirement states delegation can be documented “by position or name of the delegate”, but the Measure indicates that evidence includes a document that includes the name of the individual to whom an authority has been delegated. Recommend removal of reference to individual names as documentation to that level significantly increases the administrative burden associated with this Requirement. Additionally, it is currently unclear if every approval within CIP-002 and CIP-004 – COP-011, and its subsequent delegations, must be documented individually. Strongly recommend indicating that a global delegation is acceptable.
Yes
No
The VSLs for R5 and R6 are too severe. The VSLs for these two requirements should start at the lowest level and follow the 5%/10%/15% guidance since the integrity of the Cyber Asset/Cyber system is not compromised by this violation. This violation is for an administration non compliance and not a violation that has a direct impact on the security controls and integrity of the Cyber Asset. Also, the term “delegate” should be changed to “delegate(s)” throughout this standard and all other CIP standards where appropriate. Language should be added to the VSLs to allow for a procedure based Roles and Responsibilities approach, including delegations, that does not require documentation of each delegation e. The procedures would pre-define those positions and the evidence should be consistent with the procedure requirements. This will avoid a documentation nightmare for delegation by person or positions every time a Senior Manger is not available.
Yes
Yes
Yes
Yes
Yes
No
Change the term “delegate” to “delegate(s)”. The SDT should add language to R6 to allow for self-identified and corrected administrative and documentation findings during quarterly or annual assessments/reviews. These should not be counted towards automatic violation of the standard since the discrepancy or non-compliance was self-identified, corrected by the entity.
Yes
No
Change the term “delegate” to “delegate(s)”. The SDT should add language to R6 to allow for self-identified and corrected administrative and documentation findings during quarterly or annual assessments/reviews. These should not be counted towards automatic violation of the standard since the discrepancy or non-compliance was self-identified, corrected by the entity.

Yes
No
The statement “Note that a user ID is not considered an authentication factor.” Implies that user ID/password is not a method of authentication. Recommend clarifying as follows: “Note that the combination of a User ID and its association Password is considered as one authentication factor. A User ID alone is not considered an authentication factor.”
Yes
No
We recommend removing the word “egress” from the Measures of 1.2 for Medium Impact assets. The program established access controls which are designed to restrict access. This should be sufficient for the Medium Impact category. We recommend removing the word “complimentary” from 1.3 since the requirements requires two or more physical controls. The words “and complementary…” is misleading and can be construed as requiring additional physical controls. For R1 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances because there may be circumstances that require providing physical access control to individuals not on the authorized list.
No
For R2 overall, the SDT needs to include language that allows for deviations from the controls during CIP Exceptional Circumstances
Yes
Yes
Yes
No
It is not necessary to install Security Patches in all cases. A Security Patch when released should be assessed for BES Cyber Asset/System impact based on the configuration and external connectivity and other implemented security controls. Where remediation was deemed unnecessary, a documented justification with basis must be provided. It should be explicit in 2.2 that the plan could include not implementing the patch.
No
In Part 3.3, 30 days is not a reasonable time frame to assess, test, document, analyze, and implement a patch in a control system. We recommend 60 days as an appropriate time frame.
No
For R4.1 – the SDT should include “BES” just prior to “Cyber Security Incident” to correct the definition. Requirement 4.1.4 should be removed, as it is too broad and undefined. Recommend defining “Malicious Activity” as being one that has a direct adverse impact on the core functions of the BES Cyber Assets/Systems
No
In R5.1, it is not clear what is meant by “validate credentials”. We suggest the following language, “ Validate that users are authorized before granting electronic access to each BES Cyber System.”
No
The VSLs for R1 and R2 are too severe since there are other security controls that complement this control such as portable media control, physical access control, Training, etc. All these controls collective provide the necessary defense –in-depth based protection. We recommend a graduated approach starting with the Low VSL level. The way it is written, a failure to disable one port or the failure to install one patch or update in a timely manner would be a Severe VSL, while the actual potential impact to the BES is very limited.
Yes

No
We recommend changing the wording of R2.1 as follows, " When a Cyber Security Incident occurs, the incident response plans must be used (except in CIP Exceptional Circumstances) and include identification of any deviations from the plan during the incident or test.", because there may be circumstances that require deviating from the plan. Also, the words "and justifies" should be removed from the Measure for R2.1. In R2.2 the term "initially upon" should be changed to "prior to". If the standard is effective on January 1, 2015, it would be difficult to be in compliance if the initial test of the plan is not until January 1.
No
In R3.5, we recommend changing the word "Communicate" to "Distribute" and make the corresponding changes to the measures for better clarity.
Yes
No
R1.5 needs to be clarified that the retention period for raw event logs is no more than 90 days.
No
CIP-008-5 and CIP-009-5 appear to have similar type requirements, but the language is inconsistent between the standards. Where applicable, similar type language should be utilized in these two standards. Recovery Planning is a component of the Incident Response Planning for recovery, thus SDT must ensure consistency and seamless transition between these two (2) standards.
No
Change "initially" to "Prior to" in 3.1 . Also, CIP-008-5 and CIP-009-5 appear to have similar type requirements, but the language is inconsistent between the standards. Where applicable, similar type language should be utilized in these two standards. R3.5 should use the word Distribute, instead of Communicate.
Yes
No
We recommend the following changes to R1 and its subparts: 1) Add the term "intentionally installed" to 1.1.4 for better clarity since scripts are intentionally installed based on client requests 2) Language in the Requirement 1.2 section needs to be corrected as follows: "Document changes to the BES Cyber System that deviate from the existing baseline configuration, including the authorization by the CIP Senior Manager or delegate(s)." for better readability 3) 1.4.2 language should read – "Following the change verify that the required cyber security controls are in place, and the BES Cyber System is available, and" for better readability 4) 1.5 Language should read - "Prior to implementing any change in the production environment, except in CIP Exceptional Circumstances, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System in enough detail to verify and validate the integrity of the required cyber security controls." This change is necessary since there can be exceptional circumstances that may require implementing changes in the production environment without going first thru a test environment. In addition, the revised write-up provides clarity on what needs to be done.
No
We recommend the language in R2.1 should be changed to read, "…(as defined per CIP-010 R1, 1.1, excluding physical location)."because physical location is not a monitored logical parameter within a Cyber Asset/system.
No
We recommend changing the word "Initially" to "Prior to" in 3.1 and 3.2 for purposes of clarity. In section 3.1, the terms "security controls" and "controls" should both be changed to "required security controls" for clarity. We recommend changing the language in section 3.4 to be consistent with the language in CIP-011 section 1.3, as the language in CIP-011 is more clear.
Yes

No
In section 1.3, we recommend changing “Initially upon” to “Prior to” for purposes of clarity.
We recommend changing the language in section 2.2 to read “..shall destroy the media or take action…” The current sentence is lacking clarity and specificity.
No
The VSL for R2 in the high category should be rewritten to focus on the failure to purge the media or destroy the media prior to disposal, not a failure to precisely follow the prescribed process as the failure to destroy or purge the data is the core of the security risk. We suggest the following language, “The Responsible Entity has documented or implemented one or more media disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the media, but the Responsible Entity failed to purge or destroy the media prior to disposal.”
No
The minimum implementation time frame of 18 months is not sufficient. The timeframe for implementation should be extended in order to allow time for assessment, planning, budgeting and approval thereof, physical or logical modifications, development of new programs and procedures, including related training and full implementation of the requirements. With the additional requirements that include some activities at all generating facilities, there may be limited resources (both internal to companies and external third party resources) available to implement the requirements in this short duration. We recommend a minimum implementation period for CIP-002-5 of 12 months, and implementation for the remaining version 5 CIP standards for High and Medium Impact BES Cyber Systems at 24 months. Low Impact systems would be compliant within 36 months.
Group
City of Garland
Ronnie Hoeinghaus
Yes
“Cyber Asset” – should not include any portable memory devices such as USB memory devices, CDs, etc. “BES Cyber Security Incident” should read as follows: A malicious act that: • Compromises a BES Cyber System or BES Cyber Asset, or • Disrupts the operation of a BES Cyber System or BES Cyber Asset, or • Results in unauthorized physical access into a Defined Physical Boundary. “BES Cyber System Information” should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a “Schweitzer” relay (or even an “SEL 2030”), the information should not require special treatment. “BES Reliability Operating Services” should be clarified so that the CIP Auditor does not feel licensed or obligated to perform a “693” audit – there are many opportunities as written for the CIP Auditor to “branch out” into areas that have nothing to do with Cyber Security. There are ample 693 standards and 693 auditors for those standards.
Yes
The addition of a “Low Impact” rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit.
No
The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards

themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards.
No
Consider rewording so that the initial identification and categorization required by R1 is no later than the effective date and updated once each calendar year.
No
This should not apply to visitors – should read “shall make individuals who have authorized unescorted access…”
No
Change 30 days to 90 days
No
Need lower and moderate VSLs
No
Table Part 1.1 - Strike the “Security Awareness Program” from Requirement and Measures. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
No
Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary. Recommendation is to strike item 2.10. Providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. Strike R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training.
No
Table Part 4.2 - too prescriptive - residency and educational history is not revelant to a criminal history - current 7 year criminal check is sufficient - if language remains, add language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
Table Part 5.2 Add language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required). For clarity, recommend changing 5.1 from "authorized electronic or unescorted physical" to "authorized electronic or authorized unescorted physical"
No
The CIP Senior Manager should not be the person that authorizes access in Table Part 6.1, 6.2, 6.3 –

this should be up to the Responsible Entity's business process owner
No
Table Part 7.1 It is impossible to always revoke access upon the termination date or resignations in the cases where OEMs are involved. We cannot enforce this in 3rd party companies. Additionally, it is impossible to change locking mechanisms in remote substations that are spread across large geographical regions. Table Part 7.2 While this may work in a control center, it is not practical or reasonable in transmission substation settings, particularly for devices that are not remotely connected. Please Note: Promoting someone or transferring someone does not make that person a security risk and should not be treated as such.
No
need lower and moderate VSLs
No
Table Part 1.5 IDS should not be required - a firewall should be sufficient. Should clarify requirements for low, medium, high impact BES Cyber Systems
No
Table 2 Part 2.3 – remove this statement from measures "Note that a UserID is not considered an authentication factor." "Associated Protected Assets" needs to be defined
No
Should have lower and moderate VSLS – not just higher & severe
No
Table 1 – Strike "egress" from measures – egress is not stated in the requirement Table 1 Part 1.6 - vague and needs to be clarified
No
Table 2 Part 2..2 – logs should be kept for 1 year – for a 6 year audit cycle, 6 years is too long to be required to keep logs – requirement should clearly state that the logs may be destroyed after 1 year so that an auditor will not ask for 1 year's worth of logs on a date 6 years ago to prove that the entity was compliant with 1 year of logs on that date
No
Table 1 Part 1.1 – Need provision for TFE Table 1 Part 1.1 indicates that the requirement is applicable to "systems", but measure focuses on "assets". Need a system approach if this requirement is intended to be applied at a broader level. The term "BES Cyber Asset" should be removed from measure if the requirement can be applied to "system". Table 1 Part 1.2 – Need provision for TFE
No
Table 2 Part 2.1 – remove comma after the word "patches," - the comma in the sentence requires that all software patches be included whether they are security related or not. Additionally, it is not practical to include firmware as very few vendors post when firmware updates become available Table 2 Part 2.2 – requires a "remediation plan" – if the patch is applied, there is no reason to require a "remediation plan" – should be reworded or struck
No
Table 3 Part 3.3 – needs to define when the 30 days start – when the EMS vendor says it can be applied or when the virus definition manufacturer says it is available. Additionally, needs provision for TFE in case the virus definition kills the application. Table 3 Part 3.4 – measure is too prescriptive for the requirement Table 3 Part 3.5 – should not apply to USB memory devices – if it does, requirement should be struck as this would be extremely burdensome.
No
Table 4 Part 4.1 – Although this may be practical for PCs, many substation devices do not have any logging capability at all – needs provision for TFE Table 4 Part 4.1.1 – Electronic Access Points should be addressed under CIP-005 Table 4 Part 4.1.4 – use of the word "potential" is vague and is not auditable Table 4 Part 4.3 – strike "before the end of the next calendar day" – end sentence with "failures" Table 4 Part 4.5 – strike 4.5 completely – it is a duplication of 4.2 and 4.3
No

Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.]
No
should have lower and moderate VSLs
No
No
Table 2.1 – strike deviation language from requirement – “lessons learned” exercise after the incident will be sufficient. Additionally, allowances need to be made in the requirement for the entity to deviate from “the plan” if circumstances call for a deviation without being penalized by the auditors. “Emergencies” or “Disasters” exist because something in everyday business life did not go as planned – requirements should allow for responses to be flexible to handle the unforeseen
No
Table 3 Part 3.1 – Consider rewording so that the initial incident response plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
should have lower and moderate VSLs
No
Should state that ‘reconstitution of site is not required’ Table 1 Part 1.5 – should be struck completely – preservation of forensic evidence should never take priority over the restoration of the BES
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 2 Part 2.2 – remove the word “any” from the requirement Table 2 Part 2.3 – should be struck as it is a duplication of 2.1 – problems with 2.3 as written are what constitutes a full operational test of the plan – is it sufficient to reload one server or one workstation or replace a card in a computer? Additionally, if there are 4 scenarios written in the plan, do you have to do an operational test of each scenario?
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
should have lower and moderate VSLs
No
Table 1 Part 1.1.4 – strike completely - entirely too prescriptive – base line should not go beyond information from what a standard vulnerability scan application can provide Table 1 Part 1.2 – strike CIP Senior Manager – this should be a business function covered by the change management process Table 1 Part 1.4.2 – strike “availability” – “availability” is a business function, not a security function – question – if you make 40 changes in a year and “availability” goes down 1% (if you can determine that), how do you verify Table 1 Part 1.5 – strike completely – it is a duplication of 1.4 regardless of whether the change involves a control center or not
No
Table 2 Part 2.1 – strike completely – CIP-007 requirements are sufficient
No
Consider rewording so that the implementation is no later than the effective date. Table 3 Part 3.2 – strike completely – 3.1 should be sufficient
No
should have lower and moderate VSLs

No
Consider rewording so that the implementation is no later than the effective date
No
should have lower and moderate VSLs
Yes
Group
Corporate Compliance
Summer C. Esquerre
Yes
a. BES Cyber Asset – The sentence, “This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services” makes the definition more confusing. This is a suggestion to improve the definition: BES Cyber Asset - A Cyber Asset that is currently in operation if rendered unavailable, degraded, or misused would impact one or more BES Reliability Operating Services within 15 minutes. The 15-minute timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. b. The effective dates says the following: "18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." This seems to state that CIP 002 - 009 Version 4 is never going to be implemented, this is confusing. It would be better to state: " 18 Months Minimum – The Version 5 CIP Cyber Security Standards (including CIP 010-1 and 011-1) shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. In the event CIP-002-4 through CIP-009-4 do not become effective, CIP-002-3 through CIP-009-3 will remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." c. In the definition for a BES Cyber Asset it states: "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services." The term "adversely impact" needs to be further defined, this seems to basically result in the same lack of clarity that resulted in the need to have versions 4 and 5 to ensure assets where identified as critical.
Yes
Attachment 1 does not indicate if these rules apply to non-dispatchable units (i.e. wind, solar, etc.), this should be defined. For Items 1.4 – Control Centers, 2.1 – Generation greater than 1500 MW, 2.3 – Generators designated by the Planning Coordinator and 2.4 Blackstart units, the definition of BES Cyber System that can impact BES Reliability Operating Services would force the inclusion of RTU’s, Governors, Power System Stabilizers and Protective Relaying. Item 2.1 - Need to better define what the phrase “adversely impact” means, i.e. if you have to lose all 1500 MW as defined under item 2.1 to result in an adverse impact Item 2.11 addresses Special Protection Systems (SPS), need to define if this includes SPSs which are associated with Generation sites. Item 2.12 - Under Frequency Load Shedding of 300 MW or more required by the regional load shedding program. Currently NPCC and RFC are seeking approval for their UFLS programs which would require generators who trip above the regional UFLS curve to independently arrange with the local DP for the equivalent amount of UFLS MW’s. While we have not yet evaluated our plants in NPCC and RFC, if they cannot meet the proposed UFLS curves, they would be pushed up into a Medium Impact Rating. Item 2.2 the former version had BES in front of Reactive Resource. The BES should be restored to make clear that this is transmission level as stated in the application notes. Item 2.3 uses the phrase “long-term planning horizon” which is later defined as one-year or longer, it would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. Item 2.3 uses the phrase “long-term

planning horizon" which is later defined as one-year or longer, it would be better if the time horizon was defined with a number of years, otherwise it would be hard to have it audited. Item 3 does not provide a minimum site MWs or interconnection voltage, would recommend nameplate rating greater than 20 MVA or gross plant/facility aggregate nameplate rating greater than 75 MVA including the generator terminals through the high side of the step-up transformer(s) connected at a voltage of 100 kV or above. This is in line with the Bulk Electric System (BES) definition developed under NERC Project 2010-17 Definition of the Bulk Electric System. Overall, the new rules are ripe for confusion. If the need was to ensure that the definition for what assets fell under the requirements, changing the definitions on what Cyber Assets are to be protected has no relation to this goal. It would seem to make more sense to define the Physical assets in the Bulk Electrical System (BES) which have potential to negatively impact the BES, then define how to protect Cyber Assets that are potentially open to external access, protecting them from internal assault through physical and logical access controls. The proposed definitions should return to Critical Assets and the Critical Cyber Assets at these sites would then be defined as: Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1; the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. Critical Cyber Assets are qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.

No

a. CIP-002-5 R1.1 which states "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category" implies that the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems is constantly being performed by the Responsible Entity – as stated in the rationale for R1 "…configuration of the BES is subject to changes due to new demands and requirements for Bulk Power and to environmental changes and operational events. When changes to the BES are planned, the effect of these changes on the set of identified and categorized BES Cyber Assets and BES Cyber Systems must be analyzed to ensure that the adequate level of protection is still applied to them." To ensure that every configuration change of the BES is fully accounted for with regards to the identification or categorization of the BES Cyber Assets or BES Cyber Systems, CIP-002-5 R1.1 as drafted requires that the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems is required to be performed with 30 calendar days of the configuration change of the BES. This is burdensome as every configuration change of the BES needs to be tracked, dated, and evidence of the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems be documented. An alternative method should be considered – for example, when planning studies reveal that the configuration change of the BES is material, they it would trigger the process to identify or categorization of the BES Cyber Assets or BES Cyber Systems. This will then start the 30 day window as stated in CIP-002-5 R1.1. b. Need to add discrete identification of Low Impact BES Cyber Assets or BES Cyber Systems, you are going to have to review each based upon Attachment 1 criteria; this will be the way to demonstrate compliance in a manner that is auditable. General Comment: In the background section of CIP-002 (specifically CIP-002 page 7), there is reference to being able to group Cyber Assets. The example provided refers to applying requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets. So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply. It is unclear what this means exactly and what the overall benefit. Overall Comment related to the Background and Application Guidelines included in each of the Standards, it is unclear what the applicability is related to these sections. From a compliance perspective will Registered Entities will potentially be penalized for not following the sections from the EROs since they are not included within the Standard and do not serve as the Standard's requirements, but is additional material for the EROs to use to determine compliance. Recommend either including specific language from the guidelines as applicable to address FERC Order 706 and cyber security or removing from future versions of the draft standards.

No

a. To add clarity to CIP-002-5 R2, any change in the identification or categorization of the BES Cyber

Assets or BES Cyber Systems in between the “once each calendar year” review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval. b. It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders
No
FPL disagrees with the fundamental requirement to perform a review upon a change to the BES and therefore disagrees with the associated VSL associated with this requirement. See response to question 3
No
To add clarity to CIP-003-5 R1, CIP Senior Manager delegate that has the ability to approve Cyber Security Policy required in CIP-003-5 R3 shall also be identified by name. This will ensure that there is clear delegation of authority and ownership for the CIP program within an organization.
No
May need to look at the topics stated as they seem to be redundant – need to look at the overall structure of the CIP V5 standards
No
a. The CIP Senior Manager delegate may also review each of its cyber security policies and provide the approval. This is a suggestion to improve CIP-003-5 R3: Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager or delegate, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. Also, any change in the Responsible Entity’s cyber security policies in between the “once each calendar year” review/approval of the CIP Senior Manager or delegate does not require the CIP Senior Manager or delegate approval. b.It would be easier to ensure compliance if the requirement to review the list on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.
Yes
No
a. The CIP Senior Manager should also be able to delegate the authority for any approvals and authorizations required in the CIP standards including the approval of the Cyber Security Policy required in CIP-003-5 R3. This is a matter of efficiency and does not detract from the intent of “clear lines of authority and ownership for security matters.” b. This will be difficult to manage in a large organization and provides no value. Just have the Senior Manager appoint any delegates for his role, then identify a Compliance Manager who will sign the appropriate documentation in their area.
Yes
Yes
Yes
No
a. In Part 2.1 under “Requirements” change “Define the roles that require training” to “ dentify each role and specify training required for each role.” The statement “Define the roles that require training” implies that some roles do not require training. b. The “Applicability” stated in CIP-004-5 Table R2 – Cyber Security Training Program and CIP-004-5 Table R3 - Cyber Security Training are inconsistent. CIP-004-5 Table R2 – Cyber Security Training Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R3 - Cyber Security Training has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent.
No

a. The “Applicability” stated in CIP-004-5 Table R2 – Cyber Security Training Program and CIP-004-5 Table R3 - Cyber Security Training are inconsistent. CIP-004-5 Table R2 – Cyber Security Training Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R3 - Cyber Security Training has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include training on cyber security as part of the requirements to have authorized access. b. In order to add clarity to the role-based nature of the cyber security training program, suggest rewording CIP-004-5 R3 to: Each Responsible Entity shall implement its documented role-based cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training. This is to emphasize that the training is geared towards the individual’s role when the individual requires authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program. 3.2 states Cyber Security Training must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders. c. If the individual’s role is changed from one role to another as defined in CIP-004-5 R2 Part 2.1, the Responsible Entity needs to show evidence that the training was completed within 30 days of the change of role. This is not currently in CIP-004-5 R3 and needs to be explicitly required to ensure proper role-based cyber security training is provided to individuals requiring authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program. d. If the role definition as documented in CIP-004-5 R2 Part 2.1 changed (i. e., a defined role has its specific training requirement changed), for every individual whose role definition changed the Responsible Entity needs to show evidence that the training was completed within 30 days of the change of role definition. This is not currently in CIP-004-5 R3 and needs to be explicitly required to ensure proper role-based cyber security training is provided to individuals requiring authorized electronic or unescorted physical access to each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.
No
a. The “Applicability” stated in CIP-004-5 Table R4 – Personnel Risk Assessment Program and CIP-004-5 Table R5 – Personnel Risk Assessment are inconsistent. CIP-004-5 Table R4 – Personnel Risk Assessment Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R5 – Personnel Risk Assessment has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. b. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include a Personal Risk Assessment (PRA) as part of the requirements to have authorized access.
No
a. The “Applicability” stated in CIP-004-5 Table R4 – Personnel Risk Assessment Program and CIP-004-5 Table R5 – Personnel Risk Assessment are inconsistent. CIP-004-5 Table R4 – Personnel Risk Assessment Program has High Impact BES Cyber Systems and Medium Impact BES Cyber Systems listed whereas CIP-004-5 Table R5 – Personnel Risk Assessment has High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets listed. CIP-004-5 R2 and CIP-004-5 R3 need to be consistent. b. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements

for authorized access; it would make sense to include a Personal Risk Assessment (PRA) as part of the requirements to have authorized access
No
a. The requirement states that it is only valid, including in its parts, for Medium and High Impact BES Cyber Systems, as well as Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include them in the Access Management Program as part of the requirements to have authorized access. b. In Part 6.2 under "Requirements" the wording should be changed from "The CIP Senior Manager or delegate shall authorize unescorted physical access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions." to "The CIP Senior Manager or delegate shall authorize unescorted physical access, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions." The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 6.2 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). c. In Part 6.4 under "Requirements" the wording should be changed from "Verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access to BES Cyber Systems were authorized for such access." to "The CIP Senior Manager or delegate shall verify at least once each calendar quarter that individuals provisioned for unescorted physical or electronic access were authorized for such access." The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 6.4 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). Also specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the quarterly review. d. In Part 6.5 under "Requirements" the wording should be changed from "Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions." to "The CIP Senior Manager or delegate shall verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions." Specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the "once each calendar year" review. e. In Part 6.6 under "Requirements" the wording should be changed from "Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions." to "The CIP Senior Manager or delegate shall verify at least once per calendar year, but not to exceed 15 calendar months between verifications, of access privileges to BES Cyber System Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions." Specifying the CIP Senior Manager or delegate removes the vagueness of who is required to review and approve the "once each calendar year" review. f. This is the first requirement in CIP-004-5 R6 that mentions access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) – access to BES Cyber System Information did not require any role-based cyber security training program (per CIP-004-5 R2 and CIP-004-5 R3) nor one or more documented personnel risk assessment programs (per CIP-004-5 R4 and CIP-004-5 R5) – is this the intent of CIP-004-5 R6? g. To clarify for Part 6.1, CIP Senior Manager delegates allowed to authorize electronic access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.1) need not be identified by name. CIP Senior Manager delegates allowed to authorize electronic access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring

Systems, and Associated Protected Cyber Assets (as stated in Part 6.1) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. h. To clarify for Part 6.2, CIP Senior Manager delegates allowed to authorize unescorted physical access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.2) need not be identified by name. CIP Senior Manager delegates allowed to authorize unescorted physical access to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.2) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. i. To clarify for Part 6.3, CIP Senior Manager delegates allowed to authorize access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) need not be identified by name. CIP Senior Manager delegates allowed to authorize access to BES Cyber System Information to High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets (as stated in Part 6.3) need only be identified by their position and necessary description of their authority to grant such access as part of the Responsible Entity's BES Cyber Systems access provisioning program. j. 6.5 states verification that all accounts/account groups or role categories and their specific associated privileges are correct and the minimum necessary for performing assigned work functions must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders k. 6.6 states verification of access privileges to BES Cyber Systems Information to confirm that access privileges are correct and the minimum necessary for performing assigned work functions must be done at least once every calendar year, but not to exceed 15 calendar months. It would be easier to ensure compliance if the requirement to complete the training on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders.
No
a. The requirement states that it is only valid, including in its parts, for Medium and High Impact BES Cyber Systems, as well as Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets. CIP 005-5 R1.1 includes Low Impact BES Cyber Systems with External Routable Connectivity and requires restriction of unauthorized electronic access. CIP 006-5 includes Low Impact BES Cyber Systems requires that you need to restrict physical access. These two requirements mean you have to define who can have access and the requirements for authorized access; it would make sense to include them in the Access Management Program as part of the requirements to have authorized access. b. By not specifying the amount of time to revoke access in Part 7.1 and relying on the Responsible Entity's judgment and interpretation of what constitutes the time element or meaning of the phrase "at the time of the resignation or termination" would result in various interpretations by auditors during a CIP spot check. Does this mean good faith effort by the Responsible Entity? If the intent is for "immediate revocation", we suggest clarifying Part 7.1 to state "For resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access at the time of the resignation or termination during the same calendar day of the individual's resignation or termination. In extenuating circumstances that the revocation is not possible during the same calendar day, document the extenuating circumstances and revoke access as soon as possible. The documentation of the extenuating circumstances shall be signed by the CIP Senior Manager or delegate." By specifying the "the same calendar day", it will clarify the expectation that the revocation of the individual's unescorted physical access and Interactive Remote Access is performed immediately (and at most, within same calendar day) as recorded by the Responsible Entity. A provision to allow for documentation for "extenuating circumstances" is also included but would require a signature from the CIP Senior Manager or delegate; an example of an extenuating circumstance is that the time of revocation is close to the end of the calendar day (e. g., 11:55 pm) and revocation could not be completed by the same calendar day – this instance could be deemed as a valid extenuating circumstance. Please take note that the proposed rewording removed the phrase "to BES Cyber

Systems" since it is consistent with the "Applicability" column. The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 7.1 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets) c. Since the individual may change roles or that roles may be modified but may still require some form of electronic access or unescorted physical access, we suggest rewording of Part 7.2 to "For reassignments, transfers, role changes, or role modifications, revoke the individual's unneeded electronic and/or unneeded physical access by the end of the next calendar day. Please take note that the proposed rewording removed the phrase "to BES Cyber Systems" since it is consistent with the "Applicability" column. The phrase "to BES Cyber Systems" is inconsistent the list of systems/assets listed in Part 7.2 under "Applicability" (High Impact BES Cyber Systems, Medium Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets). The "and/or" for unneeded electronic access and unneeded electronic access covers all possibilities/combinations of the individual's current access. d. There should also be a table entry (i. e., an additional part in CIP-004-5 R7 in the CIP-004-5 Table R7 – Access Revocation table) "For reassignments, transfers, role changes, or role modifications, revoke the individual's unneeded access to BES Cyber System Information by the end of the next calendar day." An individual's access to BES Cyber System Information due to reassignments, transfers, role changes, or role modifications may need to be modified.
Yes
No
a. The requirement R1.1 states "Define technical or procedural controls to restrict unauthorized electronic access," yet the measures for the requirement states "Evidence may include, but is not limited to, documented technical and procedural controls that exist and have been implemented." These two are mutually exclusive; the requirement being "technical or procedural controls" yet the measure indicates you have to have "technical and procedural controls." Recommend both say "technical or procedural controls." b. Part 1.1 We recommend rewording the requirement to better align with Applicability and Change in Rationale: Define technical or procedural controls to restrict unauthorized interactive remote access c. Part 1.2 (Page 11) Applies to Associated Physical Access Control Systems – Requirement says "control and secure all routable and dial up connectivity through the use of identified EAPs" – Does this mean we will need to consider the whitefloor firewalls as an EAP? Although that is not the definition of an EAP, how will this work with our current architecture (i.e., Picture Perfect being a PAC sitting on the whitefloor)? d. R1.3 Are comments and explanations besides the rules sufficient to satisfy the requirement, also can there be a definition of what "explicit criteria" means. e. Part 1.4 Definition of interactive / non-interactive access is not clear. Definition should be added to the Definition of Terms. f. Requirement R1.5 states "A documented method for detecting malicious communications at each EAP" yet the Change Rationale states "The Order makes clear this is not simple redundancy of firewalls, thus the drafting team has decided to add the security measure of malicious traffic inspection (intrusion detection systems / intrusion protection systems) a requirement for these ESPs." If that is the case, why not just have the requirement state so for clarity. g. R1.5: The wording is too vague, measures and rational don't match, suggest breaking down the requirement to specify what needs to be done for detecting malicious communication, i.e using AV, IDS, etc. h. Part 1.5 does not define the term "malicious". A definition is needed to avoid interpretation.
a. Part 1.2 (Page 11) Applies to Associated Physical Access Control Systems – Requirement says "control and secure all routable and dial up connectivity through the use of identified EAPs" – Does this mean we will need to consider the whitefloor firewalls as an EAP? Although that is not the definition of an EAP, how will this work with our current architecture (i.e., Picture Perfect being a PAC sitting on the whitefloor)? b. R1.3 Are comments and explanations besides the rules sufficient to satisfy the requirement, also can there be a definition of what "explicit criteria" means. c. Requirement R2.1 states "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." It would seem a firewall or router meets this requirement, but we do not believe that is what was discussed in "Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3" document. Recommend that requirement state directly that the Electronic Access Point (EAP) does not meet this requirement. d. Requirement R2.2 states "Require encryption for all Interactive Remote Access

sessions to protect the confidentiality and integrity of each Interactive Remote Access session." Does that mean encryption is required only between the Intermediate Device and the EAP to the BES Cyber System or Protected Cyber Assets, or does it include the connection between the Cyber Asset being used to conduct remote access and the Intermediate Device? Recommend that this requirement be clarified as to the above and recommend it does not include the connection between the Remote Cyber Access and the Intermediate Device. e. Part 2.2 – clarification is needed where encryption is required. Is encryption needed from the intermediate asset to the BES Cyber Systems or Protected Cyber assets? Since, in many applications, it may not be technically feasible to implement encryption between intermediate device and BES Cyber Asset, we propose rewording requirement to: f. Require encryption between remote Cyber Asset and intermediate device for all Interactive Remote Access sessions to protect the confidentiality and integrity of each Interactive Remote Access session. g. Part 2.3 – multi factor authentication is used interchangeably with two-factor, should standardize on one. Term not defined in the Definition of Terms.
No
Suggestion to propose a fine monetary estimation for each VSL and establish a guideline regarding the how fines are determined, as it correlates to the number of devices with the PV, the exposure, the mitigations, and risk factor to the BES.
No
a. Requirement R1.1 requirement states "Define operational or procedural controls to restrict physical access" yet the measures for the requirement states "Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented." Recommend this be clarified, using "operational or procedural controls." b. R1.1 not specific enough in regards to what kind of physical controls need to be limited to restrict access. CIP-006-5 R1.1 Entity based Operational or procedural controls to restrict physical access – To allow for programmatic protection controls as a baseline for Low Impact BES Cyber Assets and Physical Access Control Systems. This does not require detailed lists of individuals with access. c. Part 1.1, 1.2 – We recommend that Associated Physical Access Control Systems are moved from requirement 1.1 to 1.2 in order to better align with the remaining CIP standards; for instance, the access management requirements in CIP-004. d. Requirement R1.3 states "Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible." Clarify if the statement means that a Technical Feasibility Exception (TFE) can be filed for this (give scenarios in the guidance where it would apply). e. Part 1.6 - Does log entry only require date or is time also required. If time is required, then it should be added. Since the concept of a “visit” is used for visitors, is the same concept used for the personnel with access? (see Part 2.2) f. The requirement does not state if you must protect cabling between Defined Physical Boundaries, please clarify. g. Deletion of identification of physical access points h. “Appropriate” use of access controls is part of CIP-004-5 2.3 i. Defense in depth needs to be moved out of the guidance section and into the requirement j. Definition of an access point needs to be added to the requirement: “Typically any opening greater than 96 square inches with one side greater than six inches in length would be considered an access point into the Defined Physical Boundary. Protective measures such as bars, wire mesh or other permanently installed metal barrier could be used to reduce the opening size as long as it is leaves no opening greater 96 square inches or no more than six inches on its shortest side.”
No
a. Requirements R2.1 and R2.2 do not mention Associated Physical Access Control Systems under Applicability, does this mean that they cannot be accessed by visitors or that they can. Recommend that Associated Physical Access Control Systems be included under Applicability section for both. b. Part 2.1 continuous escort is not defined. Requirements of a continuous escort should be clearly stated.
No
Part 3.2 (Page 18) – If the intention is to have a process underneath this to mitigate the risks when outages occur, recommend explicitly stating this in the requirement. There is further guidance in the end of the CIP but this should be included and a measure developed.
Yes
No

a. R1.2 states under Applicability that it is only applicable to "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems at Control Centers." Based on what you are trying to accomplish, it would make sense to include "Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, as well as any "Medium Impact BES Cyber Systems." b. R1.2: Applicability – Change "Medium Impact BES Cyber Systems at Control Centers" to "Medium Impact BES Cyber Systems" c. The requirement does not address services that are not required for operation, this will potentially allow a major vulnerability, recommend services be added to R1.1 d. Table R1 – Ports and Services e. R1.1 – Requirements – Content Change i. Original Content - Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. ii. Proposed Change – Enable only logical accessible ports needed for normal and emergency operation, including port ranges where required. f. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC requests within order 706 without adding security benefits. g. We see this as being applicable and valid for logical ports and services however disabling connectivity to all physical ports on devices such as servers within the applicable compliance areas could be cost prohibitive. Additionally this is mitigated by physical security controls preventing access to the physical devices. h. CIP-007-5 Table R1 – Ports and Services Part 1.1 Measures: Required evidence includes "screen shots" showing accessible ports. Screen shots are only one method to show evidence and requirement should not be so prescriptive. Evidence could be a listing or a report created from a database of ports. Some systems are not capable of capturing screen shots. i. CIP-007-5 Table R1 – Ports and Services Part 1.2 Measures: Same comment as above.

No

a. Table R2 – Security Patch Management b. R2.1: Requirements – Content Change i.Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. ii.Proposed Change - Identify a source or sources that are monitored for the release of security related patches, or security related updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. c. R2.2: Requirements – Content Change i.Original Content – Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii.Proposed Change – Identify applicable security-related patches or security related updates from the identified source that addresses the vulnerabilities within a defined timeframe within 30 days of release and create a remediation plan, or revise an existing remediation plan, within 60 days of release, unless the patch has been installed within 60 days of release. d. Part 2.3 (Page 14) – How will we prove compliance with this in the event that after the assessment, we decide that a patch will not be implemented due to the existence of mitigating controls? There will not be a remediation plan if the mitigating controls are already in existence and there will be no implementation logs. e. Requirement 2.3 states "A process for remediation, including any exceptions for CIP Exceptional Circumstances" as a requirement. Recommend that the term CIP Exceptional Circumstances be defined in the requirement. f. Part 2.3 (Page 15) – In the change rationale, is this implying that we now have to assess and implement within 30 days of release date? What is the beginning point for this 30 day window g. Throughout CIP-007-5 Table R2 – Security Patch Management Part 2.1 and 2.2: FPL does not agree with phrase "hotfixes and/or updates. The intent is to monitor for security vulnerabilities and this implies that CIP-007-5 R2 must be applied for software fixes and enhancements. Hotfixes and/or updates should only apply to this standard when hotfixes and/or updates contain security patches. h. CIP-007-5 Table R2 – Security Patch Management Part 2.3 does not have a timeframe associated with the requirement, yet the "rationale" states that a 30 day window has been given to complete the documentation. We recommend modifying the requirement to read: i. A process for remediation, including any exceptions for CIP Exceptional Circumstances shall be documented within 30 calendar days from the actual implementation

No

a. CIP-007-5 Table R3 – Malicious Code Prevention Part 3.3: FPL does not agree with requirement to update signatures within 30 days of availability. This is not practical if the entity has a process to test the signatures before implementing. Suggest making the requirement consistent to implementing security patches b. Requirement R3.3 states "Update malicious code protections within 30 calendar

days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." Recommend that you add the following statement to make consistent with Requirement CIP 007-5 R2.1: "Identify a source or sources that are monitored for the release of signature or pattern update availability (where the malicious code protections use signatures or patterns). c. Since some malware "engine or application" updates require rebooting, which is not compatible with BES Cyber System reliable operation, recommend you add two requirements, consistent with CIP 007-5 R2.2 and R2.3: "Identify applicable malware engine or application updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe" and "A process for remediation, including any exceptions for CIP Exceptional Circumstances." d. R3 – Malicious Code Prevention e. R3.4 Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. f. R3.5 Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and they do not appear to be Transient Cyber Asset related. g. Requirements – Append “to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets” to the end of the requirement. h. Measures – Content Change i. Original Text - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii.Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. i. R3.2: The measures for R3.2 only ask for configurations or a response, not the actual disarming or removal of identified malicious code. As such, these measures seem incomplete and the expectation is that an auditor would request to see evidence of malicious code disarmed or removed. Please include evidence of malicious code disarming or removal in the measures. j. Requirement 3.5 seems incomplete. Log each Transient Cyber Asset connection to what? The measure is clear, however, the requirement is not specific to what connections need to be logged.

No

a. 4.1 Requirements – Content Change i. Original Text – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: ii. 4.1.1. Any detected failed access attempts at Electronic Access Points iii.4.1.2. Any detected successful and failed login attempts iv. 4.1.3. Any detected malware v. 4.1.4. Any detected potential malicious activity. vi. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: vii. 4.1.1. Any detected failed access attempts at Electronic Access Points viii. 4.1.2. Any detected successful and failed login attempts ix. 4.1.3. Any detected malware x. 4.1.4. Any detected potential malicious activity. xi. ADD: Devices that cannot log a particular event do not require a TFE to be generated. b. 4.2: Applicability – Proposed deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. c. R4.1 and 4.2: The measures should include actual system generated logs or alerts if auditors will request this information in an audit. d. R4.5: does not give guidance for a sample size. Please give guidance on what an acceptable sample size would be to meet compliance. e. Part 4.5 (Page 24) – Can we suggest that this is applicable only in cases where automated alerting is NOT available f. CIP-007-5 Table R4 – Security Event Monitoring i.Part 4.1: Requirement does not clearly reflect the Change Description and Justification: This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term “system events related to cyber security” from informal comments received on CIP-011. Changes made here clarify this term by allowing entities to first define these security events. ii.We recommend rewording the requirement to include the word “define,” and better align with previous language in CIP-007 R3: iii. Define log generated events for the identification of, and after-the-fact investigations of, Cyber Security Incidents, as a minimum, each of the following types of events, even if such are null: 1. 4.1.1. Any detected failed access attempts at Electronic Access Points 2. 4.1.2. Any detected successful and failed login attempts 3. 4.1.3. Any detected "malicious code" 4. 4.1.4 Any detected "malicious activity" g. Since, according to the Guidelines and Technical Basis, “It is not the intent that if a device cannot log a particular event that TFE must be generated,” we recommend revising the Measure section to provide this clarification by revising its language to include: h. Evidence may include, but is not limited to, a paper or system generated listing of event classes for which the BES Cyber System is configured to generate logs. This listing must include the required event types "even

if such log generated event capabilities are not technically feasible" i. Part 4.2: We recommend rewording the requirement to align with implied requirement to perform and document an analysis to determine which events constitute a real-time alert described in Measures and Change Description and Justification sections: i. 4.2 Document alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. 4.2.1 Implement such real-time alerts j. Part 4.3: This is a tremendous undertaking to be able to monitor every cyber asset for logging failures within 1 day. It would even be a technical challenge to automate the detection. k. Part 4.3: The documentation of failures is also implied within requirement and Measures. We recommend revising such requirements to clearly outline this requirement, for example: l. 4.3 Detect and activate a response to event logging failures before the end of the next calendar day. i.4.3.1 Document event logging failures within 30 calendar days

No

a. R5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. b. R5.2: is not feasible for large Registered Entities or entities where the CIP Senior Manager is a company executive. c. R5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. d. R5.4 - How do you demonstrate 'unique' and does that introduce potential compliance concerns? e. Requirement R5.4 states "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required." State if a TFE can be submitted for this requirement if it is not technically feasible. f. R5.4: how is compliance achieved / demonstrated when it is technically feasible to change a default password or the default password is blank but the vendor does not recommend changing the password due to system instability? g. R5.5- Add language to 5.5.3 to cover instances where accounts may not be able to support password change as follows to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. h. Requirement R5.6 states "A process to limit, where technically feasible, the number of unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts." State if a TFE can be submitted for this requirement if it is not technically feasible. i. General: The suggested password change frequency is going to make managing these systems difficult, it will add significant workload to the personnel who have to do so, especially with all the documentation that will result.

Yes

No

a. Requirement 1.2, the term Reportable BES Cyber Security Incident only applies to BES Reliability Operating Services and those do not include EACMS or PACS. Is that the intention of this requirement? I believe the applicability section should state more clearly what systems are in scope for this throughout the standard. b. In the Guidelines and Technical Basis section, the definition of a Reportable BES Cyber Security Incident is not the same as the Version 5 Definitions. What is a "necessary response action?" An action is necessary with every Cyber Security Event in order to determine if it's reportable. c. What agencies are incidents reportable to? That should be defined within the requirements.

No

a. R2.1, where it says, "or test," is this a test of the CSIRP? If so, this is more applicable to requirement 3.2. This requirement also addresses all Cyber-Security Incidents. I recommend changing to Reportable BES Cyber Security Incidents. If left as written, this brings all non-reportable Cyber-Security Incidents into scope. b. R2.1 – The use of the word incident is repeated in requirement. We recommend rephrasing requirement: c. R2.2 reads funny, it appears to read as if we are to implement the CSIRP upon the effective date of the standard and then implement the CSIRP again thereafter. If the intent of the standard is to "exercise" the CSIRP, that is more clear than "implement." d. When a BES Cyber Security Incident occurs, the incident response plans must be used. Deviations taken from the plan during the incident or test shall be recorded.

No

a. A timeframe for updating the plan from lessons learn is restrictive. If there is a process change identified that has a major business impact, 60 days may not be enough time for implementation. Recommend a word change to state, "Update the BES Cyber Security Incident Response Plan upon

the implementation of any documented lessons learned within 60 calendar days of implementation." b. General comment: None of the measures mention actions plans from CSIRP exercises. If action plans will be requested as evidence, they should be listed as a measure c. R3.5 Roles and responsibilities may be assigned to a group, not a named individual. We recommend rewording/replacing "each person" with personnel. The use of each person implies superfluous, administrative burden to demonstrate compliance. d. Communicate each update to the BES Cyber Security Incident response plan to personnel with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.
Yes
No
a. R1.3 - We do not agree with the introduction of "protection" within the Recovery Plan requirements. We recommend that information protection requirements be fully addressed in CIP-011 standard b. Specific to Part 1.4 – our current process calls for backups to occur daily, including a mix of incremental and periodic full backups. A manual verification of media on a daily basis is not feasible. Is this intended to be a manual process or can it be supported by system generated notifications of successful backup notifications? Also, what actions should be taken if a backup is unsuccessful? c. It is not clear whether the exercise of the one or more documented recovery plans for Physical Access Control and / or Electronic Access Control or Monitoring systems must be addressed at the system or component level. If the exercise can be met either with a system exercise or for the loss of an access point to the PSP / ESP needs to be stated. d. R 1.5 - Does the data need to be kept for more than 30 days after the analysis or diagnosis of the cause of the event?
No
a. Testing on the effective date of the new standard should be within a year of the new standard being approved. An entity could have conducted the exercise of the plan a couple of months prior to the adoption of the new standard and now be in violation due the wordings in the standard. This comment applies to the other requirements in this standard. b. Allow for the flexibility to combine an operational exercise that addresses both High Impact and Medium Impact BES Cyber Systems. c. Operational Exercise need to be defined. It is not clear whether NIST SP 800-84 definition of a Functional Exercise, which could be met with a paper exercise with personnel simulating their roles and responsibilities, meets the requirement for R2.1 & R2.3 d. R2.1, the wording should be changed to "Exercise the recovery plan." It appears to read as if we are to implement the Recovery Plan upon the effective date of the standard and then implement the Recovery Plan again thereafter. If the intent of the standard is to "exercise" the Recovery Plan, which is more clear than "implement." e. R2.2, the measures should indicate what acceptable evidence is. Is an actual restore expected or proof that the information is available for restoration? In addition, does the word "initially" refer to the effective date of the standard? f. Pursuant to R2.3, is an operational exercise considered the actual recovery of a system? Also, should each asset defined within the scope of a plan be tested or will a recovery of one of the systems within the plan be acceptable? g. R2.2 - It is not clear if by the use of the word "any" the intent is that testing of the media to restore any one component of a BES Cyber System satisfies the requirement.
No
a. None of the measures mention actions plans from Recovery Plan exercises. If action plans will be requested as evidence, they should be listed as a measure. b. R3.1 R 3.4, the level at which an organizational level needs to be stated. For a recovery plan, it is more applicable for changes in the roles and responsibilities of the responders and / or organization. c. R3.3, the 30 day time frame is too restrictive and may not be possible based upon resource constraints. Recommend a word change to state, "Update the recovery plan(s) upon the implementation of any documented deficiencies or lessons learned within 30 calendar days." d. R3.5 Roles and responsibilities may be assigned to a group, not a named individual. We recommend rewording/replacing "each individual" with personnel. The use of each individual implies superfluous, administrative burden to demonstrate compliance: e. Communicate each update to the BES Cyber Security Incident response plan to personnel with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.
No
R2 - The standard needs to allow for a period not to exceed 15 months from the effective date of the

standard or notification that the standard will be effective for the responsible entity to conduct the initial test.
No
a. R1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset: -- This seems to exclude any software that may have been unintentially installed or installed automatically, such as automated installs. b. R1.1.4. Any custom software and scripts developed for the entity: --- To which extend do we document a baseline of the scripts, do the scripts have to be associated with the reliability of the BES Cyber System. c. R1.2: This seems to be an extensive task to the Senior Manager (SM) or Delegate (D), I believe that delegation is presumed here, as the measures allude to it by “where an individual with the authority to authorize the change was in attendance.” d. R 1.2 is problematic in that changes to the BES Cyber System baseline will require authorization from Senior Management. This requirement needs to be limited to major changes in the BES System and have “major” clearly defined. Another approach is to have the ability for proper delegation. e. There is concern about requirement 1.1.4 and the scope of software and scripts that this requirement applies to. f. Changes need to be defined as infrastructure changes and/or software changes that require Cyber Security Testing. Changes to a software function that only involves software modifications need to be excluded. What constitutes a requirement for Cyber Security testing for software changes must be explicitly determined. We suggest that Cyber Security Testing be carried out when a change to the baseline system include: (a) introduces communication to or from another system that is not within the ESP, (b) requires a new listening port and service, (c) requires a patch update to the operating system, (d) requires a new application or generic account, (e) requires a new third party application to be introduced to an existing or new cyber asset, or (f) requires a new cyber asset installation or replacement of an existing cyber asset.
No
a. R2.1 – To better address the basis described in Application Guideline section associated with technical infeasibility to implement automated technical monitoring controls for every BES Cyber System, we recommend rewording the requirement: b. 2.1 Define method(s) and associated periodicity(ies) implemented to monitor changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). c. 2.1.1 Document and investigate the detection of any unauthorized changes.
No
R3.2: Elaboration on the requirement requested: “perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used” Additionally, what if the utility does not have a 1 to 1 test to production.
No
The High VSL severity appears to go beyond what’s in CIP-10 R1. It implies that even though no cyber security controls were deemed to be impacted, that a test still needs to be done to verify that none were affected, The conditions under which Cyber Security Testing must be done for a change in the base configuration from a software change must be explicitly included in the document by the committee.
No
a. For 1.2 and 1.3, the column heading for the second and third columns says “Part” instead of “Requirement” and “Measure.” Is that intentional or is that a typo? b. For 1.2, the measures do no give an indication of what is acceptable evidence. It is a given that documentation will be stored either in electronic or hard copy. However, how will the access control of this requirement be measured? For example, will user access on a need to know basis require an access request form to prove compliance or will the results of the assessment performed in R1.3 demonstrate compliance? c. R1.2 The requirements for this, based upon the evidence that is mentioned, seem to meet at least the level of SECRET classification management in DOD, see especially the following potential two evidence types: " Records indicating information that is stored, transported, and disposed in a manner consistent with the documented process"and " Hardcopies of information stored in a locked file cabinet with keys provided to only authorized individuals". This seems excessive, the evidence outlined as "Records from an information management system containing electronic copies of BES Cyber System Information with user access implemented on a need-to-know basis" indicates the level of document control to provide the protection that should be sufficient. d. For 1.3 if there are changes

made to an existing IPP as a result of this new version, assessing adherence upon the effective date of the standard is unreasonable. I suggest that a 60 window be provided to assess adherence to an IPP to allow for any possible changes to be made to any applicable documentation. e. R1.3 States " Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process". It would be easier to ensure compliance if the requirement to review was done on an annual basis, the suggested rule is more likely to result in a violation and is more difficult to automate in calendar reminders. f. In addition, the example evidence stated evidence that the records were disposed of - there should be clarification on this (i.e. are disposal logs or retirement notices enough?) This needs to be clarified better so there is not over-reaching interpretations of what is acceptable. g. Also, is there a required time frame for an action plan to be implemented? Suggestion would be < 90 days.

No

Although the Guidelines and Technical Basis will not be included in the standard, the strong encouragement to use NIST SP800-88 guidance for media sanitation could be interpreted as the framework that all Registered Entities will be judged by when their media sanitation processes are reviewed by the regions. Is NIST SP800-88 the expectation, recommend providing additional verbiage to remove ambiguity and confusion?

Yes

No

The effective dates says the following: "18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan." This seems to state that CIP 002 - 009 Version 4 is never going to be implemented, this is confusing. It would be better to state: " 18 Months Minimum – The Version 5 CIP Cyber Security Standards (including CIP 010-1 and 011-1) shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. In the event CIP-002-4 through CIP-009-4 do not become effective, CIP-002-3 through CIP-009-3 will remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan."

Individual

Martin Kaufman

ExxonMobil Research and Engineering

No

Yes

CIP-002-5 Requirement R1 requires classification of assets as High, Medium, or Low Impact. Per Attachment 1, all assets that are not High or Medium Impact are , by exception, classified as Low Impact. Classifying all non-High and non-Medium Impact assets as Low Impact assets creates a conflict and logic error with exemption 4.2.4.4 “Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems” [Language from CIP-004-5, but similar language is in the NERC Reliability Standards CIP-003-5 through CIP-011-5]. This exemption is common to CIP standards CIP-003-5 through CIP-011-5 and is used by many small entities that possess no means for remote access. However, it requires the identification of no cyber systems rather than Low Impact assets. As NERC Reliability Standard CIP-002-5, does not allow for the identification of no Cyber Systems, the Standard Drafting Team should modify Attachment 1, CIP-002-5 Requirement R1, or the exemption sections of NERC Reliability Standards CIP-003-5 through CIP-011-5 to correct this logic error.

No

CIP-002-5 Requirement R1 requires classification of assets as High, Medium, or Low Impact. Per Attachment 1, all assets that are not High or Medium Impact are , by exception, classified as Low

Impact. Classifying all non-High and non-Medium Impact assets as Low Impact assets creates a conflict and logic error with exemption 4.2.4.4 “Exemptions: 4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems” [Language from CIP-004-5, but similar language is in the NERC Reliability Standards CIP-003-5 through CIP-011-5]. This exemption is common to CIP standards CIP-003-5 through CIP-011-5 and is used by many small entities that possess no means for remote access. However, it requires the identification of no cyber systems rather than Low Impact assets. As NERC Reliability Standard CIP-002-5, does not allow for the identification of no Cyber Systems, the Standard Drafting Team should modify Attachment 1, CIP-002-5 Requirement R1, or the exemption sections of NERC Reliability Standards CIP-003-5 through CIP-011-5 to correct this logic error.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
No
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
No

No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No

The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not

identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to

develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and

correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.

No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No
The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
No

The currently enforceable Version 3 CIP Standards and draft Version 4 CIP standards adequately address the cyber and physical security requirements of NERC registered entities that have not identified critical assets or cyber critical assets. The removal of an exemption for smaller entities from NERC Reliability Standards CIP-003-5 through CIP-011-5 will require all NERC Registered Entities to develop a programs and procedures that provide no reliability benefit to the Bulk Electric System. The Standard Draft Team should review the exemptions detailed in the Version 4 CIP Standards and correct the logic error that makes exemption 4.2.4.4 in NERC Reliability Standards CIP-003-5 through CIP-011-5 unusable.
Group
Members Representative Committee
Michael Quinn, Chair
Yes
Revise 2.4 to read “Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would still be in the Medium Impact category; however, those Blackstart Resources without External Connectivity would have less cyber risk and move to the Low Impact category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through the Electronic Access Point. Thus, many ERCOT Blackstart Resources would not fit in the Medium Impact category.

Individual
Mikhail Falkovich
PSEG
Yes
1. Capitalization: Only defined Glossary terms or terms in the definitions document (and the standards) should be capitalized when used. Several undefined terms are capitalized, such as Responsible Entities (sometimes not capitalized), Power System Stabilizers, Maintenance Cyber Asset, Automatic Voltage Regulation, Static VAR Compensators, Over and Under Frequency, and Demand Response. Other terms that are defined in the Glossary are not capitalized, such as spinning reserves, contingency reserves, and non-spinning reserves 2. BES Cyber Asset: a. The third sentence that describes the 15-minute time frame and relies on the asset being operational, yet the first sentence states that the asset may be rendered unavailable. This contradiction needs resolution. b. The third sentence should have the last word “BES” changed to “BES Reliability Operating Services.” c. BES Cyber Assets should be tied to a BES Facility. d. An asset rendered unavailable may take more than 15 minutes to impact a BES Reliability Operating Service. For example, if a coal conveyer supplying fuel to generator from a remote fuel storage area is rendered unavailable, the unit itself may not be adversely impacted for hours, depending on its on-site fuel storage capacity. e. What is meant by “adversely impact?” A threshold should be defined. f. Many of the BES Reliability Operating Services are an economic as well as a reliability service (e.g. unit commitment). If the economic aspect of the service is impacted, but not its reliability function, it would appear that the service is not “adversely impacted,” but this should be clarified. g. The definition should have a guideline developed for it that a registered entity could use to develop its BES Cyber Assets. h. The following definition is offered for consideration to the SDT: BES Cyber Asset A Cyber Asset that, when its operation is required, either failed to operate or misoperated, and as a result, an adverse impact would occur on one or more reliability-related functions of one or more BES Reliability Operating Services within 15 minutes. The 15-minute timeframe is measured from the time when the BES Cyber Asset should have operated correctly and the time when adverse impacts begin. A BES Cyber Asset shall be associated with one or more BES Facilities. Cyber Asset redundancy is not a valid reason for not classifying a Cyber Asset as a BES Cyber Asset. A Transient Cyber Asset is not considered a BES Cyber Asset. 3. BES Cyber Security Incident: a. Add “as predefined by the Responsible Entity” after “suspicious event.” [Note: If this is added to the definition, then the Responsible Entity must have a requirement to define this must be included in a CIP standard.] 4. BES Reliability Operating Services a. Dynamic Response to BES Conditions i. Third bullet – spell out “transformer.” ii. Third bullet – if “voltage” is added to the phrase “- Current, frequency, speed, phase” then the fifth and six bullets can be eliminated since they would be redundant to the third bullet. iii. Fourth bullet - why are “Sensors, relays & breakers, possibly software” mentioned? Sensors and relays are part of any Protection System. Circuit breakers are not, although the control circuitry that operates the trip coils is. “Possibly software” is

unacceptable – the SDT should describe the characteristics of the intended software. b. Balancing Load and Generation i. First bullet – “real time” should be “real-time.” ii. Third bullet – Change “&” to “and.” iii. Third bullet – What is meant by “load schedules?” Is it intended to mean “load forecasts?” c. Controlling Reactive Power i. Opening phrase, replace “bounds” with “limits.” ii. Fourth bullet – eliminate “transformer tap changers” since they are not an inductive source. Tap changers raise voltage on one side of a transformer, while lowering it on the other. They move VARS by this action. Any transformer is an inductive source, but reactors, not transformers, are used as a source of inductive capacity. The entire parenthetical should be replaced by “reactors.” d. Managing Constraints i. Fourth bullet – “SOL’s & IROL’s” should be “SOLs and IROLs.” ii. “Identify and monitor Flowgates” should have a bullet e. Restoration of the BES i. First sentence – delete “without external assistance” because it is untrue. ii. Second bullet – replace “planned” with “documented.” iii. Second bullet – “path” should be plural. f. Situation Awareness i. First sentence – delete “planned” ii. Second bullet – delete “Change management” because it is vague. If left in, a time frame should be defined. iii. Third bullet – delete “& Next Day” since Situational Awareness is “current.” 5. CIP Exceptional Circumstance: All of the conditions that define an “exceptional circumstance” may not have been considered in the proposed definition. Therefore, we suggest that the definition be more flexible in defining an exceptional circumstance. The wording should be changed to add the phrase “, including, but not limited to” after “conditions.” 6. Defined Physical Boundary: For clarity, suggest that the last phrase be modified to “for which physical access is controlled.”
Yes
• 1.3 & 1.4 - For Attachment1, Section 1.3 and 1.4 substitute the word "criteria" with the word "section" for clarity purposes. • 2.1 - For Attachment1, Section 2.1: Since the Interconnection is a defined term that is not applicable to this discussion, please remove the capitalization of the term "Interconnection" in this context, and change ".. in a single Interconnection" to "at a single interconnection". • 2.3 - For Attachment1, Section 2.3: We recommend deleting "or Transmission Planner.." to ensure that only one entity is responsible for designating appropriate generation. • 2.8 - For Attachment1, Section 2.8: We recommend changing "Transmission Facilities.." to "BES Transmission Facilities" for consistency purposes. • 2.9 - For Attachment1, Section2.9: Please provide a definition for ther term "Flexible AC Transmission Systems FACTS" for consistency purposes. • 2.13 - For Attachment1, Section2.13: We propose to change the wording "generation control center" to "generation Control Center" for consistency purposes. • 3 - For Attachment1, Section3: we propose to change the wording "..or Section 2 Medium.." to "..Section 2 as having a Medium.." for consistency purposes. • For Attachment1, Section 1 where the statement reads "Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at:" we propose a change to say "Each BES Cyber Asset within a BES Cyber System which is used and located at:" - This is to remove redundancy of the definition from the statement. • For Attachment1, Section 2 where the statement reads "Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for:" we propose a change to say "Each BES Cyber Asset within a BES Cyber System not included in Section 1, and which is used for:" - This is to remove redundancy of the definition from the statement. • We would like to include the following example in the guideline to clarify the categorization of Low Impact BES Cyber Assets and Systems. Due to the need to categorize the Low Impact BES Cyber Systems, an example of a methodology would be to: (1) Identify the physical plant locations (facilities). (2) Determine the possible adverse impact of those physical plant locations (facilities) on the BROS (BES Reliability Operating Services) (3) If low adverse impact to the BROS, then categorize all BES Cyber Systems within the physical plant locations (facilities) to be Low Impact without discretely identifying each system. (per R1.)
Yes
• CIP-002 R1: a. In the wording of the Rationale section, the language states "Cyber Assets and Cyber Systems..". We recommend the language be changed to "BES Cyber Assets and BES Cyber Systems.." instead. b. Please provide a definition of "application of the required controls (last sentence of M1)" Background section comments: • Please provide a clarification on the following statement - "So it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply (Page 7, 2nd paragraph, last sentence.)" - Does this mean that the entity can choose the devices that need to follow the malware protection within a given BES Cyber System and choose those devices that are excluded? •

Since "RE can use the well-developed concept of a security plan for EACH BES Cyber System to document the programs…(last sentence on page 7.)", does this imply the discrete identification of Low Impact Cyber Systems is required?
No
• CIP-002 R2: a. The following wording should be added to the Measure in CAPs,"BES Cyber Assets and BES Cyber Systems initially upon….." should become "High and Medium Impact BES Cyber Assets and BES Cyber Systems initially upon….." • Evidence Retention comment: a. 1.2 We recommend the deletion of the following sentence "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." as it contradicts the requirement to retain the data for three calendar years.
Yes
Yes
Yes
Yes
No
• CIP-003 R5: For the third bullet under M5 we would recommend breaking it out into a table to allow for easier readiblity.
Yes
Yes
Yes
No
• CIP-004 R2: a. For sub-requirement 2.5: We propose to change the wording "Training on the visitor control program." to say "Training on the visitor control program for both physical and electronic security." for completeness purposes. b. For requirement 2: Please provide a guideline (sample deck) of acceptable level of training.
No
• CIP-004 R3: a. For requirements 3.1,3.2,5.1, and 5.2, Applicability section of the table: To stay consistent with the other requirements' applicability we propose to remove the following items from the Applicability Section: Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, Associated Protected Cyber Assets
No
• CIP-004 R4: a. For Requirement 4.1 rationale section - We propose to change the wording "Specified that identify.." to "Specified that identity.." to correct the typo. b. There are times when a web-conference or a shared screen scenario can occur with a vendor for support (or other) purposes. In such a case, we believe that the electronic access is in fact 'escorted'. We propose the following change in the wording in the Rationale for R4: To ensure that individuals who need authorized unescorted electronic or unescorted physical access to BES Cyber Systems have been assessed for risk. Additionally we propose that two defined terms be added to the glossary: Escorted Electronic Access and Unescorted Electronic Access. Thus all of the references which specify 'electronic access' within the standards would become Unescorted Electronic Access.
Yes

Yes
Yes
Yes
No
• CIP-005 R1: a. Applicability - Please provide guidance on what would constitute such systems. Similarly, if no discrete identification of such assets is specified by R1 in CIP-002, an entity would not necessarily be able to identify whether External Routable Connectivity exists or not. We propose to remove the language 'with External Routable Connectivity' from any Applicability sections within the standards. b. For Measures for requirement 1.1 we propose to change the following language: "Evidence may include, but is not limited to, documented technical and procedural controls that exist.." to "Evidence may include, but is not limited to, documented technical or procedural controls that exist.." for clarification purposes c. For Requirement 1.3 (Applicability section) we propose to change the following language: "Electronic Access Points at High Impact BES Cyber Systems" with "Electronic Access Points at High Impact BES Cyber Systems with External Routable Connectivity" for clarification purposes. d. For the change rationale in R1.5: There are times that a single device can provide multiple distinct security measures such as a firewall and an IDS in the same hardware. Please confirm that 'two distinct security measures' can exist on the same device as part of the guideline.
No
a. For requirements 2.1,2.2 and 2.3: We recommend adding the wording "where technically feasible" at the end for all requirement sections within the R2 table.
No
• There is no gradation within the VSLs for this standard. We recommend that Multiple levels of VSLs should be created.
No
• CIP-006 R1: a. For Requirement 1.3 Please provide an example within the guideline of two or more complimentary physical access controls. (Would a magnetic lock and an access card reader be sufficient?) b. The VSLs specify an action to be taken within a limited amount of time (15 minutes). The standard does not specify a time duration. This timed requirement either needs to be removed from the VSLs or added into the standard language. c. For Requirement 1.1: This requirement would force the entities to discretely identify Low Impact BES Cyber Systems. We propose that the wording the Applicability Section is changed to: "facilities containing Low Impact BES Cyber Systems" d. For the Measures in Requirement 1.1: We propose a change in wording - "Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented." to be changed to "Evidence may include, but is not limited to, documented operational or procedural controls exist and have been implemented." e. For the Measures in Requirements 1.2 and 1.3: Due to safety, operational concerns, and local fire codes we propose the wording be changed from "..plan that describes the physical boundaries and how ingress and egress is controlled by two or more different methods.." to "..plan that describes the physical boundaries and how ingress is controlled by one or more different methods…." f. For Requirements 1.4 and 1.5: We propose the following wording change "..in response to unauthorized physical access through any access point.." to be changed to "..in response to unauthorized individuals obtaining physical access through any physical access point.." We also propose that requirements 1.4 and 1.5 are combined. g. For the Measure in Requirement 1: We propose a change in wording "Measure must includes.." to be changed to "Measure must include.." h. For Requirement 1 - Change Description: This language would force the entities to discretely identify Low Impact BES Cyber Systems. We propose that the wording in the Change Description section is changed to: "...this includes how the entity plans to protect facilities containing Low Impact BES Cyber Systems and.." Evidence retention comments: • For Evidence Retention: Three year evidence retention seems excessive and places undue burden and costs for compliance. We recommend a shorter period of a year or 18 months.
Yes

Yes
No
• In the case of the Medium VSL an entity would be punished for an omission of a part of the log, but if an entry was missed wholesale, that event would not be identified and therefore no punishment meted out.
No
• CIP-007 R1: a. For Requirement 1.1: We propose the following language instead of the current version "Disable or restrict access to unnecessary listening logical network accessible ports and document the need for any remaining listening logical network accessible ports" b. For Requirement 1.2: We propose to change the requirement language as follows: "….console commands, or removable media." to "….console commands, or removable media, where technically feasible." c. For Requirement 1.2: Does this language duplicate the physical security requirements already covered under CIP-006-5 R1.3?
No
• CIP-007 R2: a. For requirement 2.1 – measure: We propose that clarification language be included in the guideline that specifies: If a given vendor provides a system with multiple components and multiple softwares, then it is acceptable for the Registered Entity to go to the single vendor as a valid source for the patches and/or updates for all software and firmware. b. For Requirement 2.3: We propose the following changes: "A process for remediation…" to be changed to "A process for the implementation of the remediation plan"
No
• CIP-007 R3: a. For requirement 3.2: Does this language duplicate the requirements in the incident response standard CIP-008-5 R1 and it's sub-requirement? We propose to remove this requirement and add appropriate language to the guideline document of CIP-008v5 so that malicious code removal is addressed. b. For requirement 3.5 - measure: Please provide clarification: Are manually kept logs sufficient for those systems that cannot identify the connection? c. For the Rationale section of R3: Please provide a definition of "Maintenance Cyber Asset". d. For Requirement 3.1: We propose to change the requirement language as follows: "Deploy method(s) to deter, detect, or prevent malicious code." to "Deploy method(s) to deter, detect, or prevent malicious code., where technically feasible." e. For requirement 3.2: We propose to change the requirement language as follows: "disarm or remove identified malicious code" to "disarm or remove identified malicious code, where technically feasible" f. If malicious code constitutes a BES Cyber Security Incident, the first and third bullet points have already been addressed in Part 1.1 and 1.3 of CIP-008v5 R1 respectively. g. For Requirement 3.4: We propose adding ",where technically feasible." at the end of the requirement. h. For Requirement 3.5: We propose adding ",where technically feasible." at the end of the requirement. i. We propose to separate this requirement into 3 sub-parts: 1. Part 1 of 3.3 - Identify signature or pattern update availability (where the malicious code protections use signatures or patterns) 2. Part 2 of 3.3 - Update malicioius code protections within 30 calendar days after the release of approval from the identified source/sources that address(es) the updates 3. Part 3 of 3.3 - the implementation of malicious code protections
No
• CIP-007 R4: a. for requirement 4.3: This language implies that all entities have a seven day a week operations staff in this area. It may be more prudent to change the requirement from next calendar day to next business day. b. For Requirement 4.1.3: We propose adding ",where technically feasible." at the end of the requirement. c. For Requirement 4.1.4: We propose adding ",where technically feasible." at the end of the requirement.
Yes
No
2. VSL: • R2: a. For the VSLs applicable to Requirement 2: We recommend adding the following breakdown of the severity levels instead of having a single Severe level applied: -Severe being no source identified and patches not reviewed within 30 days -High being not all patches reviewed within 30 days or no remediation plan implemented for reviewed patches -Medium being no source identified • R3: a. Similarly to the comment for R3.2. the language in the R3 VSL references the disarming and

removal of identified malicious code which may be a duplicate of the incident response VSLs in the standard standard CIP-008-5 R1 • R4: a. For the VSLs applicable to Requirement 4: Under the High VSL the language references the need for real-time alerting for logging failures which is not identified in the standard requirements. We recommend removing this language. Additionally, an entity may choose to designate a real time alert requirement for a piece of hardware/software that technically is not able to perform logging. Thus, a technical exception may be needed. b. We propose the following change to the Severe VSL applicable to Requirement 4: "The Responsible Entity failed to identify and implement methods to generate alerts for events that it determines to necessitate a real-time alert" to be changed to “The Responsible Entity failed to identify and implement methods to generate real-time alerts for events it determined necessary to have real-time alerts”
No
a. We recommend that the first sentence is changed to “R1 provides for consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems.”? The third sentence should be changed to: “Once the number and severity of events rises to the level of becoming a Reportable BES Cyber Security Incident the current version of EOP-004 directs..."
No
• CIP-008 R2: a. 2.2 - We propose adding "exercise" for the first bullet and "test" for the second and third bullets to provide a clear description of what actions need to be taken to implement the BES Cyber Security Incidence response plan. The suggested languages are as follow: -"exercise" by responding to an actual incident, or -"test" with a paper drill or table top exercise, or -"test" with a full operational exercise b. 2.3 - The term "documentation" is too vague. "records" would be more concise term for this requirement. c. 2.2- The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. d. We suggest deleting "when incident occurs" after” response plans must be used" to eliminate redundancy. The proposed language is as follow: “When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording …..”
No
• CIP-008 R3: a. Requirement - 3.4 - We suggest breaking down this requirement into 2 parts: 30 days for technology changes and 60 days for organizational changes, which may take longer to address. The proposed language is as follow: Update the BES Cyber Security Incident response plan(s) within: -1.THIRTY calendar days of any TECHNOLOGY changes that impact the plan and -2. SIXTY calendar days of any ORGANIZATIONAL changes that impact the plan b. Requirement 3.1 - The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to review its BES Cyber Incident response plan on the effective date even though it’s not required to have its initial response plan until the effective date per R1.
Yes
No
• CIP-009 R1: a. For requirements 1.4 and 1.5, titles of second and third column should be "Requirements" and "Measures" respectively b. For Requirement 1.4, delete “initially after backup" from the requirement due to the fact that the back up process is self-checking by default. c. For requirement 1.4, please provide clarification on the frequency of backup verification. We agree that backup verification should be undertaken; however, we believe that verification after each backup is counterproductive. d. For requirement 1.5, we believe that this should be moved to CIP-008 standard
No
• CIP-009 R2: a. For rationale section of requirement 2, please provide a definition for "Operational Exercises" b. For rationale section of requirement 2, delete "28" in the beginning of the last sentence of the "Functional Exercises" section c. For requirement 2.1, we recommend replacing "upon the" with "within the first calendar year of the effective date of the standard" d. For requirement 2.1, we recommend adding: -"exercise" to the first bullet -"test" to the second bullet -"test" to the third bullet e. Requirement 2.1 and 2.3 - The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because they would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table

top exercise or a full operational exercise.
No
• CIP-009 R3: a. For requirement 3.1, we recommend removing "or lessons learned" at the end of the sentence b. For requirement 3.4, we suggest to allow 60 days for updating organizational changes related to recovery plan(s) c. For requirement 3.5, we suggest to allow 60 days for communicating recovery plan updates. d. Requirement 3.1- The language “initially upon the effective date of the standard” appears in this requirement is unreasonable because it would require each Registered Entity to review recovery plans on the effective date even though it’s not required to have its initial recovery plan until the effective date per R1.
Yes
No
• CIP-010 R1: a. For requirement 1.1, please provide a clarification on how often the baseline should be updated. b. For requirement 1.1.3, we recommend changing it to “Any commercially available application software (including version) intentionally installed by or at the request of the Responsible Entity on the BES Cyber Asset" c. We propose the following modified language to requirement 1.4.1: Prior to the change, determine required cyber security controls that could be impacted by the change AND TEST THE NEW CONFIGURATION IN A TEST ENVIRONMENT d. We propose the following modified language to requirement 1.5.2: the measures used to account for any differences in operation between the test and production environments BEFORE THE CHANGE IS MADE.
No
• CIP-010 R2: a. For Requirement 2.1, we recommend that the guideline includes the following statement: "physical hardware changes that do not affect the functionality of the system to be excluded from the requirement" (example I/O port rewiring or power supply changes)
No
• CIP-010 R3: a. We feel that the language “initially upon the effective date of the standard” appears in requirement 3.1 and 3.2 is unreasonable because it would require each Registered Entity to perform assessments on the effective date of the standard. Please provide a guidance section that would detail alternative times (such as, prior to the standard going into effect) that would allow the Registered Entity to comply effectively. b. For requirement 3.2, we recommend that the standard mention that the active vulnerability assessment be performed in either a test OR production environment For the Guidance and Technical Basis section: • Within the guidance document section R3(first sentence), we propose to change "not" to "note" Compliance: • For the Compliance section (on page 20), we propose first bullet of sec 1.2 to be changed to "Each Responsible Entity shall retain data or evidence from the last completed audit…" from "Each Responsible Entity shall retain data or evidence for since the last completed audit…"
Yes
No
• CIP-011 R1: a. The language “initially upon the effective date of the standard” within this requirement is unreasonable because it would require each Registered Entity to perform an assessment on the effective date of the standard
Yes
No
• This VSL should be updated to include “…initially within the first calendar month or quarter after the effective of the standard…”
No
1. The example on p. 3 of the Implementation Plan document for unplanned changes, power flows are not a criterion for the impact level of any BES Cyber Assets, so the example needs to be revised. Nevertheless, for “planned” changes by one Responsible Entity that impacts another Responsible Entity, what is the timeline for compliance by the other Responsible Entity and would the causal Responsible Entity be responsible for the compliance cost for the other Responsible Entity? For other standards (e.g., TPL) an entity that whose planned changes result in another entity being out of

compliance is responsible for the entire cost of compliance associated with its actions, both for itself and other entities that it impacts. 2. Although this issue is addressed in particular standards and not in the Implementation Plan, it will cause significant implementation issues if not addressed. Common language that requires implementation of a requirement “initially upon the effective date of the standard” appears in numerous standards. These requirements are unreasonable because they require an action on the first day (and first day only) that the standard is effective. Here is a list of where this language appears in the v5 standards for requirements that are unreasonable when this language is used. a. CIP-008-5, R2.2 is unreasonable because it would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. b. CIP-008-5, R3.1 is unreasonable because it would require each Registered Entity to review its BES Cyber Incident response plan on the effective date even though it’s not required to have its initial response plan until the effective date per R1. c. CIP-009-5, R2.1 and R2.3 are unreasonable in that they would require each Registered Entity to perform an action that is not valid unless performed on the effective date, such as conduct a paper drill or table top exercise or a full operational exercise. d. CIP-009-5, R3.1 is unreasonable because it would require each Registered Entity to review recovery plans on the effective date even though it’s not required to have its initial recovery plan until the effective date per R1. e. CIP-010-1, R3.1 and R3.2 are unreasonable because they would require each Registered Entity to perform assessments on the effective date of the standard. f. CIP-011-1, R1.3 is unreasonable because it would require each Registered Entity to perform an assessment on the effective date of the standard.
Group
PowerSouth CIP Review Team
Tim Hattaway
No
Yes
Yes
Yes
Yes
Yes
No
Would like to see this changed to 60 days.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
No
Further clarification is needed regarding what part of the communication path to the destination host must be encrypted or if the entire communication path is the intent of the regulation. The lack of clarity leaves this open for interpretation by an audit team.
No
Under the measures section, it states "…and how ingress and egress is controlled by two or more different methods…" implies that both ingress and egress must be controlled by two or more different methods (physical access controls). We feel that a single egress physical access control should be acceptable for authorized individuals exiting a restricted space.
No
Clarify or Remove: "and records of disposition of security related event logs beyond ninety day up to the evidence retention period." To what extent do you mean "records of disposition"? How do you prove log data for a Cyber Assets was deleted from a log server after a certain age? This needs to be clarified more to identify exactly what is required. If the standard states you need to keep logs for 90 days, you shouldn't have to keep them longer to prove to an auditor that you had the logs for every 90 day period since the last audit. If that is the intent, then the standard should state that.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Individual
David Dockery
Associated Electric Cooperative, Inc
Yes
BES Cyber Asset Definition CHANGE FROM: BES Cyber Asset - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. CHANGE TO: BES Cyber Asset - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Service, without regard to the initial time of asset compromise. A Transient Cyber Asset is not considered a BES Cyber Asset. RATIONALE: 1) Brevity, clarity, and less is better. 2) Deleted stuff belongs in guidelines. BES Cyber Security Incident Definition - Bullets #1 & #2, Change: “was an attempt” To: “was an apparent attempt" Rationale: we cannot judge intent BES Cyber System Definition Change: “Maintenance Cyber Asset” To: “Transient Cyber Asset” Rationale: Consistency and no definition proposed for Maintenance Cyber Asset. BES Cyber System Information Definition Move: the “(e.g., network addresses…)” parenthetical To: immediately follow “Electronic Access Control Systems” Rationale: group EAC Information examples immediately with the EACs clause. Associated Electric Cooperative also agrees with NRECA's comment BES Reliability Operating Services –AECI believes the following BES services should be removed from the BES Reliability Operating Services, because they fail to meet the “real-time reliable operation of the BES” 15-minute adverse-impact criteria: 1) Balancing Load and Generation, (other than ACE, nothing else in this category can have a 15-minutes or less impact, and ACE availability and integrity are addressed within the BAL Standard, so including here is double-jeopardy.) 2) Managing Constraints, 3) Restoration of BES, (actual control likely will be performed by hand with field personnel) 4) Situational Awareness – Frequency Monitoring – (While frequency monitoring is important, contrary to the underlying position within the CIP standards, redundancy of frequency monitors really does matter, and the standard should probably leave this one off, in order to avoid only a few instances of frequency-monitoring equipment being implemented. Also, the availability of a reliable Frequency Monitoring signal is subject to a strict BAL standard. CIP Senior Manager Associated Electric Cooperative agrees with NRECA's comment Control Center Definition Change: “BES generation facilities or transmission facilities” To: “BES generation facilities or BES transmission facilities” Rationale: Clarity of scope. Comment: AECI's understanding that this definition's use of the NERC glossary "System Operator", inherently limits the scope of this definition to only "manned" locations where BA, TOP, GOP, or RC functions are performed. Electronic Access Point (“EAP”) Definition Comment: There appears to be a loop-hole in this definition, with regard to dumb terminals utilizing dial-up or routed access from the other end. By definition here, old dumb terminals are not Cyber Assets because they are not programmable. (Ok, most of the “later” models had EPROMS). This definition dictates “between Cyber Assets”. (This potential flaw may carry over to “External Connectivity” and “Interactive Remote Access” definitions as well.)
Yes

Appendix 1, both Sections 1.3 and 1.4 APPEND: ", at two or more locations" RATIONALE: Clarity of intent and consistency with Control Center definition. Appendix 1, Section 2.4 CHANGE: "Each" TO: "At least one" RATIONALE: 1) Current wording will result in many black-start resources being removed from Transmission Operator's black-start plans, thereby decreasing overall system reliability in case of a real system-restoration emergency, and 2) consistency with the way the drafting-team's CIP-002-5 Guidelines addresses redundant assets within an entity's SRP black-start unit's cranking-path. Appendix 1, Section 2.5 CHANGE: "the Cranking Paths" TO: "the section 2.4 identified Resource's Cranking Path" RATIONALE: consistency with AECI's proposed change to 2.4 above Please note that AECI encourages the CSO 706 SDT to consider the following set of proposed Appendix 1, Section 1.2, 2.13, and new 2.14 changes and corresponding guidelines as a package. ===Begin==== Appendix 1, Section 1.2 CHANGE TO: "Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection". RATIONALE: 1) Consistency with the bright-line risk cited throughout CIP-002-5 Appendix 1, 2) smaller BAs are automatically caught by CIP-002-5 Appendix 1 Proposed Section 2.14 Medium Impact Rating, and 3) legitimate APPA and NRECA concern for cost versus quality and risk of additional High Impact Rating controls and measures, versus expected return on industry's investment forced on these small entities. Appendix 1, Section 2.13 CHANGE TO: "Control Centers not included in High Impact Rating (H), above, that perform (1) the functional obligations of Transmission Operators or Transmission Owners that directly or indirectly control 1500 MW of generation; or (2) generation control centers that control 1500 MW or more of generation." RATIONALE: 1) Inconsistency in this draft's proposed usage and citation of UVLS and UFLS 300 MW load-shed threshold. UVLS and UFLS concern is expected shedding of load amounts necessary to stabilize system voltage or frequency, whereas this scope of concern is sudden and unexpected loss of generation. 2) Consistency with impact of Appendix 1, Section 2.1, although the impact of loss in 1500 MW generation, diversified across several electrical network locations, is expected to be much less than for 1500 MW single plant loss concentrated at one location within a network. 3) Section 2.14 is proposed below to manage remaining scope of this previously worded section. 4) BAs below 1500 MW are not exempted as are TOs, TOPs, and GOPs, because the scope of their interconnectivity with other control centers poses a greater risk to the BES. 5) See corresponding Guidelines below. Appendix 1 - Section 2.14 ADD: "2.14 Control Centers, not previously included in High Impact Rating (H) or Medium Impact Rating (M), above, that perform the functional obligations of Balancing Authority, Transmission Operators or Transmission Owners, or Generation Operators, and that do not implement protected data connections with other Control Centers in a manner as to prevent themselves from being used as cyber-attack vectors into other Medium Impact or High Impact Rating Control Centers." Rationale: In the CIP-002-5 Guidelines p.30 Bullet#1 (on that page), the SDT provided no explanation as to why all transmission control centers should be deemed Medium Impact, although they did provide some impact consideration for generation control centers. AECI strongly encourages the SDT to adopt this recommended change along with our proposed corresponding guidelines, in consideration of FERC requests for consideration of control center impacts and connectivity risks (FERC Order 706, paragraphs 280, 281, 282, and FERC NOPR Docket No.RM11-11-000, paragraphs 41, 43, 53), and to incent our industry toward deploying true mono-directional "routable" (data-diodes) and non-routable (hardened mailbox RTU) data-interface connectivity, where applicable, as mitigating measures that would lower these local-control-centers to their true Low Impact category, and to incent further innovation and deployment of hardened communication interfaces. Also, per Appendix Section 3, the Control Centers excluded from Medium Impact Rating (M), must necessarily exercise Low Impact Rating (L) controls specified within the standards, and be subject to audit, which would necessarily include assessment of all their "protected data connections" required within this section. See also companion changes to CIP-002-5 Appendix 1, Sections 1.2 and 2.13. Appendix 1 Guidelines, Section 2.13 ADD GUIDELINE: "2.13 The phrase - directly or indirectly control - encompasses the potential to open multiple breakers or otherwise issue automated command controls from a compromised Control Center, in such a manner as to cause separation of 1500 MW or greater net generation from an Interconnection. This standard selects 1500 MW for compatibility with Section 2.1." ========End======== Appendix 1 Guidelines, Section 2.14 ADD GUIDELINE: "2.14 Beyond direct or indirect impact above the bright-line threshold for generation or load, there is legitimate concern that any interconnected Control Center may serve as a cyber-attack vector into neighboring Control Centers. The CIP Standards' Physical and Electronic controls, specified for High and Medium impact Control Centers, function to mitigate those prolonged-exposure threats. This section recognizes that our industry's cyber-security

will benefit from their installing hardened data-communication interfaces that practically function as “air-gaps” against opportunistic hacking, and it seeks to incent such deployment at all Control Centers where the real-time BES impact would otherwise be rated as Low Impact. At the time of this standard’s ratification, some data-diodes or hardened mailbox-RTUs can meet this need, but it is likely that future developments will provide even more secure, robust, and economically attractive solutions. For responsible entities that identify their control-centers as Low Impact, the CEA will verify that the installed communications protection device(s) and implementation(s) on every communication interface with other Medium or High Impact Control Centers, are such that the Low Impact control centers have a low probability of being used as a cyber-attack vector on other Control Centers. Evidence the CEA might look for could include but not be limited to device configuration information, file structures used for the exchange of data, and related procedural controls. These devices should be protected and managed in a manner similar to that which is applied to devices serving as electronic access points to protected networks. Specifically, the responsible entity must be prepared to show evidence to the CEA that these interfaces to High and Medium impact Control Centers, have been and are being actively maintained through a deliberate program of security-patch awareness, evaluation, and deployment based upon their evaluation.”
No
R1.1 CHANGE: “and Facilities is placed” TO: “and Facilities being placed” RATIONALE: Grammatical.
No
R2 Rationale CHANGE: “Manager’s approval” TO: Manager’s responsibility in approval” RATIONALE: the Senior Manager or delegate performs an approval, but the responsibility remains with the Senior Manager. R2 CHANGE: “initially upon the effective” TO: “initially prior to or upon the effective” RATIONALE: “it should be permissible for the Senior Manager to perform this duty before the effective date, rather than confining that action to the exact date this body of standards become effective. M2 CHANGE: “Manager review” TO: “Manager or delegate review” RATIONALE: Consistency with the requirement itself.
Yes
Yes
No
R2 CHANGE: Renumber bullets 2.1..2.10 rather than 1.1..1.10. RATIONALE: Consistency with the Requirement number. R2 CHANGE: Tighten scope of requirements, succinctly, to match scope identified within guidelines RATIONALE: Legal requirement scope could be interpreted too broadly, by either responsible entities or auditors. Is Physical Security related to Cyber Assets, personnel, cyber-related personel, or general building security? Is System Security for the Electrical Power System, the Cyber System, or the Alarm System, and how is it differentiated from Electornic Security and Physical Security. While page 20 and 21 of the guidelines are invaluable here, the legal scope of this requirement could and should be narrowed.
Yes
Yes
Yes
No
R6 CHANGE: “thirty” TO: “sixty” RATIONALE: Senior Managers are busy and so long as there were no underlying violations within a program, it was working. And corresponding R6 VSL CHANGE: “30” TO: “60” RATIONALE: Senior Manager change will encompass a lot of responsibilities for very busy people. Making 30 days SEVERE is unreasonable. ALTERNATIVE PROPOSAL R6: no change R6 VSL: Low: Senior Manager change undocumented greater than 30 days but less than 60 days. Moderate: Senior Manager undocumented or one delegate undocumented greater than 60 days but less than 60 days. High: Senior Manager remained undocumented 60 days but less than 90 days or two or more delegates undocumented 30 days but less than 60 days. SEVERE: Senior manager remained

undocumented 90 days or more, or three or more delegates undocumented 30 days or more. Rationale: More granularity where risk is already noted as LOW, where nothing else went wrong other than this formal documentation.
No
R5 VSL Change: Shift all columns left Rationale: If the program continues to operate properly and no additional violations were spotted, then this failure in documentation is just window-dressing. If not, then there will be plenty of additional requirements violated along with those penalties. R6 VSL: AECI proposed two alternative changes for R6 and corresponding R6 VSL, posted under R6.
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 CHANGE: “at time of resignation or termination” TO: “within 24 hours of resignation or termination” RATIONALE: Consistency with hard time-frames asserted with other sub-requirements, with reasonable delay for uncontrollable circumstances surrounding some separation of employment.
No
R4 VSL CHANGE R4 Lower VSL: “Entity had no formal PRA program per R4, yet provided evidence of PRAs having been performed within the last 7 years for all personnel with access stated within R4, and otherwise conformant to the PRA requirements within R4." CHANGE R4 Severe VSL: altered to read “and has no evidence of PRAs having been performed for individuals granted … access” RATIONALE: better match severity to risk of circumstance R5 VSL CHANGE R5 Lower VSL: “The Responsible Entity did not have a documented process for personnel risk assessment yet performed PRAs conformant with NERC CIP Standards” CHANGE R5 Severe VSL: append “and has no evidence of PRAs having been performed conformant with the NERC CIP Standards”. RATIONALE: match severity to risk of circumstance R6 VSL CHANGE R6 Severe VSL: append “and Access Privileges were in effect that did not conform to NERC CIP Standards” RATIONALE : match severity to risk of circumstance R7 VSL changes: for cases of reassigned or transferred individuals, shift the failure numbers as follows CHANGE R7 Lower VSL: “1 or 2” CHANGE R7 Moderate VSL: “3 or 4” CHANGE R7 High VSL: “5 or 6” CHANGE R7 Severe VSL: “7 or more” APPEND to 7 Severe VSL: “and Access revocation was not performed conformant to the NERC CIP Standards.” To the Severe VSL. RATIONALE: match severity to risk of circumstance (personnel retained within the company are operating at a higher trust level and with greater corporate policy controls than those who have been removed from the workplace.)
No
R1.5 Requirements CHANGE: “malicious” TO: “potentially malicious” or “unanticipated” or “unnecessary” RATIONALE: align with CIP-007-5 R4.1.4 wording, which employs “potentially” or use other wording that frees entities from being required to establish intent
Yes
No
R1 VSL CHANGE: Create R# R1.1 row with... ADD R1.1 Lower VSL: “The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access , but all sampling produced evidence of proper restrictions having been applied to EAPs” ADD R1.1 Moderate VSL: “The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access, and sampling did produce evidence that proper restrictions were not applied to

some internal EAPs and yet external EAPs were appropriately controlled" ADD R1.1 High VSL: "The responsible entity did not define any technical or procedural controls to restrict unauthorized electronic access, and sampling did produce evidence that proper restrictions were not applied to internal or external EAPs" ADD R1.1 Severe VSL: "non-applicable". RATIONALE: match severity with risk of Low Impact Assets and Systems R1 VSL CHANGE R1 VSL R#: "R1" TO: R1.2..R1.5 VSL R#: "R1.2..R1.5" CHANGE R1.2..R1.5, all VSLs: delete the phrase "The Responsible Entity did not define technical or procedureal controls to restrict unauthorized electronic access." RATIONALE: This phrase applies only to Low Impact Cyber Assets, which are addressed in the suggested companion change above. R2 VSL CHANGE R2 Moderate VSL: add the phrase "Responsible Entity had Medium Impact Assets where: ("<body of text found in the Severe column>")" CHANGE R2 Severe VSL: "Responsible Entity had High Impact Assets where ("<body of text originally in the Severe column>")" RATIONALE: match severity with risk.
No
Page 10 "Requirements and Measures, Summary of Changes, 2nd line CHANGE: "was no specific" IS: "is no specific" RATIONALE: grammatical M1.1 CHANGE: "controls exist" TO: "controls that exist" RATIONALE: grammatical R1.1 Rationale CHANGE: "how the entity plans to" TO: "how the entity plans and acts to" RATIONALE: intent of requirement and measure?
Yes
Yes
No
R1 VSL INSERT row R# R1.1 ADD R1.1 VRF: "Low" ADD R1.1 Low VSL: "The Responsible Entity has documented procedural controls but 1 or 2 boundaries failed to meet or exceed those controls" ADD R1.1 Moderate VSL: "The Responsible Entity has documented procedural controls but 3 or 4 boundaries failed to meet or exceed those controls" ADD R1.1 High VSL: "The Responsible Entity has documented procedural controls but 5 or 6 boundaries failed to meet or exceed those controls" ADD R1.1 Severe VSL: "The Responsible Entity did not have documented procedural controls, or 7 or more boundaries failed to meet or exceed their documented controls." RATIONALE: Current VSLs do not match Low Impact requirement. AND CHANGE previous row R# "R1" to "R1.2..R1.6" CHANGE "R1.2..R1.6" High VSL: remove the phrase "OR The Responsible Entity has documented and implemented physical access controls, but does not initiate a response within 15 minutes of a detected unauthorized physical access into a Defined Physical Boundary. (Part 1.6)" RATIONALE: There is no corresponding 15-minute response requirement for initiating a response to unauthorized physical access alarms. R1.6 does not apply to the violation described, and although R1.5 does somewhat match, there is no time-limit on response for that sub-requirement.
Yes
No
R2.2 CHANGE: "identified source that addresses" TO: "identified source, that addresses" RATIONALE: Clarity from inserted comma ","
No
R3.5 CHANGE: append ", and disconnection." RATIONALE: Need to know the extent of time that Transient Cyber Asset was in contact with a BES Cyber System, in order to verify it met the definition of a Transient Cyber Asset. M3.5 CHANGE: append ", and when they were disconnected as well." RATIONALE: Corresponding change to recommendation for R3.5.
No
R4.3 CHANGE: "calendar" TO: "business" RATIONALE: This standard's requirement will include small control centers with meager (0.5 –to- 2) support-staff. There is no need for weekend call-outs where non-operational event-logging has failed. Staffing demand is unreasonable for risk. R4.4 Measures REMOVE: "and records of disposition of security related event logs beyond ninety days up to the evidence retention period." RATIONALE: If the concern here is guarding Protected Information, it is addressed within CIP-011-1. If the concern is proof of prior existence, solely for audit purposes, this measurement is too onerous for the risk being managed, and the current 90-day records are sufficient.

No
R5.5.1 CHANGE: reword as “Minimum Password length of at least 8 characters, or maximum supported by the BES Cyber System if less than 8 characters is supported.” RATIONALE: Clarity R5.5.3 CHANGE: “based on” TO: “based upon” RATIONALE: grammatical
No
CHANGE R1 through R5 VSL for Medium Impact Assets MOVE R1 through R5 Medium Impact Assets High VSL text to Medium VSL column MOVE R1 through R5 Medium Impact Assets Severe VSL text to High VSL column CHANGE R1 through R5 VSL for Low Impact Assets (R5.4) MOVE R1 through R5 Low Impact Assets High VSL text to Low VSL column MOVE R1 through R5 Low Impact Assets Severe VSL text to Medium VSL column RATIONALE: align severity with risk
Yes
No
R2.1 DELETE: “when incidents occur” RATIONALE: grammatical CHANGE: “recording” TO: “notation” RATIONALE: While important to keep post-mortem notes of steps followed or omitted, “recording” implies notation of time with steps taken or time and rationale when a step is omitted, with the focus upon making certain those actions/decisions were accurately recorded. While this is reasonable during planned tests, a facility under cyber-assault is less likely to have the same luxury of time and there is no risk to after-the-fact annotations being performed by the response team. R2.1 Measures CHANGE: “documentation” TO: “follow-up documentation” RATIONALE: See rationale for accompanying suggested R2.1 change above.
Yes
No
MOVE R1 through R3 Low Impact Assets High VSL text to Low VSL MOVE R1 through R3 Low Impact Assets Severe VSL text to Moderate VSL RATIONALE: Align risk with severity CHANGE R3 VSL Low Impact Assets VSL: "30 calendar days" TO R3 VSL Low Impact Assets VSL: "60 calendar days" APPEND R3 VSL Low Impact Assets VSL: to last sentence "within 60 calendar days" RATIONALE: Consistency and align timeframe with Severity. (Failure to review within 30 days might be considered High, and written into that column – see note on Low Impact Asset VSLs above.)
Yes
No
R2.3 Guidelines ADD: Better guidelines. RATIONALE: Without some related guidelines, the phrase “in a representative environment that reflects the production environment” introduces too much ambiguity and opportunity for disagreement between Responsible Entities and Auditors. “SEE FAQS AND CIPC GUIDELINES” seems inconsistent with the quality of product being produced in other CIP version 5 standards.
Yes
No
MOVE R3 Severe VSL text to High VSL ADD R3 Severe VSL: With 60 days violation. RATIONALE: align severity with risk.
Yes
Yes
No
R3.1 CHANGE: “Initially” TO: “Prior to or upon” RATIONALE: industry flexibility in timing R3.2 CHANGE: “Initially" TO: “Prior to or upon” RATIONALE: industry flexibility in timing R3 Guidelines (page 28) CHANGE: “should not that” TO: “should note that” RATIONALE: correction
No

R1 High VSL – Remove: “OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.” Rationale: remove double-jeopardy, where other standards and/or requirements were violated because something went wrong with planned changes to the baseline
No
R1.3 CHANGE: "Initially" TO: "Prior to or " RATIONALE: industry needs flexibility in timing
Yes
Yes
No
In all Implementation Plan occurances throughout these Standards and Implementation Plan CHANGE: “18 months” TO: “24 months”, including all other related wording RATIONALE: CIP Version 4 provides for 24 month implementation plan, yet CIP Version 5 is going to bring many more Responsible Entities into scope that have not formerly been acclimated to planning and accomplishing compliance with the NERC CIP Standards. It does not seem fair for those who already have acquired this level of expertise and experience, to impose an unreasonable timeframe on the uninitiated, just because we want Version 5 to eclipse Version 4. If our industry believes it best to move directly from version 3 to version 4 of the CIP standards, then we need to come up with a better mechanism than unfairly burdening these newcomers. <<<<OTHER CHANGES AECI SAW NO PLACE TO SUBMIT>>>> CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.2, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.2, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, Introduction section 4.1.2 Bullet#5 CHANGE: “Its Transmission Operator’s restoration plan” TO: “Its Transmission Operator’s formal restoration plan” RATIONALE: Avoid entities’ violating these standards, due to unforeseen restoration conditions that cause them to reasonably activate a restoration plan outside of their formal plan. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.6, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.1.6, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.2.2, Bullet#1 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away. CIP-003-5 through CIP-011-x, A. Introduction, section 4.2.2, Bullet#2 APPEND: “, and with capability to shed 300 MW or more of load through a single system.” RATIONALE: Clarity, so exempt smaller entities can pick-up on that right away.
Group
CWLP
Roger Powers
Yes
"Large" Control Centers should not equate to functional responsibility rather impact on reliability. TOP can be an entity with less than 100 miles of 138 kV transmission. BA function can refer to small subset of BA role when entity participates in an organized market environment. There is a need to clarify how the LBA function in MISO fits with the definition. BES Cyber System uses the term "Maintenance Cyber Asset" which is not defined. Should it be "Transient Cyber Asset"? Does the 30 day reference in Transient Cyber Asset refer to consecutive days, days per year, days ever?
Yes
The Drafting Team has chosen not to define "generation control center" in item 2.13 and to distinguish control rooms from control centers. An approved definition is crucial to eliminate varying interpretations.

Yes
Yes
No
An entitiy should be allowed to designate more than one CIP Senior Manager as long as the division of responsibility is clearly defined.
Yes
No
In conjunction with the comment on the previous question, the approval should come from the appropriate Senior Manager where more than one is allowed.
Yes
No
An entitiy should be allowed to designate more than one CIP Senior Manager as long as the division of responsibility is clearly defined.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
The 30 day time frame for access privilege revocation is not sufficient for remotely located cyber assets.
No
The requirement for Low Impact BES Cyber Systems is too vague to be auditable.
Yes
Yes
Yes
No
It is unclear from the standard and associated definitions whether cameras are considered locally mounted hardware.

Yes
Yes
Allowing 45 days for remediation plan creation would facilitate compliance for smaller entities.
Yes
No
The timeframe for detection and response to event logging failure needs to be extended to the end of the next regular working day.
No
The timeframe for activating a response needs to be extended to the end of the next regular working day.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
(1) The definition of BES Cyber Asset includes criteria where if it were unavailable, degraded, or misused, "would" adversely impact one or more BES Reliability Operating Services within 15 minutes. This criteria needs to be prospective and state "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and

therefore the Cyber Asset in question does not meet the criteria for BES Cyber Asset. The definition also includes a timeframe qualifier that references sending or receiving "instructions to operate." This qualifier is too narrow. Entities may take the stance that the BES Cyber Asset must be directly involved in a supervisory control function and would eliminate non-supervisory control systems, including those providing situational awareness, from designation as a BES Cyber Asset. The definition of BES Cyber Asset also includes a statement that redundancy shall not be considered when determining availability. This statement should be modified to state "redundancy shall not be considered when determining potential impact or availability." (2) The third bullet in the definition of BES Cyber Security Incident should be modified to state "Results in 'attempted or actual' unauthorized physical access…" (3) The definition of BES Cyber System includes a statement that a "Maintenance Cyber Asset" is not considered a part of a BES Cyber System. This term, which is also used within several CIP Version 5 Standards requirements, is not defined in the definitions document, and appears to be used interchangeably within the standards with the term Transient Cyber Asset. One term should be adopted and used consistently. (4) The BES Cyber System Information definition includes a reference to "floor plans that contain BES Cyber System Impact designations." The reference to impact designations is unnecessary and alters the wording of this example of information to be protected found in previous versions of CIP-003/R4.1. The reference should be modified to state "floor plans that include BES Cyber System or BES Cyber Asset details." Similar treatment should be given to the reference to equipment layouts. The definition would also be improved by modifying the opening statement to state "Information, about one or more BES Cyber Systems or BES Cyber Assets, that include 'but are not limited to' one or more of the following." (5) The definition of BES Reliability Operating Services includes a reference to "operations planning horizon." This and other timeframe terms are used throughout the Version 5 standards. These terms need to be defined, either in the NERC Glossary or by reference to a NERC published document containing the definition. (6) The definition of Cyber Assets has been modified to eliminate communication networks from the definition and to add the qualifier "in those devices" to the specification of "data" in the definition. This revision suffers from two shortcomings. First, the elimination of communication networks from the definition could be misconstrued by the entity to now exclude networking devices (switches, routers, etc.) from identification as a Cyber Asset requiring protection if within the Electronic Security Perimeter. Additionally, the exclusion eliminates the expectation to protect data in motion within the confines of the Electronic Security Perimeter. This is a step backwards from the current version of the CIP standards and does not incorporate a FERC approved interpretation of CIP-006-3/R1.1 into the new standards. (7) The definition of Defined Physical Boundary ("DPB") is sufficiently non-specific as to potentially afford no protection at all. The DPB definition should clarify that the DPB needs to be designed to deter and detect unauthorized access. As currently written, a climbable fence with a locked gate, possibly in concert with an unmonitored substation control house could be construed as meeting the definition. The climbable fence is not a deterrent regardless of the locked gate and the unmonitored control house, while possibly a deterrent, will not serve to detect unauthorized entry. (8) The definition of Electronic Access Point ("EAP") includes references to "routable or dial-up communications" that could be construed to eliminate non-routable (e.g., RS-232 serial communications) from consideration. The definition could also be construed as meaning every network interface on every Cyber Asset within a defined Electronic Security Perimeter because of the "between Cyber Assets" terminology. It may be preferable to modify the definition to define the EAP as "an interface on a Cyber Asset that restricts or controls the exchange of data between Cyber Assets within the Electronic Security Perimeter and external Cyber Assets or networks." The ultimate intent to eliminate the requirement for protective controls from certain boundary crossing points can be readily handled through the application of the requirement to "Electronic Access points with External Routable Connectivity", "Associated Electronic Access Control or Monitoring Systems", and the inclusion of dial-up in an applicability reference. (9) The definition of External Connectivity also eliminates the consideration of serial communications. As the use of serial connectivity does not necessarily impede malicious access to a Cyber Asset, it is not appropriate to exclude serial connectivity from the definition. (10) The definition of External Routable Connectivity takes an outside-in only view of network communications. This is overly limiting in that network communication is two-way. Any Cyber Asset that can reach out to an external network has external connectivity and once the outbound connection is made, the external cyber system being reached out to has external connectivity back to the BES Cyber System. If the intent is to eliminate Data Diode controlled (single direction) connectivity from the need for protective controls, clarify the definition accordingly to state that external connectivity is limited to two-way communication. (11) The

definition of Interactive Remote Access can be read to mean that the use of an Intermediate Device sitting outside of the ESP is not Interactive Remote Access and thus anyone going through the Intermediate Device is not subject to the applicable requirements of the Version 5 CIP standards. It would be better if Interactive Remote Access was defined more traditionally and then require the use of the Intermediate Device for any such access. (12) The definition of Intermediate Device states that the device "may be located …" The definition should be modified to clarify that the Intermediate Device must reside outside of the ESP, either as a part of an Electronic Access Point or in a DMZ network. In addition, the definition would be helped by a comment that the Intermediate Device is also subject to certain protective controls of the CIP Version 5 standards even though it resides outside of the ESP. (13) The definition of Protected Cyber Asset defines that Cyber Asset as being connected via a routable protocol. This qualification is not appropriate. It is common for relays and other devices in a substation or generating plant to be serially connected to a communications processor or a serial-to-Ethernet protocol converter module. These devices, if not designated as BES Cyber Systems or BES Cyber Assets, are still reachable and potentially configurable via this non-routable connectivity and need to be included in the definition of Protected Cyber Asset. The type of connectivity is immaterial. (14) The definition of Reportable BES Cyber Security Incident should be reworded to refer to any BES Cyber Security Incident that has "attempted to or successfully" compromised or disrupted a BES Reliability Operating Service. It is important for the ES-ISAC and appropriate governmental agencies to be aware of attempted cyber attacks as part of their intelligence gathering operations. Knowledge of unsuccessful attempts may be the key to preventing a successful attack. (15) The definition of Transient Cyber Asset specifies that the device may be connected for a period of 30 calendar days or less. This is an arbitrary length of time and could afford an entity an opportunity to misuse the definition to their advantage. The definition would be better served by stating that the Transient Cyber Asset is "temporarily connected to a BES Cyber Asset or Protected Cyber Asset for the specific purpose of data transfer, active maintenance, active troubleshooting, or vulnerability assessment, and is promptly disconnected when such activity is complete." The fact that the device is capable of altering a configuration or introducing malicious code is immaterial to the definition and should be removed. In addition, the definition would be helped by a comment that the Transient Cyber Asset is also subject to certain protective controls of the CIP Version 5 standards.

Yes

Comments: (1) A number of criteria qualify with the term "would" adversely impact one or more BES Reliability Operating Services. The criteria should be prospective in nature and should use the term "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. (2) Criterion 1 includes the phrase "and located at." Entities could seize upon this nuance and determine that, for example, a BES Cyber Asset or BES Cyber System housed in a centralized data center and used by a geographically separate control center is not "located" at the control center and therefore is excluded. Either the BES Cyber Asset or BES Cyber System is used to perform the specified BES Reliability Operating Service or it does not. If it does, where the asset is located is immaterial. (3) The High Impact Rating criteria does not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. BES Cyber Assets and BES Cyber Systems that interconnect with similar systems in other Control Centers should be afforded a High Impact Rating regardless of the "span of control" of other BES Cyber Assets and BES Cyber Systems supporting that Control Center. (4) Criterion 1.4 does not consider an aggregate span of control. A generation control system could theoretically control 15,000 MW of generation without a single asset meeting the thresholds defined in the referenced criteria. The overall span of control of the BES Cyber Assets and BES Cyber Systems need to be considered by aggregating the field assets being controlled. (5) Criterion 2.5 is confusing and requires the examples found in the application guideline documentation to understand. The criteria might be improved by stating any part of the cranking path between the black start generation resource and the unit to be started where there is no diversity is designated a Medium Impacting Facility. Additionally, the fact that the black start resource may be used to start multiple units does not mean the "last mile" path to each of the units should be excluded. If the unit must be started as part of initial system restoration as defined in the TOP-005 system restoration plan, the path needs to be protected all the way to the unit. If the plan includes "if-then-else" options (e.g., start unit 1, if cannot start unit 1 then start unit 2, etc.), the first option should be the one protected. (6) Criterion 2.7 specifies a floor of 200 kV. In certain parts of the country, the 200 kV floor is too

high. Within the SPP Region, the transmission backbone is 161 kV. Setting the floor to 100 kV is more appropriate and reflects the current and new definition of the Bulk Electric System (refer to the definition of Bulk Electric System resulting from the work of Project 2010-17).
No
Due to a lack of a specific opportunity to comment on overall issues with the standard, please accept and consider the following comments in addition to comments specific to Requirement R1. (1) Previous versions of the CIP standards are applicable to Transmission Service Providers. CIP Version 5 is not applicable to the TSP function. It is not clear why the TSP function was dropped from the list of Responsible Entities. (2) Exemption 4.2.4.2 should specifically exclude communication end points from the exemption. Addition of this exclusion would be consistent with previous versions of the CIP standards. (3) In the background discussion, a comment is made that malware protection applies to a system as a whole and may not be necessary for every individual device to comply. While the intent to eliminate nonsensical requirements that ultimately require Technical Feasibility Exceptions is reasonable, how is compliance with this requirement determined? As written, an entity could theoretically install network-based malware protection at the network perimeter, ignoring the BES Cyber Assets, and be considered compliant (and protected) under this provision. In reality, network-based anti-malware is only one aspect of malware protection and is completely ineffective for malware not introduced over the network or introduced within a protected network where the configuration of the network allows traffic to pass between Cyber Assets without inspection. (4) Similarly, the grouping of BES Cyber Assets into a BES Cyber System seems to be permitted without any consideration criteria. How will differences of opinion between the entity and the auditor be resolved, or is the auditor obligated to accept any configuration, regardless of how nonsensical the configuration might be? (5) The term "would" adversely impact one or more BES Reliability Operating Services is used in the background discussion. The criteria should be prospective in nature and should use the term "could" adversely impact. Without the criteria being anticipatory, entities could take the stance that the criteria calls for a 15-minute certainty and therefore the criteria in question is not met and the BES Cyber Asset or BES Cyber System is excluded. (6) The Categorization Criteria states that Requirement R1 only requires the discrete identification of BES Cyber Systems and BES Cyber Assets for those in the High and Medium categories. Everything else is considered Low Impact. As discussed in the June 2011 SDT meeting with the regional CIP auditors, the entity will still need to enumerate all BES Cyber Systems and BES Cyber Assets in order to demonstrate the High and Medium BES Cyber Systems and BES Cyber Assets have been properly categorized. (7) The Rationale for R1 refers to "impact." It should refer to "potential impact." (8) R1 specifically states that Low Impact BES Cyber Assets and BES Cyber Systems do not have to be discretely identified. The accompanying Measure M1 states that evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls. This aspect of the requirement renders the overall requirement unauditable. If the entity only has to enumerate the High and Medium Impacting systems, the entity has insufficient evidence to demonstrate all High and Medium Impacting systems have been properly categorized. The entity must be able to demonstrate those systems that default to the Low Impact category are, themselves, properly categorized and should not have been categorized at a higher rating. It is not appropriate to advise the entity in the requirement and accompanying measurement that all assets and systems remaining after the High and Medium Impact categorization are assumed to be properly categorized as Low Impact systems. (9) Requirement R1.1 refers to the intention for the BES Element or Facility to be in service for more than six calendar months. The converse is an element or facility intended to be temporary in nature and in service for less than six months. The entity should be required to document the intent in that instance to allow the auditor the latitude to accept intent over actuality in the case where the BES Element or Facility was in service for more than six months due to unforeseen circumstances.
Yes
The requirement is agreeable with the understanding that "upon the effective date" used throughout the CIP Version 5 standards means "on or shortly before the effective date" and that the entity does not have to perform the initial activity on the precise effective date to be compliant. Read strictly, the use of the term "upon the effective date" could be misconstrued as requiring the action to be performed on that very date.
No
Percentages of non-compliance are difficult to determine; using discrete numbers of non-compliant assets would be preferable in determining the R1 VSL. This is particularly true where random

sampling of the entity's assets is performed and the number of failures is derived by extrapolation. Additionally, the R1 VSLs refer to entities with more than 100 High and Medium Impact BES Cyber Assets (or 100 or fewer such assets). Is this count determined by the entity's determinations prior to the audit or is the count determined by the auditor, adjusting the entity's initial determination upon finding a possible violation? Finally, the standard refers to BES Cyber Systems as well as BES Cyber Assets. It appears that the VSL requires the compliance monitoring and enforcement staff determining the VSL to break down each BES Cyber System into its BES Cyber Asset components in order to achieve the correct determination. As the bright line criteria remove any subjectivity from the categorization process, the R1 VSL should be binary. Either the entity got it right or the entity did not. There should be only one VSL, that being "Severe." Similarly, the R2 requirement is very straightforward and a binary VSL is appropriate in that instance.
No
Although the definition of CIP Senior Manager refers to a single person, this requirement should be clarified that a "single" CIP Senior Manager is to be appointed. The appointment documentation needs to be specific as to its intent to preclude instances where a policy document refers, for example, to the CEO of the company as the Senior Manager and a years-old set of minutes from a Board of Directors meeting naming the CEO serves to complete the "compliant" documentation of the appointment. Additionally, delegations should have the same level of documentation as the Senior Manager. As delegations can be by position or name, why not allow the CIP Senior Manager to be designated by position or name and not specify just the name of the individual. There is a greater likelihood of multiple staff in a large company with the same name and it is less likely that multiple senior staff will have the same company position at the same time.
No
To be auditable, the requirement should specify the minimum level of detail expected. Otherwise, an entity could simply state in the policy, for example, that "we will protect all BES Cyber Systems" and the auditor would have nothing to objectively base a compliance determination upon. The guidance documentation suggests a certain level is desired, however, the auditor must audit to the strict language of the requirement and not to the language in the guidance document.
No
The requirement should be clarified to explicitly require documents (company policies, procedures, etc.) referenced in the CIP cyber security policy(s) to be included in the review and approval actions. Additionally, the suggested evidence in Measure M3 (2) should include electronic approvals as well as a wet ink signatures.
No
This requirement is not auditable as written and is duplicative of CIP-004-5/R2. The suggested evidence in the Measurement section clearly shows the intent of the requirement is that the policy documentation be available to personnel with access to BES Cyber Systems. While it is possible to audit the measurement criteria, the requirement itself requires staff to be "aware" of the policies appropriate to their job responsibilities, not that the policy documents be published in electronic or hardcopy form or the staff be aware of where they might access the documents. The training/awareness issue is already addressed by another requirement. Auditing that the staff is "aware" in this context is not practical. Recognizing the intent is to no longer require a complete set of policies be made readily available to anyone with physical or electronic access, the requirement might be improved by requiring the policy documents be published and that personnel with electronic access to BES Cyber Systems or BES Cyber Assets be advised where they might access the policies if needed. For the small number of staff with physical-only access, the CIP-004-5/R2 training should be all that is required. Similar to current practice, providing a copy of the appropriate policies to contractors and vendors and deeming them to have been appropriately published with a presumption (or a required confirmation from the contractor/vendor company) that contractor/vendor personnel are then told where or how they can access the information should be acceptable. With respect to the Measures, all but the last bullet (training documentation) are appropriate. The measures can be improved by requiring the published documents be maintained up-to-date. There should be no expectation that the published policy documents be customized such that there is a "janitor" bulletin board and a different "SCADA support engineer" bulletin board or Intranet posting.
No
The requirement stipulates that the delegate may be identified by name or position. The first and

third example measures indicate a document listing personnel by title is acceptable evidence. This does not comport with the strict language of the requirement. A title may or may not be the same as the position.
No
Allowing 30 days to document a change to the CIP Senior Manager or a delegate is excessive and unnecessary. Typical practice as demonstrated in past audits is to announce the appointment via documentation with a same or future effective date and the standard should adopt that practice. Past experience has shown that it is difficult to impossible to verify a change was documented within 30 days of the actual appointment, making this aspect of the requirement unauditable. All the 30-day provision allows is for the entity to recover from an improper approval by quickly appointing the signing person as the CIP Senior Manager or delegate, similar to back dating a check.
No
The VRF for R5 (delegations of authority) should be "Medium", the same as the appointment of the CIP Senior Manager. The VRF for R6 (change in leadership or delegation) should also be "Medium" since the documentation of a change carries the same importance and impact as the original appointment. The binary VSL for R1 includes language ("single senior management official") not currently found in the requirement itself. The VSLs for R3 do not include the conditions where the policy documents were approved without any evidence of review and where some but not all of the policy documents were reviewed prior to approval.
No
Part 1.1 is vague and leaves the program entirely up to the entity with minimal guidance. As such, the auditor is left with only verifying that the entity did something each quarter, whether meaningful or not. The requirement now removes the expectation to reach the personnel with access to the protected systems, further weakening the requirement to the point of adding no value to the security program. Part 1.1 would be greatly improved if there was a requirement to reinforce the cyber security policy and to demonstrate that the awareness materials were accessible to personnel with access (e.g., placement of posters, means and locations of publishing electronic security awareness information).
No
The main requirement statement specifies that the entity will now have a role-based training program. This is a stronger statement than previous versions of the standard and could be construed as no longer permitting a common training program for all personnel. This will require entities to customize training to individuals or classes of personnel with access. For example, the operators will need different training from the software engineers who might, in turn, need different training from system administrators and supervisory personnel. Parts 2.1 through 2.10 should be applicable to Associated Physical and Electronic Access Control and Monitoring Systems and Associated Protected Cyber Assets. The reason for this recommendation is that Requirement R3, which implements the R2 training program, is applicable to the associated systems. The requirement to develop a training program should be applicable to the same Cyber Assets as the requirement to conduct such training. Part 2.1 should require the defined roles to be mapped to the training topic areas defined in Parts 2.2 through 2.10, otherwise, the accompanying measure stipulates evidence not required by the language of the requirement. Part 2.2 should stipulate whether the training on security controls is for physical controls, electronic controls, or both. Because of the requirement for role-based training, it may be necessary to split Part 2.2 into two parts, one for physical security controls and one for electronic security controls. Part 2.7 should emphasize that training should cover the identification of any potential BES Cyber Security Incident and not only those that would be deemed to be reportable.
Yes
No
Parts 4.1 through 4.4 should be applicable to Associated Physical and Electronic Access Control and Monitoring Systems and should be considered for Associated Protected Cyber Assets. The wording of Part 4.1 states an "initial" personnel risk assessment is required that includes identity verification. Part 4.2 does not include a similar reference to "initial" making it unclear whether both elements are required initially and then every seven years thereafter. Part 4.1 calls for identity verification but does not define any minimum expectations as to what identity verification entails. Would it be acceptable, for example, to accept a library card as proof of identity? The US Government has identified through

the use of the DHS I-9 form and instructions a number of identity artifacts that can be presented to confirm identity. The Canadian and presumably the Mexican governments have similar defined expectations that were used in the development of an interpretation request. Those government-accepted proof-of-identification documents should be stated as appropriate for the purposes of this requirement. Part 4.2 prescribes that the background check must be conducted for all locations where the individual has resided, been employed, and/or attended school for six months or more. This requirement should be clarified that "employed" or "resided" includes those locations where a long-term (six-month or longer) onsite contract engagement was performed. Part 4.3 requires criteria or a process to be used to evaluate the personnel risk assessment results to determine if access is to be denied. This requirement is vague and begs the question: would "to be determined on a case-by-case basis" be sufficient to demonstrate compliance? Part 4.4 is similarly vague. Is the entity now required to perform the personnel risk assessment on the contractor/vendor staff? Does the entity have to formally approve the contractor/vendor's program? Does the entity have to see the results of the personnel risk assessment performed by the contractor/vendor, which may be contrary to state laws and company policies? Does the verification process include evaluation of the contractor/vendor's disqualification criteria and that the criteria were properly applied in all instances?

No

The measures for Part 5.1 should include documentation of the CIP Exceptional Circumstances in the event access is granted before a personnel risk assessment is performed. Allowing the personnel risk assessment to be updated every seven "calendar" years could permit the entity to go as long as nearly eight years between assessments. There is no reason an entity cannot plan ahead and renew a personnel risk assessment on or before the seventh anniversary of the current assessment. The requirement should be modified to require the renewal on or before the seventh anniversary. Additionally, the Evidence Retention section should be modified to prescribe that personnel risk assessment documentation shall be retained at least until completion of the first compliance audit following the expiration or renewal of the personnel risk assessment.

No

The rationale for R6 states that the requirement of CIP-004-4/R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access. From an audit perspective, the entity still needs to be able to demonstrate that everyone with access is known and accounted for. During an audit, the entity will be required to produce a list of every individual with electronic and/or unescorted physical access for sampling purposes and will be required to demonstrate that list is complete in all respects, including that the access and associated access rights were properly authorized. How the entity maintains or creates the list is up to the entity. The rationale section should be updated to make that expectation clear to the reader. The second example evidence defined in the Measures for Part 6.1 prescribes a signed document, workflow or email showing such persons have authorization. Any such authorization documentation needs to include the specific access rights that were authorized. Part 6.4 states that the entity must verify each calendar quarter that individuals provisioned for access were authorized for such access. This can still be interpreted as requiring a review of access rights to ensure the granted access rights were properly authorized. This does not appear to comport with the rationale statement where the quarterly review appears to be simply a review of individuals with access without regard to the actual access rights granted. Similarly, Part 6.5 requires an annual verification that all accounts/account groups or role categories and their specific associated privileges are correct and the minimum necessary for performing work functions. It is not clear from this statement if there is a requirement to verify individual personnel are properly granted such access to those accounts/groups/roles as opposed to verifying the rights on those accounts/groups/roles are correct. The same confusion exists with Part 6.6. It is not clear if this part requires verification that individuals have the proper access rights versus the access rights are properly defined or configured. The Measures for Parts 6.4, 6.5, and 6.6 do not always align with the language of the respective part requirements. The various parts of R6 need to be clarified to explicitly state when individual grants to access rights are to be verified and when access rights are to be verified as properly defined or configured without regard to individuals holding such access.

No

Part 7.1 should specify that physical, domain, and remote access is to be revoked at the time of termination. Domain access is currently missing. Revoking domain access, especially within the control center environment, is not a difficult task and helps ensure that should the terminated staff

gain network access, the individual cannot log onto the network or system. Part 7.2 needs to explicitly allow for an overlap transition period for transferred personnel. The losing and gaining managers should collaboratively determine an effective or "agreed to" date whereby prior access will no longer be required and is to be revoked. In the absence of this agreed to date, the auditor can only rely upon the effective date of the transfer as recorded by an HR personnel transaction, putting the entity at risk of a possible violation for failure to revoke access timely. Part 7.4 needs to be clarified to explicitly include application and database accounts. As written, the reader could inadvertently assume the requirement only pertains to domain and local operating system-level user accounts. Part 7.5 requires shared account passwords to be changed within 30 calendar days. This is excessive for any account in a control center environment and especially excessive and risky for shared accounts that are highly privileged (e.g., system administration accounts). The recommendation is to change the shared user account within the same calendar day for highly privileged accounts and within seven calendar days for lesser-privileged and field asset accounts. There is already a provision for extenuating circumstances to be applied if a much shorter time frame cannot be complied with (e.g., access passwords on relays and other BES Cyber Assets in field environments). Should there be extenuating circumstances, a completion date certain should be included in the extenuating circumstances documentation and passwords should be changed on or before the documented date. Allowing an additional ten calendar days is not necessary and without a date certain when the passwords will be changed, the entity could unnecessarily prolong the required activity for convenience. Additionally, the application guideline for Requirement R7 states that no action is required in the instance of the death of the access holder. While "immediate" action might not be required, access still needs to be revoked sooner rather than later. Also, the application guideline for Requirement R7 states "For transferred or reassigned individuals, the requirement states a review of access privileges must be performed." Parts 7.2 and 7.5 of the requirement imply, but do not explicitly state such a review is required. Additionally, the requirement needs to address the revocation of access to BES Cyber Security Information associated with the transfer of reassignment of personnel. Part 7.3 only applies to resignations and terminations, and Part 7.5 (which applies to transfers) only addresses the need to change the passwords for shared user accounts.

No

Because of the risk in not promptly revoking access, the VRF for R6 should be Medium. The High VSL for R4 refers to "required documented results" and to Part 4.5. The documented results are a requirement of R5 and there is no Part 4.5. The Severe VSL for R6 refers to Part 6.7. There is no Part 6.7.

No

The requirement no longer requires the entity to discover previously unidentified electronic access points. This opens a potential risk point that needs to be addressed. It may be possible to accomplish this task as part of defining the system baseline configuration (CIP-010-1/R1), but the task needs to be explicitly required. Part 1.1 requires technical or procedural controls to "restrict" unauthorized electronic access. The intent of the term "restrict" needs to be explained. Part 1.1 and Part 1.2 potentially conflict if both types of systems are collocated on the same network. The requirement needs to assert Part 1.2 prevails in the instance of a mixed categorization environment. Part 1.4 is applicable to dial-up access for "non-interactive" Remote Access. The requirement to perform access authentication for non-interactive access and not also for interactive access appears to be nonsensical. It is not clear what the real intent of this requirement is. Part 1.5 requires a documented method for detecting malicious communications at each EAP. Malicious communications needs to be defined. Additionally, the requirement may be too narrowly focused. Detection of malicious communication can often be detected via Intrusion Detection/Prevention systems running outside of the EAP. The change rationale for Part 1.5 states that ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured, and that Part 1.5 is an attempt to address that need. Part 1.5 fails in this endeavor in that Intrusion Detection Systems are detection systems and not protection systems. To achieve the expectations of the FERC Order paragraphs cited in the rationale, an Intrusion Protection System would be required.

No

Part 2.2 requires encryption for all Interactive Remote Access sessions. This is problematic if the terminus of the encrypted session is inside the ESP since packet inspection at the ESP border is not possible. It also makes little sense to require encrypted Remote Access sessions but not require encryption anywhere else, such as communications between systems in different ESPs (e.g., primary-

backup control centers, ICCP traffic between control centers).
No
The Severe VSL for Requirement R1 needs to be specific as to which systems are in focus of the first condition. Perhaps a Part number reference would be appropriate as has been used elsewhere in the VSLs for other standards.
No
Part 1.2 suffers from an insufficiently defined term "Defined Physical Boundary" (See the comments in response to Question 1, item 7). Part 1.3 requires the use of two or more "different and complementary physical access controls." This needs to be defined or at least the intent clarified. FERC's intent, as stated in Paragraphs 572 through 576, is to implement defense in depth such that the Cyber Systems and Cyber Assets continue to be protected in the event one of the control systems fails. The Application Guideline for Requirement R1 offers examples of compliant applications that include "card key and pin code" and "card key and biometric scanner." These examples fail if the two-factor authentication is managed by the same Physical Access Control System. The failure of that system would result in the simultaneous failure of both controls. A compliant application of this requirement might be a card key/magnetic lock or door strike system with a logged and alarmed key override system. The failure of the primary Physical Access Control System would keep the door locked and the key override system would provide access. The key override system, being alarmed and logged, continues to provide protection by providing immediate alerting in the event the key override is used. Part 1.6 is too restrictive in requiring logging by personnel who control entry when automated means are not used. This implies security personnel whose primary responsibility is to control physical access and would not necessarily include escorting personnel. It would be better to require manual or electronic logging of access without restricting the logging to security personnel. Additionally, the date and time of access should be recorded and not just the date of access in support of CIP-006-5/R2.
No
Part 2.1 should prescribe "Require 'and perform' continuous escorted access…" Part 2.2 is confusing and unnecessarily broad. Basing the requirement on a 24-hour basis could also lead to inadvertent logging failures. It would be better for the requirement to permit the logging of initial ingress and final egress and permit brief exit/reentry as long as the time between the exit and reentry does not exceed a prescribed time period. The intent would be for someone to be able to run out to their truck as discussed in the Application Guideline without having to log out and right back in. However, leaving for lunch, to pick up a part, or other prolonged period between the exit and reentry should be logged out and back in. The suggestion is to log the visitor out and back in if the visitor is out of the DPB for more than 15 or 30 minutes and to not consider a visitor to have exited a DPB when traversing through successively layered perimeters (e.g., having to go through the control room DPB to enter the computer room, a separate DPB.
No
Maintenance and testing of Physical Access Control Systems can and should be performed far more frequently than once every 24 calendar months within routinely occupied facilities such as the primary control center. The suggestion is to require monthly testing in routinely occupied facilities. Part 3.1 specifies that the Physical Access Control System must be tested prior to commissioning and at least once every calendar 24 months thereafter. The requirement also needs to require that testing of the controls needs to be performed on or before the effective date of the CIP Version 5 standards to avoid the "book marking" issues seen with previous versions of the CIP standards.
No
The second condition of the High VSL for Requirement R1 includes the failure to initiate a response within 15 minutes of a detected unauthorized physical access. The 15 minute criterion is not specified in the language of the requirement itself. This condition also references Part 1.6, which does not appear to be correct. Part 1.4 is more applicable to this condition.
No
Part 1.2 should also be applicable to Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems.
No
Part 2.1 permits the entity to choose one or more sources for monitoring the availability of security

patches. The Change Rationale indicates that this could include the SCADA system vendor that "certifies" a patch before the entity can install it. There is a difference between "availability/applicability" of a patch and the ability to "install" a patch. The risk begins when the vulnerability is identified and may or may not coincide with the initial availability of a patch from the source vendor. There are a number of patch consolidation sources in addition to original patch providers that can be monitored. Allowing the entity to rely upon the SCADA or other vendor to "certify" a patch before it is considered available is an unnecessary delay and increases the risk to the reliability of the BES. If the vendor, for example, does not certify a patch for several years (if at all), the entity under this process has no expectation of addressing the vulnerability at all. As demonstrated by past history, the majority of cyber systems infected with malware are compromised because an available security patch was not installed. The certification, accompanied by the entity's own testing, determines if the patch can be installed. Regardless, the patch is applicable and available and compensating measures need to be adopted to address the vulnerability in the event the patch cannot be installed. The current practice of some vendors is to only report out "certified" patches against the current baseline product, which means some available and applicable, perhaps not installable patches will be overlooked. The requirement would be better if the entity was required to monitor the availability of a patch from the original provider, either by monitoring that vendor's site or by use of a vendor-agnostic patch monitoring service. The entity should only rely upon the application vendor if that vendor customizes and re-releases the security patch originally provided by a different vendor. Once the patch has been identified as available and determined to be applicable, the entity can and should wait for their application system vendor to certify the patch as compatible with their system. Part 2.3 needs to specify a remediation time frame where the patch is implemented or compensating measures are implemented pending the installation of the patch. The vague wording of this requirement would allow, for example, an entity to define a remediation process whereby the security patches are only installed as part of a system replacement once every several years. The suggested remediation timeframe is 30 calendar days after a patch is determined to be applicable for BES Cyber Systems in a control center and the next scheduled outage for plants and substations, with a requirement to implement compensating measures in lieu of the patch within 30 days of the patch availability whenever possible in the plants and substations. The provision for CIP Exceptional Circumstances can address the outlier issues.

No

This requirement needs to adopt and use common terminology, either the already defined term "Transient Cyber Assets" or the currently undefined term "Maintenance Cyber Assets." The term "Maintenance Cyber Assets" is used in the Rationale for Requirement R3. The vagueness of Part 3.1 could result in either a very subjective audit or potentially ineffective "compliance." For example, is the deployed method appropriate for the system to be protected? Is a perimeter-based solution, such as a network-based anti-virus or Network Intrusion Detection/Prevention System sufficient? Part 3.2 needs to define a timeframe in which malicious code is to be disarmed or removed. As written, the entity could effectively ignore the malware, citing a future plan or process to perform the required disinfection. Part 3.3 specifies malicious code protections shall be updated within 30 calendar days of the signature or pattern update. This is excessive, especially in a control center environment, where such updates are frequently provided by the anti-malware vendor in response to emerging threats. The signature files can typically be downloaded, tested, and rolled out to production within a couple of days of the release of the update. This requirement also suffers from the elimination of the requirement to "test" the update before rolling it out into production, although the Application Guideline for R3 still refers to testing prior to implementation. Past experience has demonstrated that anti-malware updates occasionally return a false-positive and have crippled systems in the past as a result of the automated response of the anti-malware system to the "detected" problem. Part 3.4 needs to be modified to require methods to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media "prior" to connecting them to BES Cyber Assets or Protected Cyber Systems. The goal is to prevent plugging in a device already compromised with malware. Part 3.5 should be modified to log both the connection and the removal of the Transient Cyber Asset. Logging the removal demonstrates the transient nature of the connection.

No

Part 4.1 requires the entity to log generated events. The Measures should include evidence that the logs are being generated with the appropriate information. Having a listing of what is to be logged is not the same as demonstrating the logs are being generated. Part 4.2 implies an automated system is

required in order to generate "real-time alerts." Allowing the entity to determine what it feels are required real-time alerts, with no minimum set of expectations, is a meaningless requirement. The auditor will either perform a highly subjective audit, or the auditor will be obligated to accept whatever the entity has determined, even if the entity has determined that there is no need for any real-time alerting. The Measures accompanying Part 4.2 should also include examples of actual alerts demonstrating the monitoring system is properly configured and operating. Part 4.4 Measures suggest that records of disposition of security related event logs are required. The requirement is to maintain logs for the past 90 calendar days and the auditor will only seek evidence that the entity has at least 90 days worth of logs. Maintenance of disposition records does not directly support the language of the requirement. Part 4.5 permits sampling of logged events in lieu of a 100 percent manual or automated review. This is impractical for firewalls and other high-volume logging systems. The intent of the FERC order was to require a periodic manual review to confirm the automated Security Incident and Event Monitoring (SIEM) system was properly configured and not overlooking events of interest. A manual process where automation can be deployed increases the risk to the BES reliability. Additionally, should the sampling continue to be permitted as currently drafted, the requirement needs to define a minimum expectation as to sample size and procedure. Otherwise, the entity will have the latitude to devise a meaningless and insufficient review for convenience.

No

Part 5.4 permits a default password to not be changed if "the default password is unique to the device or instance of the application." This provision is nonsensical. Passwords need to be changed on a regular basis as mitigation from possible inadvertent disclosure or discovery. And, technically, whoever set the initial password has knowledge of that password and thus access. Unless that individual is approved for access, the password needs to be changed to revoke the unauthorized access. Additionally, disabling or renaming system default accounts such as Guest and Administrator is good security practice and should continue to be required where appropriate and applicable. Part 5.5 already requires passwords to be regularly changed. Unconditionally requiring a default password to be changed prior to placing a system into service is good security practice and also affords the entity the opportunity to clearly understand and document the necessary procedure for changing the password on the device. Part 5.5.3 has removed the requirement to change the password at least annually and now permits the entity to specify its own time frame. This is a very vague requirement and will result in either a highly subjective audit or an obligation of the auditor to accept whatever the entity has defined, regardless of how nonsensical that time frame might be. The "where technically feasible" language has been removed, yet there may be instances where a password cannot be changed for valid technical reasons. The drafting team should consider restoring the technical feasibility provision. The VSL for this requirement already includes TFE language. Additionally, the measures for Part 5.5 include attestations that procedurally enforced passwords meet the password parameters. This is problematic to auditors as GAGAS does not permit the acceptance of attestations as primary evidence. Part 5.6 requires a failed password lockout or alert notification after an undefined number of failed attempts. The requirement needs to specify what is reasonable, perhaps with options including number of consecutive failed attempts and elapsed time before automatic lockout expiration.

No

Because of the risk, Requirement R2 should have a High VRF. The High VSL for Requirement R3 is essentially the same as the first condition of the Severe VSL, with the exception of applicability to Transient Cyber Assets. The Moderate and High VSLs for Requirement R4 are run-on statements that lose the required context. The last condition of the Severe VSL for Requirement R4 should include the specific requirements stipulated in Part 4.1. The Severe VSL for Requirement R5 should include conditions for where the account use was not authorized by the CIP Senior Manager or delegate (Part 5.2).

No

Identifying criteria for reportable Cyber Security Incidents per CIP-008/R1.3 has been very inconsistent across entities to date. Part 1.2 does nothing to address this inconsistency because, like previous versions of the CIP standards, this requirement does not establish minimum expectations or criteria for reporting. Additionally, Part 1.2 has dropped the requirement to ensure reportable incidents are reported to the ES-ISAC. This requirement can be improved by restoring the requirement to report the incident and by providing minimum expectations for what is considered reportable.

No
The requirement statement in Part 2.1 is awkwardly worded and confusing. The requirement can be broken into two expectations: (1) follow the documented Incident Response Plan in the event of a BES Cyber Security Incident or plan test, and (2) Document the execution of the plan and any deviations from the plan during the response for future evaluation and possible plan update. Part 2.3 should require the entity to retain "all" relevant documentation. The accompanying Measure should provide examples of documentation, such as logs, police reports, e-mails, phone logs, voice recordings, response team member notes, response checklists, forensic analysis results, restoration records, and post-incident review notes.
No
Part 3.1 requires an update, if necessary, following the annual review of the BES Cyber Security Incident response plan. If the entity has properly complied with the requirements of Parts 3.3 and 3.4, the need for an update following the annual review should be negligible. To be compatible with the currently in effect CIP-008 and CIP-009 standards, Parts 3.2 through 3.5 should be applicable to Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems. Part 3.3 should be modified to require the update to be completed within 30 calendar days of completion of the annual review, test, or actual incident response. The current wording requires an update within 60 calendar days and only requires the update following the annual review. Part 3.5 allows 30 calendar days to distribute the updated BES Cyber Security Incident response plan to each person with a defined role in the response plan. Thirty calendar days is excessive. A seven calendar day period is suggested.
No
The High and Severe VSLs for R3 do not reflect relative significance of the documented failures. Failure to update a plan, whether or not reviewed, should be a Severe VSL. Updating the plan but not distributing the plan timely should be High, not Severe.
No
Part 1.1 only requires the conditions for activating the recovery plan(s) to be documented. In the absence of setting minimum expectations, an entity could define a recovery plan that is only activated in the event of a catastrophic destruction of all control centers (primary, backup, etc.) and be found compliant. The recovery plans need to address (1) single BES Cyber System/Asset failure, (2) combined failure of the primary and backup BES Cyber Systems/Assets at one location, (3) the combined failure of the primary and backup BES Cyber Systems/Assets at more than one location, (4) the loss of multiple BES Cyber Systems/Assets at one or more locations, and (5) the catastrophic loss of one or more facilities with accompanying loss of the BES Cyber Systems/Assets at those locations. Part 1.1 also does not require the entity to document the recovery plan steps themselves, which should be the most important requirement of any documented recovery plan. A documented recovery plan with recovery steps is required to perform the requirement specified in CIP-009-5/R2. Part 1.4 requires the backup media to be "verified." The requirement needs to specify what verification entails. Does verification simply entail looking at a log file to confirm the backup process did not fail? Does it involve performing the verification option step as part of the backup process? Does it require a separate step for cataloging the backup media to verify the media can be successfully read end-to-end? Or does it include steps to confirm all information required to successfully restore a system has been captured?
No
Part 2.2 requires the entity to initially and annually thereafter "test" any information used in recovery of BES Cyber Systems that is stored on backup media to ensure the information is usable and "reflects current configurations." Similar to the comments submitted against CIP-009-5, Requirement R1, Part 1.4, what does "test" mean? Does it simply require a step for cataloging the backup media to verify the media can be successfully read end-to-end? Does it include steps to confirm all information required to successfully restore a system has been captured? Or does it require a full restoration of the BES Cyber System from the media? What is meant by reflecting current configurations? And, most importantly, does each media set require testing (e.g., test after every backup cycle)? If not, what are the parameters for demonstrating compliance with this requirement? Part 2.2 needs to be significantly clarified before entities fully understand the requirement and auditors know how to evaluate compliance. Part 2.3 requires an operational exercise of each of the recovery plans initially and then every three years thereafter. Must every Cyber Asset or type of Cyber Asset be tested?

What if the recovery plan is generic and broadly stated? How many Cyber Assets need to be "restored" to adequately demonstrate the adequacy and completeness of the recovery plan?
No
Part 3.1 requires the recovery plan to be reviewed when BES Cyber Systems are replaced. In addition to replacement, the recovery plan should be reviewed following a major update of the BES Cyber System (e.g., hardware component addition or upgrade, network connection update, or major software revision level upgrade). A major update is less than a replacement, but could still change the system sufficiently to require modifications to the recovery plan. Part 3.3 requires recovery plans to be updated within 30 days of the review of the results from a recovery plan test required by Part 3.2. This requirement should also require recovery plans to be updated within 30 days of the plan review required by Part 3.1, if changes were identified.
No
The second condition of the High VSL for R2 (testing the recovery plan at least once every three years) should be a Severe VSL.
No
Part 1.1 should include an additional requirement (1.1.7) to document the cyber security (system hardening) controls. This is more than simply the configuration of ports and services already required. Part 1.2 needs to provide for both routine, planned changes where documentation and approvals can be obtained prior to implementing the change and for emergency (it is 2:00 AM and the system is down, must be fixed now) changes where documentation and approvals are taken care of after the fact. As currently written, the requirement could be interpreted as requiring documentation and approvals prior to any change implementation. Emergency changes as discussed in this comment do not fall into the CIP Exceptional Circumstances exemption. The prior version reference for Requirement R1 (all parts) should be CIP-007-4 to be consistent with the rest of the standards.
Yes
No
Parts 3.1, 3.2, and 3.3 need to define what a paper and an active vulnerability assessment is. The Application Guideline attempts to define these types of assessments; however the auditor cannot audit to the language of the guideline. The expectation needs to be clearly defined in the requirement itself. Part 3.3 should require an active vulnerability assessment prior to placing a new BES Cyber Asset, new BES Cyber System, new Physical Access Control System, or new Electronic Access Control or Monitoring System into service as well as adding a new BES Cyber Asset to an existing BES Cyber System or Electronic Access Control or Monitoring System as currently prescribed in the requirement. Part 3.4 requires an action plan to remediate or mitigate vulnerabilities identified in an assessment and the execution status of the action plan. To date, entities have struggled with understanding what this requirement entails. The requirement needs to clarify that the action plan needs to have measurable milestones similar to a mitigation plan associated with a compliance violation. The requirement should also require the execution status of the action plan to be updated/reported at least quarterly.
No
The VRFs for Requirements R1 and R2 should be Medium, not Lower. The third condition of the High VSL for R1 should be Severe, not High. The graduated VSL conditions (performance of the vulnerability assessment) should be combined and set as a High VSL. The failure to perform a required Part 3.1 or Part 3.2 vulnerability assessment prior to the effective date of the standard and the failure to perform a Part 3.3 vulnerability assessment prior to placing a new BES Cyber System or BES Cyber Asset into service should be Severe VSLs.
No
The requirement statement in Part 1.1 is too vague. To be auditable, the requirement needs to prescribe the definition of measurable criteria for identifying BES Cyber System Information. Additionally, the accompanying measures may demonstrate the outcome of the application of the prescribed identification methods, but the suggested measures do not directly support the requirement itself. Part 1.3 requires the entity to implement an action plan to remediate deficiencies identified during the assessment required by Part 1.3. The requirement needs to clarify that the action plan needs to have measurable milestones similar to a mitigation plan associated with a

compliance violation. The requirement should also require a quarterly update/report of the execution status of the mitigation plan.
No
Parts 2.1 and 2.2 need to require the documentation of the process steps comprising the action taken to destroy the media (required by Part 2.2) or to prevent the unauthorized retrieval of BES Cyber System Information from the media (required by Parts 2.1 and 2.2). To be consistent with the VSL conditions for Requirement R2, the requirement also needs to prescribe documentation of the media purge or destruction activity. Additionally, the requirement should prescribe that the media will be physically protected from unauthorized access until such time as the media is purged or destroyed, even if the media or the Cyber Asset housing the media has been taken out of service.
No
The High VSL for R2 covers the instance where the documented purge or destruction process was not followed. If the entity cannot demonstrate that the documented process was ever followed, the VSL should be Severe. High is only applicable if the procedures were followed for some, but not all purge or destruction actions.
No
In the Scenario of Unplanned Changes table, the last scenario (add 12 months to the above) should be simplified to state 24 months. The last paragraph of the Implementation Plan states "following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved." What is the time frame whereby the entity is expected to either demonstrate full compliance or file a self-report of non-compliance?
Individual
Shari Heino
Brazos Electric Power Cooperative, Inc.
Yes
Add a definition for Interactive Remote Access. Control Center should probably be defined just for CIP-002 or just for the CIP standards.
Yes
The standard should clearly identify who has authority to determine the level of granularity of systems identified. BEPC is concerned that the standard as drafted would allow an auditor to second guess its designation of systems and how they are protected. For Attachment 1, CIP-002: A GOP Control Center could end up being treated as High Impact after being run through the analysis of Section 2.1 and then 1.4 depending on how those sections are interpreted. A GOP Control Center should not be High Impact merely because it represents 1500MW or more. Section 2.13 wording problem first part of sentence does not grammatically fit with (2). Section 2.5, In ERCOT, black start units change every two years pursuant to a competitive selection process; therefore, black start cranking paths change every two years. This will lead to much expense and effort on the part of TOs for something that may only have a medium impact designation for two years (and, given the implementation plan, may only be compliant for one). Additionally, “initial switching requirements” is unclear.
No
See ACES Power Marking comments (joined by Brazos).
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No

See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
Role based training is acceptable; however, companies should not be prohibited from overtraining employees. It is sometimes simpler to train employees all together rather than create and schedule several different trainings.
No
See ACES comments.
No
See ACES comments.
No
Because of other legal requirements, it should be made clear that registered entities will not be required to hand over PRAs from third parties to auditors.
No
Segregation of duties might not be possible in smaller organizations.
No
See ACES comments. Also, under Measures #(ii), requiring a print of a system generated list every time there is a termination would be onerous. Next calendar day is not always reasonable because HR will often do terminations at 5pm on Friday; use next business day.
No
See ACES comments.
No
In the Measures for 1.1, change “and” to “or” (technical or procedural instead of technical and procedure).
No
See ACES comments.
No
See ACES comments. Also, the guidelines for R2 should be moved to the standard itself for clarity.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also, provide an exception in 1.1 for software’s use of dynamic ports (e.g., any answering port).
No
For 2.1, clarify that sources that registered entity chose to use are acceptable. The entity is not required to use a source identified by auditor.

No
See ACES comments. Also, for 5.6, account lockout is a bad idea; alerting is a better option. Account lockout can be used to institute a denial of service to legitimate users.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also: For 1.4: Define what is meant by “verified.” This could be an onerous process. For 1.5: This requirement should modified to only require data preservation where it does not cause additional system down time. Time limit of preservation of data should also be limited.
No
See ACES comments. Also, For 2.2: Remove the word “any” – this is overly broad. For 2.3: This requirement is too onerous. Testing in a test environment is very expensive. Generally, provide more clarification about the amount of testing to be performed (entire system?).
No
See ACES comments.
No
See ACES comments.
No
See ACES comments. Also: For 1.1.4 and 1.1.6: It is excessive to require a new baseline after every script or security patch. For 1.2: Change control already handles this process. It should not require CIP Senior Manager approval.
No
See ACES comments. Also, for 3.2, performing a vulnerability assessment in a test environment will provide little information of value. An assessment in the production environment should be allowed as well. Production environment assessments provide more useful information.
No
See ACES comments.
No
Clarify in the requirement itself that marking is not required for BES Cyber System Information information; only that the information is recognized as such. Some information is not in a format that allows easy marking of the information.
No
No
See ACES comments. ALSO, Brazos has some general concerns about the version 5 drafts as listed below: (1) Because guideline documents are not binding on auditors, guidelines should be part of standard if important. Guidance documents are also a hassle because they are one more place we have to look to find information. (2) Clarify that evidence lists in measures do not require an entity to have all types of evidence listed. (3) Where retention period is less than audit cycle, provide examples of alternative evidence other than actual logs, etc. that would demonstrate compliance for the entire

audit period. (4) Some requirements appeared to drop the 90 day logging requirements, possibly unintentionally. These time limits should be reinstated where appropriate.
Group
Progress Energy
James Eckelkamp
Yes
Agree with EEI comments for this question
Yes
Agree with EEI comments for this question and addition have this comment for section 2.4. The diverse and distributed nature of the Bulk Electric System necessitates a design that allows for multiple sources to restart the electric system in the event of a blackout. Due to the multiple combinations of restoration paths, selecting an initial path for system restoration from selected blackstart units would be more feasible in the development of a restoration plan with the flexibility of choosing other restoration paths in the absence of the initially designed restoration path. This does not preclude the need for additional blackstart capable units, but allows for reasonable protection of specific assets for system restoration without placing undue burden on protecting all blackstart assets. Proposed: We would recommend the critical asset definition as it pertains to blackstart units remain limited to those blackstart resources in the electrical path of transmission lines used for initial system restoration.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
R4.2 Requirement should be effective on or after the effective date of the standard and not retroactive for personnel processed under previous revisions of the standard since this interpretation expands the scope of the PRA to include checks where the person was employed or attended school for six months or more.
Yes

No
Agree with EEI comments for this question with addition to: R6.4 –We had concern over the wording “calendar quarter”. Comment: define quarter; or + or – 30 days on quarterly measurement. R6.5 Original content: Verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all accounts/account groups or role categories and their specific, associated privileges are correct and the minimum necessary for performing assigned work functions. Proposed content: The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question with the addition of the following change: Table 1.1 Change “and “ to “or” under Measures.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question with these additional comments: Original content: Severe The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions. Proposed content: Lower The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 1-30% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 1-30% of Interactive Remote Access sessions. Moderate The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 31-60% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 31-60% of Interactive Remote Access sessions. High The Responsible Entity did not implement encryption to protect the confidentiality and integrity for 61-90% of Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for 61-90% of Interactive Remote Access sessions. Severe The Responsible Entity did not implement encryption to protect the confidentiality and integrity of all Interactive Remote Access sessions OR The Responsible Entity did not implement multifactor authentication for all Interactive Remote Access sessions.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question 5.2 Evidence Retention Under CIP-006-5 Section C (Compliance) 5.2 it states that each entity shall retain data or evidence for three calendar years or the duration of any regional Compliance Enforcement Authority investigation; whichever is longer. Comment: Version 5 evidence retention criteria goes beyond retention requirements of the current standard. Propose that the legacy evidence retention requirements for CIP-006 remain intact. Extending retention requirements will significantly increase administrative burden and costs with no added value. • Access logs (manual and/or electronic) retained for a period of 90 days (unless related to a reportable cyber security incident) • Outage records regarding access controls, logging, and monitoring for a minimum of one year (unless related to a reportable cyber security incident)
No
Agree with EEI comments for this question with additional comment Table 3.1 Original Text: Prior to commissioning, and at least once every 24 calendar months thereafter, maintenance and testing of the Physical Access Control Systems and locally mounted hardware or devices at the Defined Physical Boundary to ensure the required functionality is being provided. Propose: After the effective date or prior to commissioning Physical Access Control System(s) used at a Defined Physical Boundary shall be tested at least once every 24 calendar months thereafter to ensure required alerting and control

functionality is provided. Entity shall provide maintenance as necessary to support Physical Access Control System(s) functionality. Rationale: This sub requirement cites maintenance and testing to be conducted “prior to commissioning.” In many instances controls may already be in place or will be expected to be in place prior to V5 adoption, therefore language is needed to capture existing devices in service at the time the standard becomes effective.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question – but has this additional comment in the compliance section under 1.2 first bullet: Original content: Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer. Proposed content: Each Responsible Entity shall retain data or evidence for 1 year or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
Yes
No
Agree with EEI comments for this question

No
Agree with EEI comments for this question
No
Agree with EEI comments for this question
No
Agree with EEI comments for this question with the additional sentences on the first paragraph in the comment section. The existing time frame of 18 months is seen as too short, given the extensive enhancements within the standards as a whole, and particularly specific to the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions. In the event that Low Impact assets are a component of the enforceable requirements on day 1 it is likely that additional time would be required. We recommend a timeframe of no less than 24 months for high, medium, EACM's, PACM's systems or assets and more time required for low Impact BES Cyber Systems as scope in unclear at this point.
Individual
Joe Tarantino
Sacramento Municipal Utility District
No
• The term "BES Reliability Operating Services" in the definitions includes language that result in unintended over-reach in the standard. Specifically, the language "activities, actions, and conditions" is used in the definition of many services. This language may be interpreted to mean that the cyber assets used to control the climate control system of the control room in which the operator performs his or her duties is subject to regulatory compliance. Therefore, the language needs to be changed so that the reference is only to cyber assets that directly implement the services listed in "BES Reliability Operating Services".
No
• This requirement requires the responsible entity to identify and categorize its "BES Cyber Assets" and "BES Cyber Systems" by impact level according to the criteria defined in Attachment I. The criteria in Appendix I, in turn, refers to the impact based upon adverse impact to one or more "BES Reliability Operating Services". The term "BES Reliability Operating Services" is so broad that it essentially covers everything that a utility does. There is nothing left to not include. • The definition of "BES Cyber Asset" in the CIP Version 5 definitions qualifies "BES Cyber Assets" based upon the 15 minute criterion. In Attachment I, in the definition of the High and Medium impact levels, the term "BES Cyber Asset" is used in conjunction with the 15 minute criterion. This is logically inconsistent because the term "BES Cyber Asset" does not include assets that have already been excluded by the 15 minute criterion. • The 15 minute criterion does not apply to the vast majority of systems covered by the standard because power system apparatus and computer systems generally operate in the time frame of five seconds or less. • Throughout the Application Guidelines language includes the following statements "Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions." For example in "Situational Awareness" this language may be interpreted to mean that the cyber assets used to control the climate control system of the control room in which the operator performs his or her duties is subject to regulatory compliance because it determines the environmental conditions in which the operator performs the function of awareness of system conditions. Therefore, the language "Activities, actions and conditions" needs to be changed so that the reference is only to cyber assets that directly implement the services listed in "BES Reliability Operating Services". • The Low Impact Rating (L) definition is much too broad because it includes "All other BES Cyber Assets and BES Cyber Systems not categorized in Section 1 as having a High Impact Rating (H), or Section 2 Medium Impact Rating (M)." The CIP Version 5 standard needs to be written in a way that clearly limits its scope to assets that have significant impact to Bulk Electric System operation. We propose a defined Low Impact Rating as having minimal impact and create a "No Impact Rating" for all remaining BES Cyber Assets and BES Cyber Systems.
No
• The BES Reliability Operating Services encompasses everything a utility does. If this definition were used, it would encompass all assets. • The term "BES" is not defined in CIP standard Version 5. Definition of this term is crucial because it defines the scope to which the standard reaches. NERC is

in the process of defining the BES term in its NERC Project titled “2010-17 Proposed Definition of Bulk Electric System and Related Rules of Procedure Team”. While it will be possible to reference this external definition in the CIP standard, entities would become instantly non-compliant in the event that the external definition changes.
No
• How will FERC / NERC help the Utility Industry to have the authority necessary to conduct a broader and a more comprehensive Criminal History Records Check (CHRC) such as through the Federal Bureau of Investigation (FBI) that is a National check to ensure that individuals do not circumvent the process?” These types of comprehensive FBI CHRC are being done for Nuclear Regulated Facilities employees through the Nuclear Regulatory Commission (NRC) for years and have been extremely effective.
No
• C4-Table R6 Part 4: The Measures list two options which both require verification of evidence that conflicts with explanations in the rationale: 1. That the focus of this requirement is on the integrity of provisioning access rather than individual accounts. 2. That an administrative or clerical error should not be considered a violation of the standard. To be consistent, the Measures should only include evidence that the verification was completed, but not the results of the verification.
No
• C4-Table R7 Part 1: Revocation wording “at the time of” is not clear. Language such as “at the time” and “immediate” in a requirement are vague and difficult to both enforce and defend. Further, these terms imply a requirement of human perfection, which is a faulty concept. Language in the Standard must take into account the possibility for human error and the potential inability to meet the requirement due to unforeseen circumstances. • C4-Table R7 Part 1: Commission Order 706 provides the additional possibility that the ERO may “define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible”. The Standard needs to include language that allows the entity the ability to document what circumstances justify an exception to “immediate revocation”. • C4-Table R7 Part 2: The standard should include language to document when it was not possible to implement immediate revocation due to unexpected circumstances without the threat of a non-compliance finding. • C4-Table R7 Part 2: For reassignments and transfers the Standard requires that an individual’s unneeded electronic and physical access to BES Cyber Systems be revoked by the end of the next calendar day. The language should be changed to say “next business day”.

No
• C7-Table R1 Part 1.1: The Measures imply that screen shots that show the accessible ports of BES Cyber Assets will be required. A screen shot implies that only proof at the machine level is acceptable evidence. This is an administrative burden to supply snapshot each and every logical port implemented in each system. This means that entities will need to provide this proof for every system. The Measures should simply state that the entity provide a list of ports that it is using. This makes it possible to use one list to represent the configuration of many systems. • To sync this with the rationale the 1.1 requirement needs to add the following language: “and document the need for any remaining physical input/output ports.” • C7-Table R1 Part 1.2: All High and Medium impact devices are already within a physical security perimeter. There is no need for further physical protection within these facilities. Further, physical Control Ports is a good example of scope creep. This occurred because clarification was requested regarding the meaning of the word “port” in prior CIP revisions. FERC confirmed the original meaning was for software ports. In its response, FERC “encouraged” entities to address hardware ports. This requirement would be expensive, administratively burdensome to administer, and provide little, if any protection. This requirement is unnecessary and it is suggested that this requirement be dropped. • C7-Table R1 Part 1.2: The words “network connectivity” are not clear and needs further definition. The wording should be changed to say “ports used for routable protocols”.
No
• C7-Table R2 Part 2.2: There is no provision for simply using an existing remediation plan or a patch handling procedure – which is most often the case. Most patches are handled the same way – with a procedure that is used to handle all patches. The Measures imply that there is a different Remediation Plan for each patch (eg. a “dated” remediation plan). This could be improved by simplifying the language that allows for including the use of an existing Remediation Plan. • Referring to the identification of the security patches, the statement “that addresses the vulnerabilities within a defined timeframe” is confusing. Does this mean that provided our plan is documented within 30 days, that we have unlimited time to deploy the patch? • C7-Table R2 Part 2.3: The Requirements language is very confusing because the requirement that there is process for remediation has already been established in R2.2. The Measures don’t match the Requirements. In addition, the Measures imply that the entity must prove that the changes were actually made in the systems. The Measures imply that recorded employee confirmation that the patch has been installed (e.g. from a workflow) would not be acceptable evidence. At the time of audit, the state of any system cannot be relied upon at the time of audit to contain the evidence. The reason for this is that any time, the installation of a major software upgrade would eliminate all the evidence associated with the prior release in which the patch was installed. This means that the entity must insure that it captures evidence of every patch installation at the time that each patch is installed. It is sufficient to simply use a time stamped workflow specific to the subject patch to document confirmation by the employee that the installation for that patch was completed. This would relieve entities of the risk of violation due to human error for failure to collect physical evidence of a patch installation that no longer exists on its systems at the time of audit. Further, this approach would eliminate the costly administrative overhead needed to make that evidence available. • C7-Table R2 Part 2.3: The measures only allow for the installation of the patches. What if the patches cannot be installed? What measures will be permitted to document the CIP Exceptional Circumstances?
No
• C7-Table R3 Part 3.3: Entities would take on a huge administrative burden and exposure of potential violation due to human error to provide the detailed technical evidence shown in the Measures. Confirmation by an employee in a time-stamped workflow should be sufficient evidence to show that the signatures were updated. • C7-Table R3 Part 3.4: Is the intent of including “removable media” actually to ensure that the media itself has some malicious software prevention capability? The rationale states that the intent is to protect the BES Cyber System. The requirement already requires that there be malicious software prevention on the assets, what is the purpose of calling out removable media as a separate thing to protect.
No
• C7-Table R4 Part 4.3: The Rationale states that the intent was to make it clear that it would not be a violation if the event logging system fails. However, this requirement conflicts with that Rationale

because it requires a foolproof system for detecting and responding to logging failures. It would be better if the requirement said “Provide Mechanism(s) to Detect and Activate a response to event logging failures” and as part of this change address the measures. The requirement in R4.5 requires manual log reviews. One of the stated intents of that requirement is to identify potential event logging failures. Requirement 4.3 then duplicates R4.5. Also, a logging failure is not an emergency that justifies a call-out on a non-business day. Next calendar day response times will necessarily lead to weekend/holiday – call-outs, which are administrative burden. ‘Next business day’ is suggest to replace the ‘next calendar day’. • C7-Table R4 Part 4.4: The Measures do not line up with the Requirement because it implies that more must be done than the requirement says (90 day retention). The Measure needs to refer to the same time frame as the requirement.
No
• C7-Table R5 Part 5.5.3: This requirement appears to be missing the link between the impact of the BES Cyber Security System to the password significance, we suggest this be re-worded.
Yes
No
• The requirement is confusing. The measure is more clear that the intent is to document that backups were successful and that could simply be the backup job report. The requirement could be interpreted to mean that the “information” on the backup media needed to be verified to confirm the backup was successful. Suggest making wording more simply, “For media backups that are essential to the BES Cyber System recovery, verify the backup process completed successfully.” In the measure add copies of backup system job reports as another measure. • R1.4: The Measure listed requires dated evidence that the verification of the backup process completed successfully. With this wording, an auditor may not accept confirmation by an employee via a Workflow that the backup process was completed and verified even though the wording of the Measurement includes the words “Evidence may include, but is not limited to…”. Backup systems can easily be automated to verify that the backup process completed successfully. Requiring dated system generated evidence that demonstrates that the backup and verification process completed successfully results in unnecessary administrative burden to the entity because of the never ending need to collect and store evidence repeatedly for many systems. Employee verification that the backup and verification processes were completed via a time-stamped workflow should be sufficient.
No
• The performance of an operational exercise of the recovery plans can be very costly, both in hardware/software and in people resources. This would require that we either take devices out of commission to facilitate the operational exercise or we have spare devices to facilitate “representative environment that reflects the production environment.” While we understand the need to ensure that you can actually do what is in the plan, we need to recognize the impact of this requirement. • R2.2 This requirement regards testing of information stored on backup media. The wording currently includes language “to insure that the information is usable and reflects current configurations.” The integrity of the information stored on backup media is not related to whether or not that information reflects current configurations because the information stored on the backup media contains the configuration of the system at the time the backup was taken. It is suggested that the wording “and reflects current configurations” be removed from both the Requirement and the Measures. • R2.3 This requirement includes a provision the entities to “Test each of the recovery plans referenced in Requirement R1,” initially upon the effective date of the standard.” It will not be possible for entities to test all of their recovery plans on that one day. As this is a new requirement, it will take many months for entities to prepare for and execute these tests. At a minimum, entities should have at least 12 months to prepare for and execute these tests.
No
• • Why not combine with Part 3.1 so it syncs with Part 3.2, add “and document any identified deficiencies or lessons learned within thirty calendar days” so that the requirements match. • R3.4

requires that recovery plans are updated address organizational changes within thirty calendar days of such change. The term “organizational changes” is undefined. When entities change their organizational structure, the computer systems and the people that support them are typically very much the same the day after the change as before the change. The reason for this is that BES Cyber Systems evolve separately from organizational changes. Moreover, the people that have the expertise to support BES Cyber Systems and BES Cyber Assets before the change are the same people who have the expertise to provide the support after the organizational change. It is suggested that the wording for this requirement state that the Recovery plans be updated when the information referred to in R1.2 changes.
No
1. Part 1.1.3 includes the phrase, “Any commercially available application software (including version) intentionally installed on the BES Cyber Asset”. Commercial providers such as SCADA vendors commonly package releases of other commercial software “eg. Oracle” into their products. In instances in which a Commercial provider’s release includes bundled releases of other commercial products, then reference to the highest level Commercial provider’s release number should be sufficient to define the baseline. The language of the standard could be improved by allowing entities to rely on the highest level Commercial provider’s release number as the definition for all bundled commercial software. 2. Part 1.2 – The requirements statement is not clear because it does not say what the CIP Senior Manager or delegate is authorizing. It is understood that the requirement is to authorize changes, but this is not stated. 3. Part 1.1.4. considers “Any custom software and scripts developed for the entity” as part of the baseline. It is unclear what the words “for the entity” mean. Software used by utilities generally contains a high level of customization. Changes occur incrementally and very frequently. Inclusion of custom software and scripts in the baseline is OK, but entities need some flexibility to determine what custom software and scripts are included as part of the baseline. Language needs to be added to provide the entities the flexibility to determine what custom software and scripts are considered part of the baseline, and what custom software and scripts are considered changes from the baseline. This will allow the entities the ability to structure their baseline and changes to the baseline in a manner that takes advantage of their existing infrastructure and systems in order to meet the desired objective without unnecessary burden. 4. Part 1.4.2 requires the entity to verify that the “required controls and BES Cyber System availability” are not adversely affected. It doesn’t make sense to require the entity to verify BES Cyber System availability resulting from the change. Whenever there is an availability problem, it will be detected and acted upon when it occurs. A future availability problem cannot be verified before it occurs. It is suggested that phrase “BES Cyber System availability” be removed from this requirement. Part 1.5.2 places an excessive administrative burden on the entities.
No
Comments: Under 3.2 the Measures require how differences between the production and test environments were accounted for in conducting the vulnerability assessment. It may be impossible to do this because the test environment will likely only include a subset of the equipment that is present in production.
Group
Arizona Public Service Company
Scott Bordenkircher
Yes
AZPS believes the definition for “BES Cyber Incident” should read “A Malicious act” not “Any Malicious act” in the first sentence. AZPS recommends changing the first bullet to “Compromises, or was an attempt to compromise, an Electronic Security Perimeter or a Defined Physical Boundary” in order to remove the language of “Physical Security Perimeter and use the new definition for PSP. AZPS

recommends the removal of the words “Critical Cyber Asset” in the second bullet since the sentence refers to BES Cyber Systems which would include Critical Cyber assets. AZPS also recommends the deletion of the 3rd bullet; this bullet is redundant to the first bullet. AZPS believes the last sentence in the definition for “BES Cyber System” should have the word “Maintenance” changed to “Transient” in order to align with the new terminology. AZPS is unclear on the definition for “BES Cyber System Information”. There is no definition of the term “BES Cyber System Impact Designations”. It is unclear what floor plans and equipment layouts would be considered BES Cyber System Information. AZPS recommends that the definition for “Restoration of BES”, bullet one should read “Blackstart restoration including planned cranking path as identified in Entity’s EOP-005 R1 artifacts.” Bullet 2 should be struck based on it being on the NRC side of the Bright Line criteria for applicability of the CIP Standards (and therefore outside of NERC jurisdiction). AZPS believes that under the definition for “Situational Awareness”, bullets 2 and 3 (“Change Management” and “Current Day & Next Day Planning”, respectively) should be struck because these functions are too long term to be considered Situational Awareness and have minimal impact on real-time operations. AZPS has 2 concerns with the definition for “CIP Exceptional Circumstance” 1) This is not defined in relation to BES reliability risk (i.e. person has heart attack in parking lot – probably not a CIP Exceptional Circumstance); 2) definition leaves no room for Entity to identify other situations wherein BES reliability is in jeopardy and declare a CIP Exceptional Circumstance as appropriate. AZPS recommends in the definition for “Control Center” that every use of the word “facilities” in this section be capitalized since it is a NERC defined word. AZPS believes in the definition for “Electronic Access Control or Monitoring Systems” including the phrase “or BES Cyber Systems” is much broader than the usage of this term in the Standards and could imply controls on all LOW impact devices. AZPS recommends deleting “or BES Cyber Systems”. AZPS recommends in the definition for “Electronic Access Point (EAP)” the word “restricts” be changed to “facilitates”. AZPS recommends the definition for “Electronic Security Perimeter” be changed to read “A collection of Electronic Access Points that protect one or more BES Cyber Systems.” AZPS believes that the definition for “Intermediate Device” should be an Electronic Access Point by definition and should be protected as such. It should not be allowed to reside outside an ESP and in fact should be part of an ESP. This definition could be rewritten as “a device that proxies communication with a BES Cyber Asset and terminates encrypted communications.” AZPS believes that in the definition for “Transient Cyber Asset”, item #3 is unnecessary and adds no value to the definition. It would also cause audit issues (e.g. proving that this criteria was met).

Yes

AZPS disagrees with 4.2 on page six. It is unclear, with the addition of 4.2.1 and 4.2.2, if the Facilities are restricted, in scope, to BES Facilities or if the identification and analysis of BES Cyber Systems is intended to expand to UFLS, UVLS, RAS, etc. that may be in Distribution Facilities. The Standard should specifically indicate, if this was the intention, that these specific Facilities may or may not actually be identified as BES Facilities but are still in scope because of their ability to impact BES facilities. AZPS would like clarity added to item 2.5 in attachment one; does cranking path imply only the primary Cranking Path, or is the intention to include all (or some) alternate Cranking Paths that have been identified in the restoration plan? AZPS disagrees with the Guidelines and Technical basis section at the end of this standard. Definitive or directive statements should not be made in Guidelines, as this leads to audit issues where Guidelines tend to be treated as more directive than they may have been intended.

No

AZPS believes in R1 that the use of the word ‘owns’ is ambiguous; should this not be the responsibility of the Entity that Operates the BES Cyber Assets/Systems? Multi-party ownership is a common business arrangement and leads to much confusion. The requirement should specifically identify which party is responsible for this identification and subsequent protection. Also, the sentence “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification,” is not really feasible. It would not be possible to identify High and Medium Assets/Systems without a full list, which would lead to the conclusion that a list of Low Impact Assets/Systems is a necessary outcome of the identification. Also, several Standards are applied to Low BES Cyber Systems, which would indicate having to know what they are. The Standard should indicate that a list of Low Impact Assets/Systems is required at least at a summary level. There is a grammatical error in the first sentence of R1.1, it reads “BES Elements and Facilities is placed into operation” and should read “BES Elements and Facilities placed into operation”.

No

AZPS recommends changing the language “initially upon” to “prior to”. In M2 of R2, the phrase “review and update, where applicable” should be replaced with “review and approve”.
Yes
Yes
No
AZPS believes R2 could be enhanced by including the expanded descriptions of each bulleted item from the guidelines. Additionally, AZPS believes topics from CIP-002-5 and CIP-003-5 should be included in the policies.
No
AZPS recommends changing the phrase in R3 “initially upon the effective date” to “prior to the effective date”.
No
AZPS recommends the statement in R4 “individuals who have access” be changed to “individuals who have authorized access”. AZPS recommends the word “contractors” used in the bulleted list for Measure 4 be changed to “third parties”. The word “contractors” is too narrow.
No
AZPS recommends clarifying the word “position” in R5. Does this mean title or generalized organizationally defined role?
Yes
Yes
Yes
No
AZPS recommends expanding the applicability column in the R2 table to all systems identified in the R3 table. AZPS recommends changing the wording in table 2.2 Requirements. The wording should be changed to “Develop role specific Training, where applicable on the security controls protecting the Responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.2 Measures to “Evidence may include, but is not limited to, training material on the security controls to protect BES Cyber Systems.” AZPS recommends changing the wording in table 2.3 Requirements to “Develop role specific Training, where applicable on the proper use of physical access controls protecting the responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.4 Requirements to “Develop role specific Training, where applicable on the electronic access controls protecting the Responsible Entity’s BES Cyber Systems.” AZPS recommends changing the wording in table 2.5 Requirements to “Develop role specific Training, where applicable on the visitor control program.” AZPS recommends changing the wording in table 2.6 Requirements to “Develop role specific Training, where applicable on handling of BES Cyber System Information including storage media.” AZPS recommends changing the wording in table 2.7 Requirements to “Develop role specific Training, where applicable on identification of a potential BES Cyber Security Incident and associated notifications.” AZPS recommends changing the wording in table 2.8 Requirements to “Develop role specific Training, where applicable on recovery plans for BES Cyber Systems.” AZPS recommends changing the wording in table 2.9 Requirements to “Develop role specific Training, where applicable on response to BES Cyber Security Incidents.” AZPS recommends changing the wording in table 2.10 Requirements to “Develop role specific Training, where applicable on BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets.”
Yes
No
AZPS recommends expanding the applicability column in the R4 table to all systems identified in the R5 table.

No
AZPS recommends changing the wording of table 5.1 Requirement to “Ensure a personnel risk assessment has been performed as specified in CIP-004-5 R4 prior to being granted authorized electronic or unescorted physical access, except for CIP Exceptional Circumstances.”
Yes
No
AZPS disagrees with the wording in the table 7.1 Requirements column “For resignations or terminations, revoke the individual’s unescorted physical access and Interactive Remote Access to BES Cyber Systems at the time of the resignation or termination.” It is not possible to implement or prove an activity was performed simultaneously with another activity. Also it is not clear if time of resignation means notice of resignation or actual effective resignation. AZPS disagrees with the time frame in table 7.2 Requirements “For reassignments or transfers, revoke the individual’s unneeded electronic and physical access to BES Cyber Systems by the end of the next calendar day.” This is not a reasonable time frame. Take the scenario where an HR system processes a transfer on a Saturday. Requiring an entity to call-out personnel on a Sunday to revoke access for a transfer provides very little security value and will add significant burden. Seven calendar days is a reasonable timeframe. AZPS disagrees with the time frame in table 7.4 Requirements “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with (R7.1 or 7.3) within thirty (30) calendar days of the date of initial access revocation.” This poses a much larger security risk than R7.2 and should allow no more than seven calendar days. AZPS disagrees with the time frame in table 7.5 “For terminations, resignations, reassignments, or transfers, change passwords for shared account(s) known to the user within thirty (30) calendar days of the termination, resignation, reassignment, or transfer of the user.” Based on this security risk, AZPS believes no more than seven (7) calendar days should be allowed. AZPS also believes the second paragraph in the original text should be deleted due to there already being allowances for CIP Exceptional Circumstances.
Yes
No
AZPS disagrees with the applicability section of R1.1 and would recommend removing the word “routable”. AZPS believes dial up should be included from a security standpoint. The Guidelines for R1 do not align with what is stated in the R1.1 Requirements column. The guideline for R1 specifies network segmentation for all BES cyber systems. The requirement text is extremely ambiguous and does not provide enough specifics for an entity to know if what they provision will be found auditably compliant. The Measures states “documented technical AND procedural controls” while the Requirement states “technical OR procedural controls”. These need to be aligned. AZPS recommends that in R1.3 in the applicability section, the words “with external routable connectivity” should be removed because, from a security perspective, this should include dial up. In the measure for R1.3, “each access rule has a documented reason” is stated yet the Requirements do not include the mandate for “a documented Reason”. AZPS recommends that in R1.4 applicability section, the wording for the phrase "Electronic Access Points that use dial-up access for non-Interactive Remote Access" should change to "Electronic Access Points that utilize dial-up for External Connectivity that is not used for Interactive Remote Access" in order to clarify the intention of the phrase “non-Interactive Remote Access”. In the Requirements section, AZPS recommends removing “where technically feasible”. There are devices readily available that can be implemented that make this technically feasible so no exception is required. AZPS would like specificity in the requirements of R1.5. If the intent is to require an IDS, make the Requirement “Implement an IDS that monitors, detects and alerts for malicious activity at each EAP.”
No
AZPS disagrees with having a “technically feasible exception” for R2. AZPS believes all aspects of the requirement are technically feasible. AZPS would like the Requirements portion of R2.2 clarified. It is not clear which endpoints we need to encrypt between. Is this between originating devices and the intermediate device or all the way to the BES Cyber System?
Yes

No
AZPS recommends changing the wording in table 1.1 Applicability. The word implement should be added to the Requirement so it matches the Measures. AZPS disagrees with the wording in table 1.1 Requirements. Move Associated Physical Access Control Systems to Applicability in R1.2 for stronger controls much like in CIP-005-5 R1.2. AZPS recommends changing the wording in table 1.2 Measures by removing the words “accompanied by card reader logs”. This could be something other than a card reader. AZPS recommends changing the wording in table 1.3 Requirements. Reword the Requirement to “Utilize two or more authentication factors to gain physical entry.” The way it is worded currently allows for two physical access controls to be identified but does not specify that they both must be used for a single entry. The Guideline implies that the intent was to require multifactor authentication. Also – remove the words “where technically feasible”, this unnecessary exemption weakens security. AZPS recommends changing the wording in table 1.3 Measures by removing the words “accompanied by card reader logs”. This could be something other than a card reader. AZPS disagrees with the wording in table 1.4 Requirements. The wording should include attempts at unauthorized physical access. AZPS disagrees with table 1.5. This should be merged with Requirement R1.4. There is no reason not to require that physical access control systems reside within a DPB. AZPS recommends adding Associated Physical Access Control Systems to table 1.6 Applicability. AZPS disagrees with the security posture in table 1.6 Requirements. This requirement should mandate logging of entry AND EXIT by authorized personnel.
No
AZPS recommends changing the wording in R2 to “…Entity shall document and implement a visitor control program…”. AZPS recommends adding Associated Physical Access Control Systems to table 2.1 Applicability. AZPS recommends adding Associated Physical Access Control Systems to table 2.2 Applicability. AZPS recommends changing the wording in table 2.2 Requirements. This Requirement should be rewritten to state “Implement a process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit and includes the visitor’s name, the name of the person conducting the escorting, and the responsible point of contact. Document all escort handoffs.” This is a far better security implementation than what this requirement has been proposed as. AZPS doesn’t believe there is any reasonable way for an Entity to research an incident if they are unable to track when visitors enter and exit and unless they are able to clearly identify WHO escorted the visitor. Mandating the tracking of a non-present Point of Contact holds absolutely zero security value. AZPS disagrees with the wording in table 2.2 Measures. Add “and the name of the person or persons conducting the escorting.”
No
AZPS recommends changing the wording in R3 to “…Entity shall document and implement maintenance and testing…”. AZPS recommends changing the wording in table 3.1 Requirement to state “…calendar months thereafter, conduct testing and perform necessary maintenance of the Physical…”. AZPS recommends changing the wording “logging and alerting systems” in table 3.2 Requirement to “Physical Access Control Systems”.
Yes
No
AZPS recommends changing R1 to read “Each Responsible Entity shall document and implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.” AZPS believes that the words “of BES Cyber Systems” should be removed from the measures in R1.1 since R1.1 applies to more than the BES Cyber System. AZPS recommends that the language in the requirement for R1.2 should be changed from “console command” to “console control” in order to clarify the type of physical port enabled.
No
AZPS recommends changing R2 to read “Each Responsible Entity shall document and implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management” AZPS believes the requirements section of R2.1 should state “Security related updates” and not just “updates”. R2.1 also mentions firmware, but the configuration requirement in CIP10 does not require the documentation of firmware levels. These requirements need to align. Under the measures section for R2.1 the words “BES Cyber Systems” should be

removed since R2.1 applies to more than the BES Cyber System. Also remove the words “The list could be sorted by BES Cyber System or Source”, these words are not necessary. AZPS recommends in the requirements and measures of R2.2 should state “Security related updates” and not just “updates”. In the measures it states “a dated implementation plan showing how the vulnerability will be addressed”; this part of the measure does not align with the guidelines, the guidelines identify the option of an event driven timeline whereas this measure dictates a DATED plan. AZPS recommends that in the measures section of 2.3 you add “Previously implemented controls” as acceptable evidence of remediation.

No

AZPS recommends changing R3 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention.” AZPS disagrees with Requirement 3.4, and recommends including removable media under R3.1. This Requirement would then be focused on Transient Cyber Assets. Also, remove the words “BES Cyber Systems” since R3.4 applies to more than the BES Cyber System. AZPS also disagrees with the measures portion of 3.4; there is no logging requirement anywhere in the standards for logging the use of removable media. Also, no inventory is required for transient devices anywhere in the standards. AZPS recommends that in the requirements and measures for R3.5, logging the disconnection of the transient asset should also be required as a better security practice.

No

AZPS recommends changing R4 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." AZPS recommends changing the wording in the Requirements of R4.1 to read “logging of generated events…” instead of “log generated events…”. AZPS disagrees with the timeframe requirement set forth in the Requirement section of R4.3 and would like the timeframe removed. Further, event logging failure needs to be clarified, from a technical perspective you can’t always detect a failure of event logging. AZPS wants more clarity and alignment between the Requirement and the Measure in R4.4. The Requirement states “for at least the last 90 consecutive calendar days” while the Measures state “logs from the past ninety days”. AZPS recommends striking the “at least” language in the Requirement and have it read “for the last 90 days”. Also, remove the words “BES Cyber Systems” since R4.4 applies to more than the BES Cyber System. AZPS believes in the Requirements for 4.5 the “potential logging failure” language should be removed since that is covered in 4.3. The language in the Requirement that states “Activate a response to rectify any deficiency identified from the review before the end of the next calendar day” should be simplified by being changed to “Activate your incident response plan”; this language accomplishes what is intended and is far clearer. In the Measures for 4.5 AZPS would like to have the “signed” language stricken, with the belief that documenting the name of the reviewer in the review proves the review was completed; implying that the review must be physically signed adds unnecessary burden. The language in the Measures that reads “showing that personnel were dispatched or a work ticket was opened to rectify the deficiency” should be changed to “showing the incident response plan was activated”; this language accomplishes what is intended and is far clearer.

No

AZPS recommends changing R5 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls.” In R5.1 AZPS recommends adding the word “user” in front of “credentials” in the Requirement section to add clarity. Also, remove the words “to each BES Cyber Systems” since R5.1 applies to more than the BES Cyber System. In the Measures for R5.1 remove the words “to each BES Cyber Systems” since R5.1 applies to more than the BES Cyber System. AZPS recommends for the Requirements section of R5.2 the words “the use of” should be deleted due to the potential for this to confuse people into thinking that every individual usage of these accounts should be authorized every time. In the Measures forR5.2 remove the words “to each BES Cyber Systems” since R5.2 applies to more than the BES Cyber System. AZPS disagrees with the Requirements section of R5.4. All of the text following the word “application” should be deleted and added in the applicability section as defined assets that are covered. This would keep consistency across all of the standards. AZPS recommends for the Requirements section of R5.5.1 and R5.5.2 remove the words “by the BES Cyber Systems” since R5.5 applies to more than the BES Cyber System. For R5.5.3 the language “of the BES Cyber System, the significance of passwords in the set of controls used to prevent

unauthorized access to the BES Cyber System and" should be removed and the word "or" should be added in place. The words are unnecessary in this section. AZPS recommends that for the Applicability section of R5.6 instead of "at Control Centers" it should state "all Medium Impact BES Cyber Systems" in order to maintain consistency.
Yes
No
AZPS recommends changing the wording in R1 from "have" to "document". AZPS believes there may be misalignment between the wording in table 1.2 Requirements and the Guidelines. The Guidelines define what is reportable but the Requirement allows the utility the latitude to define it for themselves. The intent needs to be made clear and the two need to align.
No
AZPS recommends changing the word "When" in table 2.1 Requirements to "In the event of…" Change to state "Document the use of the Incident Response Plan." Insert "Document deviation from the plan during the incident." Delete the word test, testing is covered in R2.2. AZPS believes the Measures does not align with the Requirement in that it adds the requirement to justify deviations. AZPS recommends changing the word "Implement" in table 2.2 Requirements to "Perform an exercise". Change "Initially upon the effective date…" to "Prior to the effective date…". Delete the phrase "between executions of the plan(s)"; it is not necessary. AZPS recommends changing the word "implementing" in table 2.2 Measures to "exercising".
No
AZPS recommends changing the wording in R3 from "implement one or more documented" to "document and implement". AZPS recommends changing the wording in table 3.1 Requirements from "initially upon the effective date" to "Prior to the effective date". Delete the phrase "between reviews"; it is not necessary. Add clarification to update within thirty calendar days. AZPS recommends changing the word "test" in table 3.2 Requirements to "exercise". AZPS recommends changing the requirement in table 3.2 Requirements to mandate the update within thirty calendar days instead of sixty for better security practice.
Yes
No
AZPS would like clarity in the Requirements section of R1.3. It is unclear what the intent of the word "protection" means in this context. AZPS believes the requirement would be better served with the use of the word "recovery" rather than the word "protection". Remove the words "BES Cyber System functionality" form the Requirements section since R1.3 applies to more than the BES Cyber System. Remove the words "BES Cyber System" from the Measures section since R1.3 applies to more than the BES Cyber System. AZPS recommends replacing all of the language in the Requirements section of R1.4 with "Verify that backups of information essential to recovery complete successfully." AZPS recommends replacing all of the language in the Requirements section of R1.5 with "Procedures that attempt the preservation of data of any event that triggers the activation of any recovery plans including documentation of any failures in preserving data". The Measures section of R1.5 also should be rewritten to state "Evidence may include, but is not limited to, procedures that attempt the preservation of data of any event that triggers the activation of any recovery plans including documentation of any failures in preserving data".
No
AZPS recommends changing R2 to read "Each Responsible Entity shall document and implement one or more recovery plans that collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. AZPS believes that in the Requirements section of R2.1 the word "Implement" should be changed to "Exercise" to add clarity to what is really required. Also, in the Requirements section the language "initially upon the effective date…" should be changed to "prior to the effective date…". The Measurements part of R2.1 should also be rewritten to better align with the Requirements. AZPS believes the Requirements section of R2.2 needs to have the language "of BES Cyber Systems" removed since R2.2 refers to all assets. The word "initially" should be removed and the words "prior to the effective date of the standard" should be added. Also in the Requirements section the language "information is useable and reflects current configurations",

should be changed to “information is recoverable and current”. AZPS believes the Measures section of R2.2 needs to have the language “of BES Cyber Systems” removed since R2.2 refers to all assets. The words “when initially stored” should be removed and the words “prior to the effective date of the standard” should be added. Also in the Measures section the language “information is useable and reflects current configurations” should be changed to “information is recoverable and current”. AZPS recommends in the Requirements section of R2.3 the words “initially upon the effective date of the standard and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment…” be rewritten to “at least once every 39 calendar months following the effective date of the standard through an operational exercise of the recovery plans in an environment...”. In the measurements section of R2.3 removes the language “initially upon the effective date of the standard and”, since the initial exercise is covered under R2.1 and no initial should be required to recover the entire system.

No

AZPS recommends that in the Requirements section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. Also in the Requirements section, change “BES Cyber Systems” to “Cyber Assets”. AZPS recommends that in the Measures section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. AZPS recommends a rewrite of the Requirements portion of R3.4 to state “Review and update (if appropriate) recovery plans to address any organizational changes within thirty calendar days of such change.” This new language adds the review aspect of the standard and removes the change due to technology change since that is covered in CIP10-5 R1.3.

Yes

No

AZPS recommends changing R1 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.” AZPS recommends the following changes to the Requirements section of R1.1: • Remove the words “ of each BES Cyber Systems” and “for each BES Cyber Asset identified” since R1.1 applies to more than the BES Cyber System • R1.1.3 remove the words “intentionally” and “on the BES Cyber Asset” • R1.1.4 should read “developed and installed” since just simply developed does not mean it was installed. • R1.1.5 should be deleted, because this is covered in CIP-007-5 • R1.1.6 should read “All installed security patches” • Hardware components and firmware versions should be added for better security practice. AZPS recommends in the Measures section of R1.1 remove the words “of each BES Cyber Asset in the BES Cyber System” since R1.1 applies to more than the BES Cyber System. AZPS recommends changing the Requirements section of R1.2 to read “documentation of changes” instead of “and document changes”. Remove the words “of each BES Cyber Systems” and “for each BES Cyber Asset identified” since R1.2 applies to more than the BES Cyber System. In the Measurements section of R1.2 “Evidence may include” should be changed to “Evidence of the change and the authorization may include”, since the standard explicitly requires authorization the evidence should show the authorization. AZPS recommends the wording in R1.3 be changed from “…required by a NERC CIP Standard, including identification and categorization of BES Cyber Systems as necessary…” to “required by any NERC CIP Standard as necessary…”. AZPS believes R1.5 should merge with R1.4 and require all steps for all of the items listed in R1.4 Applicability. Suggested combination and order of requirements referenced by current numbering (which of course would be renumbered R1.4.1-R1.4.5): R1.4.1, R1.5.1, R1.5.2, R1.4.2, R1.4.3.

No

AZPS disagrees with the Requirements section of R2.1 and believes the Requirement should be rewritten to read “Detect for changes of the baseline configuration within 7 days. Document and investigate within 30 days”.

No

AZPS recommends changing R3 to read “Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-010-1 Table R3 – Vulnerability Assessments”. AZPS recommends that in the Requirements section of R3.1 the language “initially upon the effective date…” should be changed to “prior to the effective date…”. The words “security controls” should be specified, the language from the Guidelines should be added here. The requirements section also needs some simplification to the language. AZPS recommends changing

"…to determine the extent to which the controls are implemented correctly…." to "to determine if the controls are implemented and operating as designed…". AZPS recommends that in the Requirements section of R3.2 the language "initially upon the effective date…" should be changed to "prior to the effective date…". Also in this section, replace the word "test" with "production environment or an…", this will allow for a VA to occur against the production environment or a representative environment without specifying it must be a test environment. AZPS does not think the Requirements section of 3.4 makes sense the way it is written. AZPS recommends that instead of "…planned date of completing the action plan and the execution status of the action plan." This should read "planned date of completing the action plan." What would also make sense would be to mandate updates to the status of the action plan at some periodicity such as quarterly.

Yes

No

AZPS recommends changing the wording of R11 to "Each Responsible Entity shall document and implement one or more processes that collectively include each of the applicable items in CIP-011-1 Table R1 – Information Protection…" AZPS recommends, in table 1.1 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends, in table 1.2 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends, in table 1.3 Applicability, deleting "Associated, protected cyber assets" because these are not included in the Definitions. AZPS recommends changing the wording of table 1.3 Requirements to "Prior to the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment."

No

AZPS recommends changing R2 to "Each Responsible Entity shall document and implement one or more processes that collectively include the applicable items in CIP-011-1 Table R2 – Media Reuse and Disposal…." AZPS disagrees with separating tables 2.1 and 2.2. Tables 2.1 and 2.2 should be combined under one Requirement. The words "Associated Protected Cyber Assets" should be deleted from Applicability. The combined table 2.1 and 2.2 Requirements should be reworded as "Media containing BES Cyber Security Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. Prior to the disposal of BES Cyber Asset media, the Responsible Entity shall destroy or take action to prevent the unauthorized retrieval of BES Cyber System Information from the media."

Yes

Yes

Group

ZGlobal on behalf of City of Lodi, City of Ukiah, Alameda Municipal Power, Salmon River Electric Coop, California Pacific Electric Company

Mary Jo Cooper

Yes

We thank the drafting team and compliment them on their work. It is very valuable and provides a good basis for appropriately allocating responsibilities according to the impact to the BES. We believe the definition of BES Cyber Asset is accurate however based on the definition we feel that the Functional Applicability for each Standard is incorrectly defined. As a result we have cast a negative vote on the Standards. Additional work is needed due to a discrepancy between the definition of BES Cyber Assets and the applicability to entities with UFLS or UVLS equipment. Definition of BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to

operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Applicability: Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or regional Reliability Standard • A UVLS program required by a NERC or regional Reliability Standard • A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard • A Transmission Protection System required by a NERC or regional Reliability Standard • Its Transmission Operator's restoration plan Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: • A UFLS program required by a NERC or regional Reliability Standard • A UVLS program required by a NERC or regional Reliability Standard The discrepancy exist because (1) The definition states “The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES.” (2) LSE’s and DP’s with UFLS equipment are required to comply with the proposed CIP Standards over BES Cyber Assets when these devices are not consider BES Cyber Asset per definition. (3) These devices sense a system condition and do not send or receive instructions. In fact in some regions a UFLS device is not required to be a cyber-equipment type. For example, in the NPCC region an electro-mechanical relay can be used to fulfill an organizations UFLS program requirement. Proposed recommendation: Modify the applicability. “Load Serving Entities and Distribution Providers with a load shedding program that is activated through receipt of an instruction to its cyber processor to operate.”
No
Yes
Yes
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.

No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functionality of the equipment to recieve or send an electronic

signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.

No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
Yes
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
No
We do not necessarily disgaree with the requirement but rather the applicability as stated in our comment regarding the definitions. This Standard should not be applicable to entities merely because they own UFLS of UVLS equipment. The functinality of the equipment to recieve or send an electronic signal to operate should be addressed.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
BES Cyber Asset: The drafting team should consider revising the definition to consider the facility the Cyber Asset is associated with, “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the ability of the facility with which it is associated with. (See comments on CIP-002-5) Additionally, the terms “adversely impact” are not well defined. BES Cyber System states, “A Maintenance Cyber Asset is not considered part of a BES Cyber System.” The drafting team should consider removing this statement (since the definition of a BES Cyber Asset excludes Transient Cyber

Assets), modifying the statement to exclude Transient Cyber Assets, or defining “Maintenance Cyber Asset.” BES Cyber System Information: The definition includes the term “BES Cyber System Impact” designations; this term is not defined and should be clarified by the drafting team. CIP Exceptional Circumstance: It is unclear the differentiation of, “A Cyber Security Incident requiring emergency assistance” and “a response by emergency services.” CIP Senior Manager: The definition should be clarified it is applicable to CIP-002 thru CIP-011, as CIP-001 is currently enforceable and does not require a CIP Senior Manager Control Center: The definition is broad and could impact small entities by including ‘control rooms.’ As proposed, “One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations” System Operator is currently defined as, “"System Operator: An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." A vertically integrated utility can have a “Control Center” with certified system operators that support the real-time operations and have a control room located at a generation plant that can perform one or more of the functions listed in the definition of Control Center. The drafting team should clarify if it is the intent to only include the Control Center with the primary responsibility for maintaining reliability of the BES, performing one or more of the functions that support real-time operations by System Operations. Reportable BES Cyber Security Incident: The definition included in CIPv5 conflicts with EOP-004-2 for both Cyber Security Incidents and Forced Intrusions for BES facilities. The drafting team should consider coordinating with the EOP-004-2 drafting team to ensure there is no overlap or ‘double jeopardy.’

Yes

FEUS supports the comments submitted by APPA.

No

FEUS concurs with the comments submitted by APPA. In addition, FEUS shares the concern, as others in the industry, that CIP-002-5 as currently drafted will not be auditable by CEA’s. CIP-002-5 R1 requires entities that own BES Cyber Assets and BES Cyber Systems to categorize those assets using Attachment 1. The definition of BES Cyber Asset includes Cyber Assets that adversely impact one or more BES Reliability Services. In order to comply with CIP-002-5 R1, the entity will FIRST have to identify ALL BES Cyber Assets and BES Cyber Systems that adversely impact BES Reliability Operating Services, then categorize the BES Cyber Assets and BES Cyber Systems using Attachment 1. Attachment 1 describes facilities that if the BES Cyber Asset or BES Cyber System meets one of the criteria, it inherits the high or medium impact with all others classified as low. In order to identify ALL BES Cyber Assets and BES Cyber Systems requires knowledge of the entities system. An auditor, who is not familiar with the system, would not be able to validate the entities assessment without knowledge of the system or FIRST looking at the entities facilities. While the requirement does not require discrete identification of Low Impact BES Cyber Assets and BES Cyber Systems, sub requirement R1.1 requires documentation of a change in the classification of within 30 calendar days for assets going from a lower impact to a higher impact. Without documentation the asset was classified as low prior to the reclassification, this would be almost impossible to audit. Additionally, the VSL’s for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified – in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a Low Impact to determine the correct VSL; thus, requiring ALL Low BES Cyber Assets being identified. FEUS agrees with Honeywell, a revised three-step process could replace the process in the current draft as follows: 1. For each BES Facility that has associated cyber assets, determine the impact using Attachment 1. 2. Determine the BES Reliability Operating Service(s) the BES facility supports 3. Identify associated BES Cyber Assets and BES Cyber Systems This allows the first step to be determined by facility, much like previous versions and the classification of BES Cyber Assets and BES Cyber Systems to be determined subsequent and inherit the designation of the facility. Thus, Low Impact facilities would not require a list of Low Impact BES Cyber Assets or BES Cyber Systems.

No

R2 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS

recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time following the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective date, not to exceed three months following, and at least each calendar year thereafter…”
No
The VSL’s for R1 are based on the number or the percent of BES Cyber Assets incorrectly identified – in order to determine the correct number or percent of BES Cyber Assets incorrectly identified, the CEA would have to determine all BES Cyber Assets, including the assets with a Low Impact to determine the correct VSL; thus, requiring ALL Low BES Cyber Assets being identified.
Yes
Yes
The topics included in the sub requirements are capitalized indicating they are defined terms. The drafting team should verify all capitalized terms are defined.
No
The drafting team should revise the statement “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time following the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective date, not to exceed three months following, and at least each calendar year thereafter…”
Yes
Yes
Yes
Yes
Yes
No
The rationale states some personnel may not require training on all topics based on their role; R2 should be revised to indicate the training is based on the roles defined in R2.1. An example of such wording could include, “Each Responsible Entity shall have a role-based cyber security training program for personnel who require authorized electronic or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items that includes each of the applicable items based on their role in CIP-004-5 Table R2”
No
R3.1 and R3.2 should clarify the required training is role-based as determined in R2.1. The drafting team should consider revising R3.1 as follows, “Require completion of the training specified in CIP-004-5 R2, based on the role defined in CIP-004-5 R2.1, prior to granting authorized access, except during CIP Exceptional Circumstances.” A similar clarification can be made to R3.2.
No
R4.2 requires the seven year criminal history check for all locations where a person has resided, been employed, or went to school for more than six months. FEUS SME’s believe it will be difficult to verify all the locations a person has resided, been employed, or went to school for more than six months without accepting an attestation of all the locations from the individual.
Yes

No
CIP-004-5 R6.1 Measure (i) requires a sampling of accounts to verify unauthorized users do not have access; FEUS recommends the drafting remove this measure from R6.1 as doesn't seem relevant to authorization of access and is more appropriate in 6.4. The same comment applies to the Measure (i) of R6.2 and Measure (i) of R6.3.
No
FEUS appreciates the change rationale stated by the drafting team. However, the drafting team should consider revising R7.2 to maintain access, based on need, following a transfer. A reassignment or transfer may be a promotion that requires the same access levels, for example, a System Operator promoted to a Senior System Operator. In addition, for small entities, with limited staff, it may be necessary to allow access for duration to allow the entity to fill the vacant position and allow for sufficient training time.
No
The drafting team should clarify the Electronic Access Points in 1.3 and 1.5 are the Electronic Access Points identified in 1.2.
No
R2.2, the purpose of encryption is to protect the confidentiality and integrity data being transferred; the drafting team should simply require, "Require encryption for all interactive remove sessions." R2.3 requires multi-factor authentication for Interactive Remote Access. FEUS agrees with requiring multi-factor authentication; however, the reference document "Guidance for Secure Interactive Remote Access" states: "Multi-Factor Authentication Multi-factor authentication technologies use authentication factors from at least two of three generally accepted categories: something known (e.g., a password or personal identification number or PIN), something possessed (e.g., a one-time password token or a smart-card), and something unique about the user (e.g., fingerprint or iris pattern).6 Systems that use two or more factors are described as using multi-factor authentication; systems that use only two factors are described as using two-factor authentication. User IDs are not considered factors in a multi-factor authentication system." The drafting team should revise R2.3 to either define multi-factor authentication, allow a minimum of two-factor, or explicitly state a minimum of two factors.
No
R1.2 requires at least one physical access control to establish a one or more Defined Physical Boundaries that restricts access. The Measures for R1.2 require a physical security plan that describes how ingress and egress is controlled by one or more methods, proof access is restricted to authorized personnel accompanied by "card reader logs." The Change justification states specific examples have been moved to the Guidelines. The guidelines allow for alternate methods to log access. FEUS recommends the drafting team clarify if control and logging of ingress AND egress is required by R1.2 and remove "card reader" from the measures to allow for other means of logging. R1.3 Measures include a plan that describes how ingress and egress is controlled by two or more methods. The drafting team should clarify if ingress AND egress is required to be controlled by two or more methods. In addition, the drafting team should remove "card readers" to allow alternate means of logging. R1.5 requires, "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems." FEUS believes this requirement is vague as to its applicability. R1.1 applies to "Associated Physical Access Control Systems", R1.2 does not apply to "Associated Physical Access Control Systems", nor does R1.3. With the exception of R1.1, which applies to Low Impact BES Cyber Systems, there is not a requirement to establish a Defined Physical Boundary for the Physical Access Control System. Additionally, the applicability section of CIP-006-5 defines Associated Physical Access Control Systems as "Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems." The drafting team should either include associated Physical Access Control Systems to the applicability of R1.2 and R1.3 or eliminate R1.5.
No
FEUS recommends the drafting team define "continuous" or remove it from R2.1 Requirements and

Measures. The term continuous is not auditable. FEUS appreciates the changes made in R2.2 to allow for intermediate ingress and egress during the visit. However, for consistency, the drafting team should revise the date and time from “entry and exit” to “ingress and egress to the Defined Physical Boundary.”
No
R3 inclusive of R3.1 and R3.2 - the drafting team should clarify what Associated Access Control Systems it is applicable to (High/Medium/Low) and capitalize Locally Mounted Hardware or Devices.
No
The VSL should take into consideration a violation of Part 1.1 vs Part 1.2 and 1.3. R2 should remove “continuous” and refer to the entities escort policy.
Yes
No
The drafting team should clarify the requirement for R2.3 is only when the “remediation” can be concluded (the measures all point to evidence of installation/updates are completed) – If testing of a security patch the entity identifies the EMS does not operate properly when applied, R2.3 should not be applied until the EMS vendor supplies an additional update that is compatible.
Yes
No
The drafting team should consider revising R4.1.4 to “Any detected malicious activity.” The drafting team should add language from the rationale to clarify R4.3, “Detect and activate a response for event logging failures before the end of the next calendar day.” Clarify if this is the failure of the event logging system (SIEM) or the individual systems sending events to the SIEM.
No
FEUS supports the comments submitted by APPA. R5.6, FEUS recommends removing “generating alerts after a threshold of unsuccessful login attempts” as this is addressed in R4.1.
No
FEUS supports the comments submitted by APPA. FEUS shares the concerns with possible conflicts with CIP-008-5 and EOP-004-2. In addition, there definition of BES Cyber Security Incident states, “A malicious act or suspicious event that: Compromises, or was an attempt to compromise, the ESP; or disrupts or was an attempt to disrupt, the operation of a BES Cyber System; or Results in unauthorized physical access into a Defined Physical Boundary.” The measures for R1.1 include in relevant portion, “BES Cyber Security Incidents targeting the Defined Physical Boundary of a BES Cyber System.” The drafting team should revise the measure to align with the definition and include, that results in unauthorized physical access.
No
The drafting team should remove the requirement to “justify” deviations taken from the plan to align with the requirement. R2.2 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”
No
FEUS supports the comments submitted by APPA. R3.1 requires approval, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to

complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”

Yes

R1.4 states backup media shall be “verified initially after backup,” the terms verified initially are vague. Many automatic backup systems run a series of backups at different times and report if the backup was successful. FEUS recommends the drafting team revise R1.4 to state “verified the backup was successful by the end of the next business day.”

No

R2.1, R2.2, and R2.3 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…” The drafting team should clarify in R2.2 what includes “any information.” In addition, “and reflects current configurations” is not achievable and should be removed.

No

R3.1 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…” R3.1 requires the plan be reviewed when BES Cyber Systems are replaced; R3.4 requires the recovery plan be updated to address technology changes within thirty calendar days. FEUS recommends removing the requirement to review when BES Cyber Systems are replaced from R3.1 and including the statement in R3.4.

Yes

No

Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration within 30 calendar days of completing the change approved in 1.2."

FEUS supports comments submitted by APPA.

No

FEUS supports the comments submitted by APPA. R3.1 and 3.2 include the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”

Yes
No
See FEUS related comment on the definition of BES Cyber System Information. There is a minor typo for the headers in section 1.2. R1.3 includes the statement, “initially upon the effective date of the standard.” CAN-0012 addresses “Completion of Periodic Activity Requirements During Implementation Plan.” It is the intent the drafting team is establishing a bookend; however, the wording is implied the bookend must be completed on the effective date and may not occur prior/post the effective date of the standard. FEUS recommends revising the requirement to allow an entity to complete the “bookend” prior to or within a reasonable time of the effective date. Since the requirement states the ongoing activity must be completed, “at least once each calendar year thereafter, not to exceed 15 calendar months” it is reasonable to concede the requirement could be revised to state, “Initially upon the effective, not to exceed three months following, and at least each calendar year thereafter…”
No
The drafting team should clarify, as referenced in the guidelines, if the media is to be reused outside of the BES Cyber System it should be properly erased as required to allow for BES Cyber Systems to be temporarily removed and reused within the same environment.
Group
Edison Electric Insititute
David Batz
Yes
The Edison Electric Institute (“EEI”) submits this executive summary concerning the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards as published 11/7/2011. EEI is the association of the nation’s shareholder-owned electric utilities, international affiliates, and industry associates world-wide. EEI takes the subject of cyber security and infrastructure protection very seriously, and is committed to the reliability of the Bulk Electric System. This commitment includes timely completion of Version 5 and filing a comprehensive set of revisions to the CIP standards for approval with the Commission. EEI appreciates the significant level of effort on the part of the CS 706 Standards Drafting Team, NERC staff, and industry stakeholders in the development of revisions to the CIP standards. EEI has provided a considerable number of comments and suggestions for revisions and enhancements to the Draft of Version 5. These suggestions for revisions are intended to improve the clarity and quality of the Draft. We encourage members of the CS 706 Standards Drafting Team to have an open mind when considering stakeholder feedback, and be willing to closely review and potentially remove new mandatory security requirements that are not specifically required by FERC Order 706 or that fail to provide meaningful security enhancements at a cost that can be afforded by the consumers of electricity. Any proposed modifications to the CIP Standards should appropriately recognize the significant investment that the industry has already made in adopting CIP Version 1, 2 and 3. New or modified requirements should build upon and leverage existing security programs and investments. We observe that there are a significant number of stakeholders who have concerns about the proposed framework change in CIP-002-5 for identification of the cyber assets to be protected and concerns with extensive changes in definitions. We recommend that the SDT carefully evaluate alternative strategies offered by stakeholders to address these concerns. In addition, we observe that there are a significant number of stakeholders who have great concern about the new proposals regarding low-impact BES cyber assets, both as to appropriate identification, and concerning the new mandatory controls that have been identified for low impact BES cyber assets. Technical experts have broadly varying positions on whether these assets should be covered by the mandatory NERC standards, as well as the nature of the controls that should be applied. IT and security systems professionals also continue to struggle with the design of the NERC standards, a template that is not ideally suited to addressing IT systems issues. Rigid adherence to a set of static requirements may serve to bring “Compliance”, but “Compliance” in this sense is not necessarily equivalent to actual enhancements in the security posture, reduction of risk, or increasing the reliability of the Bulk Electric System. With regards to addition of new administrative requirements, many in the industry are concerned that the additional cost will bring little or no security benefit. The redefinition of annual, the added requirements for delegations, along with other new administrative

requirements will not enhance security and may divert finite resources to non-security related efforts. We recommend that the SDT continue to evaluate alternative strategies that would allow for addressing the outstanding FERC Order 706 directives in a manner that does not create a situation where the electric sector is expending disproportionate resources for compliance activities associated with low impact BES cyber assets in comparison to medium or high impact BES cyber assets. We recommend that any new mandatory security controls be closely scrutinized to ensure that they provide a meaningful increase in the security and reliability of the BES that is commensurate with the amount of resources that are required to establish and maintain them. In the event that new mandatory security controls are established for low impact BES cyber assets, we recommend that implementation deadlines for the low impact BES cyber assets, where appropriate, occur after implementation deadlines for medium or high impact BES cyber assets. • There have been significant changes in the basic terms and definitions which have been used since the inception of the CIP standards, including dropping core concepts such as Critical Assets, Critical Cyber Assets, Physical Security Perimeter, and substantial changes in definitions to remaining terms. These changes are not clearly required to support FERC Order 706, or to enhance the security controls within the Bulk Electric System. EEI proposes that approved definitions within the CIP Standard (pre-Version 5) are retained whenever possible. We understand any need to modify the definition to align with FERC Order 706 or enhance security, and would much prefer new definitions over any elimination or introduction of terms. EEI members are opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes and evidence. The removal of Physical Security Perimeter as a term (replaced by Defined Physical Boundary) is the primary example where the definition could be modified while retaining use of Physical Security Perimeter. • The loss of Critical Assets removes facilities from consideration. This presents challenges in assessing BES Cyber Systems as they provide services to a facility which provides BES Reliability Operating Services – not the BES Cyber System independently. This also introduces the approach in which BES Cyber Systems are not independently assessed for impact with consideration to the specific service they support, but are assigned the impact of the BES Reliability Service (conducted within a facility). The methodology should recognize the facility within impact assessment, and allow for subsequent entity assessment of the impact of any supporting BES Cyber System, whether they reside within facility or in another location in support of the facility. • Requirements and/or Measures that use all-encompassing words like 'any,' and 'all' introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional elements that would be out of scope should more concise language be used. • Extension of the default retention requirements within all the standards from the current 'previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation,' to 'three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation' is not identified within FERC Order 706 nor does it enhance security commensurate with resource expenditures. EEI members would prefer use of the current 'previous full calendar year' retention period. • BES Cyber Asset – Proposed Definition Change o Original Text – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. o Proposed Change – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the capability of the facility with which it is associated to perform one or more BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. o Rationale – Impact Ratings as defined within CIP-002-5 focus on the role of the facilities' function specific to BES Reliability Operating Services. The BES Cyber Assets support the facility in providing that service. • BES Cyber System – Proposed Content Change o Original Text – One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. o Proposed Change – One or more BES Cyber Assets that are logically grouped together to operate one or more BES Reliability

Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. o Rationale – Absent logical grouping, there is no clear understanding of how a BES Cyber Asset qualifies as a component of a BES Cyber System. Physical grouping could infer devices within a common rack, though they may provide quite different services within the facility. • BES Cyber System Information o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact Designations; equipment layouts that contain Medium or High BES Cyber System Impact Designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – The rewording clarifies the applicability (within CIP-011) of BES Cyber Information controls. • Defined Physical Boundary – Propose reverting back to (retaining) Physical Security Perimeter. The definition can be modified to remove the 'six-wall perimeter' criteria but from a documentation stand-point, requiring renaming what may be unchanged perimeters/boundaries is an additional resource constraint with no security (or compliance) benefit. The concept of physical security provides an excellent complement to electronic security to demonstrate 'defense in depth.' o Rationale – Retaining 'Physical Security Perimeter' allows existing compliance documentation to be used for instances where PSPs are identified within drawings and equipment layouts. • Inter-Entity Real-Time Coordination and Communication – Propose renaming this to 'Inter-Entity Real-Time Coordination' to avoid overlapping existing communication requirements within the COM standards. o Original Text ♣ Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Schedule interchange • Facility operational data and status • Operational directives o Proposed Change ♣ Activities, actions, and conditions necessary for the coordination between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination Service include, but are not limited to: • Schedule Interchange • Facility operational data and status • Reliability directives o Rationale – COM-002 is in the process of defining Reliability directives. This term would provide a more concise scope once the COM-002 definition has been finalized. • Add the following definitions (from CAN-0007) o Electronic Access – Access which allows a user to manipulate software and database (setting) attributes of a CCA by direct (primary) or indirect (from outside the ESP) methods. o Physical Access – Access which allows a user to manipulate hardware settings, and may allow the direct connection of a terminal or a computer that can be used to allow electronic access. o Revocation – Action that results in the inability of an individual to access the CCA. • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Protected Cyber Assets ♣ This term loses meaning in the context of Version 5 draft 1 definitions, given the loss of logical network qualification or any other means to assess 'associated.' Only with consideration of the network portion of an address can an entity determine whether a cyber asset qualifies as being within an ESP (where network portions of address are identical). o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter ♣ Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load

and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent, or be removed. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.
No
1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern a. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. EEI Members propose the following applicability to identify a more targeted scope: i. Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." 6. Attachment I - a. High Impact Rating – Propose content change i. Original content – Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at: ii. Proposed change – Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – Some devices may not reside within a Control Center, this rewording provides clarity to focus on assets located within a Control Center in support of BES Reliability Operating Services b. Medium Impact Rating – Propose content change i. Original Content – Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: ii. Proposed Change - Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below and not included in Section 1 above, that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – The proposed edits more directly connect with the facility and its function within the BES

Bright Line criteria. c. 2.2 – Propose content change i. Original content – An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). ii. Proposed change – Each transmission facility containing reactive devices with an aggregate net Reactive Power nameplate rating of 1000 MVAR or greater. iii. Rationale – the rewording provides the filter (for transmission only facilities) at the front to better identify the applicable Facility. d. 2.7 (Table) – The "Weight Value per Line" for 700 should be replaced with a value in the range of 500-600, which is more representative of the typical rating of 230 kV lines. e. 2.8, 2.9, 2.11 – "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clearly identified basis for why certain paths are included on this list. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to or greater than 1,500 MW." This catalog is actively maintained by WECC. f. 2.11 – The table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC. As an alternative, we suggest "Each SPS categorized as a 'Wide Area Protection System' by WECC" which is the newly created mechanism within WECC to identify SPS systems of significant importance.
No
1. General Observation – Since categorization is based on the facilities role within the BES, independent of the specific BES Cyber Asset or BES Cyber System Role, appropriate categorization fails to require assessment based on the criticality of the BES Cyber Asset or Cyber System in support of applicable BES Reliability Operating Services. 2. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been properly identified and categorized. 3. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale – EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame. 4. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale – The requirement only asks for Senior Manager (or delegate) approval. EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.
No
1 – The Violation Risk Factors do not intuitively align with Violation Severity Level (VSL). Requirement 1 assigns a 'High" VRF independent of the potential low or no risk associated with instances in which BES Cyber Assets or BES Cyber Systems are assigned risk levels higher than those required. EEI would like a more risk based approach in which the compliance assessment considers risk in any non-compliance finding. 2 – For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days
No
While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have "overall authority and responsibility for

leading and managing implementation of the requirements within this set of standards" would benefit from repetition within the R1 requirement itself. Reading 'solely' this standard post rationale removal does not communicate the responsibility adequately. Propose use of 'legacy' wording and numbering schemes within this standard where possible. In this context the cyber security policy requirements should be R1, with 'leadership' requirements being R2 – EEI proposes this be made R2.
No
EEI proposes that 'legacy' wording and numbering schemes be retained within this standard were possible with the change (within CIP-003-4 R1.1) from "addresses the requirements" to "addresses the topics." This requirement should be R1. Rationale – Pre-version 5 language already captures the requirement and has been successfully vetted within the industry. FERC Order 706 did not identify any specific need to change policy language, only to provide additional guidance. Use of the legacy language would minimize approval barriers by ensuring minimal change where appropriate as long as the 'addresses the requirement' language is removed. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.
No
This goes beyond the scope of FERC Order 706. In previous versions, this requirement was a sub-requirement within R1. EEI proposes renumbering/rewording this to capture the legacy context. Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry.
No
Propose legacy language/numbering from (pre-version 5) R1 1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale – EEI members indicated making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy.
No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706), which provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.
No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. EEI proposes the use of a more gradual scale

rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
Yes
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. R2.2-4 – Can possibly be merged into a single sub requirement a. 2.2 – training on the security controls b. 2.3 – training on the proper use of physical access controls c. 2.4 – training on the electronic access controls 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. 6. Propose merging of R2.7 with R2.9 7. (R2.10) – What changes are required to existing approved training programs to satisfy this new requirement?
No
Measure 3.1 where it calls for the date that access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. 4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. EEI proposes a clearer delineation to frame instances in which personal records are not readily available – vs. impossible to obtain 2. 4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. 4.3 a. Most EEI Members favored a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' c. 4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain BES Cyber Assets remotely.
Yes
No
1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary.' a. 'Minimum necessary' as identified as difficult to prove within an audit context. 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts, which do not provide enhanced security and may impact reliability efforts when recovery processes are activated. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead. 3. 6.4 – EEI proposes conducting this task on an annual basis as the quarterly requirement

will introduce extreme resource constraints in some instances.
No
1. 7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.
Yes
No
EEI believes the Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network, where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks. • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity" (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – 1. Modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Propose elimination of Associated Physical Access Control Systems as their introduction indicates applicability to subsequent subrequirements which doesn't add to overall security and presents extensive resource requirements. 2. Requirements – Propose content change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points (EAPs). 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.
No
1. Table R2 1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted traffic is decrypted prior reaching Electronic Access Points to allow for further access control would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.
No
1. Classifying instances where no documentation of compliance exists as severe is appropriate:

instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.

No

1. Table R1 a. R1.1 i. Applicability – 'Medium Impact BES Cyber Assets with no External Connectivity' should be added 1. Rationale - Medium Impact BES Cyber Assets should only require fully Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – Propose change 1. Original content – Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 2. Proposed change – Utilize two or more different physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 3. Rationale – 'different and complementary' does not provide adequate guidance. The Measure R1.3 only references 'different. ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that

describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.

No

Table R2 1. R2.1 a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. 2. R2.2 a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and

exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor's name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that 'round-the-clock' logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn't introduce additional requirements.
No
Table R3 1. R3.1 a. Overall observations – EEI members felt that the shift from (pre-V5) maintenance on 'mechanisms' to the Draft 1 'systems' expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered 'tested' in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.
No
2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence "The list could be sorted by BES Cyber System or source." It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. 4. 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. 5. 2.3 a. Requirement – As

currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed.

No

1. 3.2 a. Requirement – Content Change i. Original content – Disarm or remove identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. 3.3 a. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. b. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). c. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria 3. 3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. 3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append "to Medium or High Impact BES Cyber Assets or Associated Protected Cyber Assets" to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.

No

R4 1. 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. 2. 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report

showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. 4.3 a. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. 4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. 4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No

R5 1. 5.1 a. Overall – EEI and its members struggled with providing alternate wording for this subrequirement. In both the original content and proposed change there exists a instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required.

No
Violation Severity Levels 1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial paragraph doesn't align with a requirement, propose striking.
No
1. Rationale R1 1. The initial sentence is fragmented, providing an incomplete framing for R1. Absent a complete sentence, proposing alternate language to better frame this rationale is difficult. Propose rewriting this sentence. 2. Regarding applicability to all registered entities – While EEI Members understand the need for all entities to have an effective process to respond to incidents within each organization, for the purposes of CIP-008 it would be best to establish applicability to entities with Medium and High Impact BES Cyber Assets/Systems, as those are the impact ratings in which Defined Physical Boundaries and Electronic Security Perimeters are required. 3. R1.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 4. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 5. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
R2 1. 2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s)

annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).

No

1. R3 1. 3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.

No

1. R1 – Severe 1. 2nd paragraph, add ‘types’ to the end of the paragraph (…plan does not identify Reportable BES Cyber Security Incident types). 2. R2 – Severe 1. The second paragraph should be modified from “The Responsible Entity has not tested the execution of its BES Cyber Security Incident Response Plan” to “The Responsible Entity has not executed its BES Cyber Security Incident Response Plan” 2. Rationale – This paragraph aligns with R2.2 which requires activation or exercising the plan. The revised words better support requirement R2.2. 3. R3 1. High VSL (first paragraph) – Content change ♣ Original content • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. ♣ Proposed Change • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 60 calendar days of completion. ♣ Rationale – This VSL combines the review (3.2) with the update (3.3) requirement, the 60 days support the 3.3 requirement.

No
• Overall 1. Propose renaming this Standard to “Recovery Plans for BES Cyber Systems” 2. The revised structure of CIP-009-5 documents requirements for backup media in both R1 and R2. Creating a requirement in which backup media requirements are consolidated (in-line with version 3) would provide a more concise means to identify media requirements. The requirements (as proposed) would be as follows: 1. R1 – Recovery Plan 2. R2 – Exercise of the Recovery Plan 3. R3 – Backup Media 4. R4 – Maintaining the Recovery Plan 3. References to ‘implement’ should be changed to ‘exercise’ regarding recovery plans to better capture activation of the plan vs. ‘release and publish’ efforts. 4. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. • Introduction 1. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. 2. Applicability 3. Background • Requirements and Measures 1. R1 1. 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: ♣ Conditions for activation of the recovery plan ♣ Roles and responsibilities of the responders 2. 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. 3. 1.3 1. Requirement – Content Change ♣ Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality ♣ Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality ♣ Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: • Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 2. Measure – Content Change ♣ Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. ♣ Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 4. 1.4 – Correct headers from ‘part’ to ‘Applicability,’ ‘Requirements,’ and ‘Measures’ 1. 1.4 ♣ The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rationale – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. 5. 1.5 1. Requirement – Content Change ♣ Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the

functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.

No

1. 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. 3.2 1. Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. 3. 3.3 4. 3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit. 5. 3.5 2. Requirements – Content Change ♣ Original – Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed. ♣ Proposed Change – Updates to the recovery plan(s) shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of being completed. ♣ Rationale – The proposed change leverages ‘pre-version 5’ language which satisfies the intent of the requirement.

Yes

No

1. R1 1. Rationale – The current wording doesn’t capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed “prevent unauthorized modifications to BES Cyber Systems.” 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1

greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. R2 1. 2.1 1. Applicability – Propose removal of Medium Impact BES Cyber Systems. ♣ Rationale – The technology required to monitor/detect for changes is relatively new and not aligned to BES Cyber Systems which would be in place within a Medium Impact facility (substations, etc.). 2. Requirements – Propose content change ♣ Original Text – Where technically feasible, monitor for changes to the

baseline configuration (as defined per CIP-010_ R1, Part 1.1) and document and investigate the detection of any unauthorized changes. ♣ Proposed change – Where technically feasible, detect and document unauthorized changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1).
No
1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rationale • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rationale – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.3 4. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes

No
1. 1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text – One or more methods to identify BES Cyber System Information. ♣ Proposed Change – Implement one or more methods to identify BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 2. 1.2 1. Overall – Correct column header labels within the table. 2. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 3. Requirements – Propose content change ♣ Original Text – Access control and handling procedures for BES Cyber System Information. ♣ Proposed Change – Demonstration of access control for BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 3. 1.3 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. 3. Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No
1. 2.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. 2. 2.2 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.
No
R1 (Severe) – Propose removal of the first paragraph as it is mirrored within the subsequent paragraphs that better frame the violation.
No
The Edison Electric Institute (“EEI”) submits this executive summary concerning the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards as published 11/7/2011. EEI is the association of the nation’s shareholder-owned electric utilities, international affiliates, and industry associates world-wide. EEI takes the subject of cyber security and infrastructure protection very seriously, and is committed to the reliability of the Bulk Electric System. This commitment includes timely completion of Version 5 and filing a comprehensive set of revisions to the CIP standards for approval with the Commission. EEI appreciates the significant level of effort on the part of the CS 706 Standards Drafting Team, NERC staff, and industry stakeholders in the development of revisions to the CIP standards. EEI has provided a considerable number of comments and suggestions for revisions and enhancements to the Draft of Version 5. These suggestions for revisions are intended to improve the clarity and quality of the Draft. We encourage members of the CS 706 Standards Drafting Team to have an open mind when considering stakeholder feedback, and be willing to closely review and potentially remove new mandatory security requirements that are not specifically required by FERC Order 706 or that fail to provide meaningful security enhancements at a cost that can be afforded by the consumers of electricity. Any proposed modifications to the CIP Standards should appropriately recognize the significant investment that the industry has already made in adopting CIP Version 1, 2 and 3. New or modified requirements should build upon and leverage existing security programs and investments. We observe that there are a significant number of stakeholders who have concerns about the proposed framework change in CIP-002-5 for identification of the cyber assets to be protected and concerns with extensive changes in definitions. We recommend that the SDT carefully evaluate alternative strategies offered by stakeholders to address these concerns. In addition, we observe that there are a significant number of stakeholders who have great concern about the new proposals regarding low-impact BES cyber assets, both as to appropriate identification, and concerning the new mandatory controls that have been identified for low impact BES cyber assets. Technical experts have broadly varying positions on whether these assets should be covered by the mandatory NERC standards, as well as the nature of the controls that should be applied. IT and security systems professionals also continue to struggle with the design of the NERC standards, a template that is not ideally suited to addressing IT systems issues. Rigid adherence to a set of static requirements may serve to bring “Compliance”, but “Compliance” in this sense is not necessarily equivalent to actual enhancements in the security posture, reduction of risk, or increasing the

reliability of the Bulk Electric System. With regards to addition of new administrative requirements, many in the industry are concerned that the additional cost will bring little or no security benefit. The redefinition of annual, the added requirements for delegations, along with other new administrative requirements will not enhance security and may divert finite resources to non-security related efforts. We recommend that the SDT continue to evaluate alternative strategies that would allow for addressing the outstanding FERC Order 706 directives in a manner that does not create a situation where the electric sector is expending disproportionate resources for compliance activities associated with low impact BES cyber assets in comparison to medium or high impact BES cyber assets. We recommend that any new mandatory security controls be closely scrutinized to ensure that they provide a meaningful increase in the security and reliability of the BES that is commensurate with the amount of resources that are required to establish and maintain them. In the event that new mandatory security controls are established for low impact BES cyber assets, we recommend that implementation deadlines for the low impact BES cyber assets, where appropriate, occur after implementation deadlines for medium or high impact BES cyber assets.
Group
PNM Resources (Includes Public Service Co. of New Mexico and Texas New Mexico Power
Michael Mertz
Yes
• The proposed definition of BES Cyber Asset has not addressed the interpretations that have clarified “Cyber Asset” in previous versions of the standard. Without clarifying the term “Cyber Asset” it will continue to result in inconsistent application of the standards. • The term BES Cyber System may include cyber assets and communication equipment and networks that are not owned and or operated by a NERC registered entity. Furthermore these assets and networks are beyond the statutory authority of FERC or NERC, and are regulated by other regulatory bodies. The terms in this document cannot be used to expand regulatory authority. The definition should be revised to exclude WAN communication systems utilized by the BES Cyber Systems similar to the exclusion in existing versions of the standard. • BES Cyber System-the term is ambiguous and will result in inconsistent application of the standards. It will be difficult for entities to determine where one “system” ends and another “system” begins. For example, where does an Energy Management “System” end, at the front end processors, the RTU’s, the I/O? Where does the substation automation system begin? These are both presumably examples of BES Cyber Systems. • The definition of BES Cyber System contains the term “Maintenance Cyber Asset”, which is not a defined term. It appears as though it should be “Transient Cyber Asset”. • The definition of BES Reliability Operating Services is lengthy and confusing. There is concern that it will be difficult to audit to this definition and that it conflicts with the established bright line criteria. • The definition of CIP Exceptional Circumstance should include the word “may” to read “A situation that may involve one or more….” • There have been significant changes in the basic terms and definitions which have been used since the inception of the CIP standards, including dropping core concepts such as Critical Assets, Critical Cyber Assets, Physical Security Perimeter, and substantial changes in definitions to remaining terms. These changes are not clearly required to support FERC Order 706, or to enhance the security controls within the Bulk Electric System. EEI proposes that approved definitions within the CIP Standard (pre-Version 5) are retained whenever possible. We understand any need to modify the definition to align with FERC Order 706 or enhance security, and would much prefer new definitions over any elimination or introduction of terms. EEI members are opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes and evidence. The removal of Physical Security Perimeter as a term (replaced by Defined Physical Boundary) is the primary example where the definition could be modified while retaining use of Physical Security Perimeter. • The loss of Critical Assets removes facilities from consideration. This presents challenges in assessing BES Cyber Systems as they provide services to a facility which provides BES Reliability Operating Services – not the BES Cyber System independently. This also introduces the approach in which BES Cyber Systems are not independently assessed for impact with consideration to the specific service they support, but are assigned the impact of the BES Reliability Service (conducted within a facility). The methodology should recognize the facility within impact assessment, and allow for subsequent entity assessment of the impact of any supporting BES Cyber System, whether they reside within facility or in another location in support of the facility. • Requirements and/or Measures that use all-encompassing words like ‘any,’ and ‘all’ introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional

elements that would be out of scope should more concise language be used. • Extension of the default retention requirements within all the standards from the current 'previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation,' to 'three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation' is not identified within FERC Order 706 nor does it enhance security commensurate with resource expenditures. EEI members would prefer use of the current 'previous full calendar year' retention period. • BES Cyber Asset – Proposed Definition Change o Original Text – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. o Proposed Change – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact the capability of the facility with which it is associated to perform one or more BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. o Rationale – Impact Ratings as defined within CIP-002-5 focus on the role of the facilities' function specific to BES Reliability Operating Services. The BES Cyber Assets support the facility in providing that service. • BES Cyber System – Proposed Content Change o Original Text – One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System. o Proposed Change – One or more BES Cyber Assets that are logically grouped together to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. o Rationale – Absent logical grouping, there is no clear understanding of how a BES Cyber Asset qualifies as a component of a BES Cyber System. Physical grouping could infer devices within a common rack, though they may provide quite different services within the facility. • BES Cyber System Information o Original Text - Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans. o Proposed Change – Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain Medium or High BES Cyber System Impact Designations; equipment layouts that contain Medium or High BES Cyber System Impact Designations; BES Cyber System recovery plans; and BES Cyber System incident response plans. o Rationale – The rewording clarifies the applicability (within CIP-011) of BES Cyber Information controls. • Defined Physical Boundary – Propose reverting back to (retaining) Physical Security Perimeter. The definition can be modified to remove the 'six-wall perimeter' criteria but from a documentation stand-point, requiring renaming what may be unchanged perimeters/boundaries is an additional resource constraint with no security (or compliance) benefit. The concept of physical security provides an excellent complement to electronic security to demonstrate 'defense in depth.' o Rationale – Retaining 'Physical Security Perimeter' allows existing compliance documentation to be used for instances where PSPs are identified within drawings and equipment layouts. • Inter-Entity Real-Time Coordination and Communication – Propose renaming this to 'Inter-Entity Real-Time Coordination' to avoid overlapping existing communication requirements within the COM standards. o Original Text ♣ Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Schedule interchange • Facility operational data and status • Operational directives o Proposed

Change ♣ Activities, actions, and conditions necessary for the coordination between Responsible Entities to ensure the reliability and operability of the BES. ♣ Aspects of the Inter-Entity Coordination Service include, but are not limited to: • Schedule Interchange • Facility operational data and status • Reliability directives o Rationale – COM-002 is in the process of defining Reliability directives. This term would provide a more concise scope once the COM-002 definition has been finalized. • Add the following definitions (from CAN-0007) o Electronic Access – Access which allows a user to manipulate software and database (setting) attributes of a CCA by direct (primary) or indirect (from outside the ESP) methods. o Physical Access – Access which allows a user to manipulate hardware settings, and may allow the direct connection of a terminal or a computer that can be used to allow electronic access. o Revocation – Action that results in the inability of an individual to access the CCA. • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated • Existing definitions that would benefit from alternative wording o Protected Cyber Assets This term loses meaning in the context of Version 5 draft 1 definitions, given the loss of logical network qualification or any other means to assess 'associated.' Only with consideration of the network portion of an address can an entity determine whether a cyber asset qualifies as being within an ESP (where network portions of address are identical). o Electronic Access Point ♣ EAPs typically have two (or more) access points and control access into an ESP (logical network) from a less trusted network or communication interface. The current wording could be applied to any port on a network switch within an ESP and fails to focus on interfaces where traffic does flow from a less trusted network to a more restricted network within an ESP. o Electronic Security Perimeter Suggest retaining the concept of logical network. This provides an easier means to identify "Associated Protected Cyber Assets" as they could be any cyber assets on the same logical network which are not identified as a BES Cyber Asset or BES Cyber System.

Yes

• Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent, or be removed. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.

No

1. Applicability – (4.2.1 and 4.2.2) reference to UFLS and UVLS is a point of concern a. Current wording implies that every distribution feeder which is part of a UV or UF load shedding scheme is now in scope, with all distribution level devices now BES Cyber Assets. This may greatly expand the scope greatly into the distribution level. EEI Members propose the following applicability to identify a more targeted scope: i. Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) under a common control system as required by its regional load shedding program. 2. CIP-002-5 R1 – Propose content change a. Original Content – Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] b. Proposed change - Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. Low Impact BES cyber systems support Bulk Reliability Operating Services but are not mentioned in the bright line criteria as noted in Attachment 1. However, failure of these cyber systems may adversely impact (i.e. not remain in the NERC prescribed category ranges) the voltage and/or frequency of the connected Bulk Electric System. Low Impact BES Cyber Systems do not require discrete identification. [Violation Risk Factor: High][Time Horizon: Operations Planning] c. Rationale – The original definition, as worded, creates the impression that all other cyber assets qualify as Low Impact, and does not communicate the

criteria within the definition of BES Cyber Asset as a cyber asset that "if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The proposed rewording contributes towards ensuring only assets which have an impact on the BES are the focus of the CIP Standards (and may ensure a more rapid adoption of the Version 5 Standards). 3. The "Rationale – R1" box uses the term "Cyber Systems," which is not a formal term. Suggest changing the case to avoid confusion. 4. The last sentences of R1 and M1 conflict with each other, providing mixed messages specific to Lower Impact BES Cyber Systems/Assets. While Requirement 1 implies there is no need for discrete identification, Measurement 1 discusses evidence for categorizing Low Impact BES Cyber Assets/Systems. 5. Requirement 1.1 a. There is a missing word – "…within 30 calendar days of <when> a change to BES Elements and Facilities is placed into operation. b. The Term "BES Elements and Facilities" used only once within the standards. Suggest changing this phrase to "BES Cyber Assets or Systems." 6. Attachment I - a. High Impact Rating – Propose content change i. Original content – Each BES Cyber Asset or BES Cyber System that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services used by and located at: ii. Proposed change – Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – Some devices may not reside within a Control Center, this rewording provides clarity to focus on assets located within a Control Center in support of BES Reliability Operating Services b. Medium Impact Rating – Propose content change i. Original Content – Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services for: ii. Proposed Change - Each BES Cyber Asset or component of a BES Cyber System located at the facilities listed below and not included in Section 1 above, that if rendered unavailable, degraded or misused would, within 15 minutes adversely impact the reliable operation of any of the following: iii. Rationale – The proposed edits more directly connect with the facility and its function within the BES Bright Line criteria. c. 2.2 – Propose content change i. Original content – An aggregate net Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). ii. Proposed change – Each transmission facility containing reactive devices with an aggregate net Reactive Power nameplate rating of 1000 MVAR or greater. iii. Rationale – the rewording provides the filter (for transmission only facilities) at the front to better identify the applicable Facility. d. 2.7 (Table) – The "Weight Value per Line" for 700 should be replaced with a value in the range of 500-600, which is more representative of the typical rating of 230 kV lines. e. 2.8, 2.9, 2.11 – "Major WECC Transfer Paths in the Bulk Electric System" is not actively maintained by WECC and there is no clearly identified basis for why certain paths are included on this list. As an alternative, we suggest "transmission paths contained in the WECC Path Rating Catalog with a maximum path rating equal to or greater than 1,500 MW." This catalog is actively maintained by WECC. f. 2.11 – The table titled "Major WECC Remedial Action Schemes (RAS)" is not actively maintained by WECC. As an alternative, we suggest "Each SPS categorized as a 'Wide Area Protection System' by WECC" which is the newly created mechanism within WECC to identify SPS systems of significant importance.

No

1. General Observation – Since categorization is based on the facilities role within the BES, independent of the specific BES Cyber Asset or BES Cyber System Role, appropriate categorization fails to require assessment based on the criticality of the BES Cyber Asset or Cyber System in support of applicable BES Reliability Operating Services. 2. Rationale R2 – Propose a content change: a. Original Text - The lists required by R1 are reviewed once a year to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. b. Proposed Change - The lists required by R1 are reviewed annually to ensure that all BES Cyber Systems have been properly identified and categorized. 3. R2 – Proposed Change a. Original Text – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. b. Proposed Change – The Responsible Entity shall have its CIP Senior Manager or delegate annually approve the identification and categorization required by R1. c. Rationale – EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is

conducted in an entity standardized time-frame. 4. M2 – Proposed Change a. Original Text – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems. (R2) b. Proposed Change – Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate annually approve, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems. (R2) c. Rationale – The requirement only asks for Senior Manager (or delegate) approval. EEI members propose instances in which tasks are required to be completed in advance of the effective date of the standard be captured within the implementation plan. By adopting the CAN-0010 definition of annual, each entity can focus on ensuring this review is conducted in an entity standardized time-frame.

No

For the Last Paragraph VSL's within R1 (failed to update its documentation), EEI proposes the following time periods: Lower – More than 30, but less than or equal to 60 calendar days Moderate – More than 60, but less than or equal to 70 calendar days High – More than 70, but less than or equal to 80 calendar days

No

While it is documented within the definition, as referenced in the Rationale for R1 the Senior Management, the requirement that the senior manager have "overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" would benefit from repetition within the R1 requirement itself. Reading 'solely' this standard post rationale removal does not communicate the responsibility adequately. Propose use of 'legacy' wording and numbering schemes within this standard where possible. In this context the cyber security policy requirements should be R1, with 'leadership' requirements being R2 – EEI proposes this be made R2.

No

EEI proposes that 'legacy' wording and numbering schemes be retained within this standard were possible with the change (within CIP-003-4 R1.1) from "addresses the requirements" to "addresses the topics." This requirements should be R1. Rationale – Pre-version 5 language already captures the requirement and has been successfully vetted within the industry. FERC Order 706 did not identify any specific need to change policy language, only to provide additional guidance. Use of the legacy language would minimize approval barriers by ensuring minimal change where appropriate as long as the 'addresses the requirement' language is removed. Sub-numbering (1.1 through 1.10) should be modified to 2.1 through 2.10.

No

This goes beyond the scope of FERC Order 706. In previous versions, this requirement was a sub-requirement within R1. EEI proposes renumbering/rewording this to capture the legacy context. Propose content Change 1. Original Content – Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2. Proposed change –The cyber security policies require annual review and approval by the senior manager assigned pursuant to R1. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 3. Rationale – The proposed revision carries forward language from previous versions of the standard (CIP-003 R1.3) which captures the root intent while providing language which has already been vetted and approved within the industry.

No

Propose legacy language/numbering from (pre-version 5) R1 1. Draft 1 content – "Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function." 2. Proposed revision – "The cyber security policy is readily available to all personnel who have electronic access or unescorted physical access to, or are responsible for Medium or High Impact BES Cyber Systems." 3. Rationale – EEI members indicated making individuals who have access 'aware of elements' of the cyber security policy does not provide adequate guidance to ensure said individuals comply with the cyber security policy.

No
Requirement 5 – propose use of legacy language: • The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, standards. Rationale – Overall responsibility and authority (from the legacy language) can accomplish "direct and comprehensive responsibility" and "clear authority" (from FERC Order 706), which provides flexibility without the prescriptive requirement for the senior manager or delegate to be responsible for all individual detailed approvals and authorizations in the standards. Citing "all approvals and authorizations" as a Senior Manager was identified as a concern as it is open ended. There were concerns of the additional administrative burden which is not commensurate with the security benefits. Neither the Blackout Report Recommendation 43 nor FERC Order 706 identify the need to establish this administrative overhead. For Security and Reliability NERC should be concerned with the outcome of the approval process, that is, the proper authorizations are being granted by the Responsible Entity which is contained in the other CIP Standards.
No
Propose use of legacy language from CIP-003-3 R2.2: Changes to the senior manager must be documented within thirty calendar days of the effective date.
No
R4 VSL 1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. EEI proposes the use of a more gradual scale rather than a single instance of non-access subject to a High VSL, and total non-access (for all) being a Severe VSL.
Yes
No
1. The rationale for R2 should be reworded from "…contains the proper policies…" to "…covers the required policies…" 2. This extends beyond the guidance of FERC Order 706. Paragraph 435 of the order calls for identifying what "role and steps should be taken by the ERO to ensure quality and consistency of trainers." This requirement should identify what areas of the standards that the training program must include. 3. EEI members question whether this requirement satisfies paragraph 434 of Order 706 where "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security. 4. R2.2-4 – Can possibly be merged into a single sub requirement a. 2.2 – training on the security controls b. 2.3 – training on the proper use of physical access controls c. 2.4 – training on the electronic access controls 5. R2.6 – Requirement – Proposed word change a. Original - Training on handling of BES Cyber System Information and storage media. b. Proposed Change - Training on handling of BES High and Medium Impact Cyber System Information and storage media. c. Rationale – Rewording supports the applicability section. Since Low Impact Cyber Systems are not applicable, information specific to Low Impact Cyber Systems should not be in scope. 6. Propose merging of R2.7 with R2.9 7. (R2.10) – What changes are required to existing approved training programs to satisfy this new requirement?
No
Measure 3.1 where it calls for the date that access was first granted is a point of concern for both legacy employees (where it may be impossible) as well as new access since existing technology may not adequately capture and retain this information. Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
1. 4.1 a. Version 5 standards should indicate whether previous PRA's would be valid for this requirement (especially within the context of 'initial'). b. EEI proposes a clearer delineation to frame

instances in which personal records are not readily available – vs. impossible to obtain 2. 4.2 – Retention requirements do not extend beyond 3 years, creating confusion regarding retention of 7 year cycle background checks. 3. 4.3 a. Most EEI Members favored a process approach over a fixed pass/fail approach independent of the individual or circumstances involved, and propose that the SDT shift away from a criteria based approach. b. The application guideline provides guidance where it is 'not possible to perform a full seven year criminal history check.' c. 4.4 – Provide language to cover contract employees where I9 verification can only be conducted by employers. Service providers also may have instances where certain individuals may be located in another country, and may access certain BES Cyber Assets remotely.

Yes

No

1. R6.1-3,6.4-6 – Propose use of language where access is appropriate for the roles and responsibilities rather than 'minimum necessary.' a. 'Minimum necessary' as identified as difficult to prove within an audit context. 2. 6.3 – Propose content change a. Original content – The CIP Senior Manager or delegate shall authorize access to BES Cyber System Information, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions. b. Proposed change – Access to BES Cyber System Information repositories must be authorized, except for CIP Exceptional Circumstances. c. Rationale – Senior Manager authorization (or management of delegations) provides additional resource and response impacts, which do not provide enhanced security and may impact reliability efforts when recovery processes are activated. Ensuring access is authorized will satisfy security controls without adding unnecessary overhead. 3. 6.4 – EEI proposes conducting this task on an annual basis as the quarterly requirement will introduce extreme resource constraints in some instances.

No

1. 7.1 - There are questions in instances where resignations and/or terminations may be retroactive, which would introduce a challenge with revocation 'at the time of' events. 2. 7.2 – Transfers or reassignments should frame access changes when no longer needed rather than the date of the transfer (as cited in the Measure (i)). 3. 7.3 – Propose use of 'approved BES Medium and High Impact Cyber System Information repositories,' to frame an appropriate location in which information can be managed and controlled.

Yes

No

The Version 5 approach (as described within the R1 rationale "Summary of Changes") of focusing on discrete Electronic Access points rather than a logical perimeter adds confusion when determining Associated Protected Cyber Assets. A discrete list fails to recognize the inherent controls and permissions within a logical network. Control of routable protocol should consider the inherent network/host identifiers embedded within the addressing scheme in which all devices with an identical network component of their address are peers within a logical network, where access points do not serve as access control. Rationale for R1 – Propose content change • Original Text - The Electronic Security Perimeter serves to control and monitor traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks. • Proposed Change - The Electronic Security Perimeter serves to control traffic at the external boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic according to a specified rule set, and assists in containing any successful attacks. • Rationale – Monitoring is not identified within any R1 requirements. Table R1 1. R 1.1 1. Applicability - Propose use of "External Connectivity" instead of "External Routable Connectivity" (to include dial-up capability). 2. Propose removal of "and have been implemented" from the end of the measure statement to avoid tracking compliance on a 'per-device' basis, otherwise this would introduce the need for tracking this information for low impact BES Cyber Systems. 2. R 1.2 1. Applicability – 1. Modify to frame applicable Cyber Systems/Cyber Assets as those with External Connectivity. 2. Propose elimination of Associated Physical Access Control Systems as their introduction indicates applicability to subsequent subrequirements which doesn't add to overall security and presents extensive resource requirements. 2. Requirements – Propose content

change 1. Original content – Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs). 2. Proposed change – Control and secure all External Connectivity through the use of identified Electronic Access Points (EAPs). 3. Rationale – The focus within CIP-005 should be on EAP devices with External Connectivity. 3. R 1.3 1. Requirements – proposed change 1. Original Text - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting or denying access permissions. 2. Proposed Change - Require explicit inbound and outbound access permissions at each identified Electronic Access Point using routable protocols, including explicit criteria for granting access, denying all other access requests by default. 4. R1.4 – There were various interpretations of 'non-Interactive Remote Access,' which implies this requirement may need some additional clarification. This seems to be the only requirement where documentation of authentication measures appears within this standard. Consider removing 1.4 and modifying 1.2 to cover both rows.

No

1. R2.1 1. Requirements – Request rewording to support placement of an intermediary device that may not be part of an ESP. 2. R2.2 1. Requirements – Propose clarification on viable termination points for encrypted traffic to support unencrypted traffic through Electronic Access Points. 2. Rationale – The ability to filter traffic effectively becomes much more difficult if the traffic is encrypted. Supporting technical implementation where encrypted traffic is decrypted prior reaching Electronic Access Points to allow for further access control would benefit security capabilities. 3. Overall – Propose breaking table R2 into a Routable and Dial-Up categories to more effectively frame routable controls and dial-up controls without introducing confusion for the alternate approach.

No

1. Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding (page 17, bottom Severe VSL). 2. VSLs addressing 'each identified EAP' and 'all Interactive Remote Access' should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.

No

1. Table R1 a. R1.1 i. Applicability – 'Medium Impact BES Cyber Assets with no External Connectivity' should be added 1. Rationale - Medium Impact BES Cyber Assets should only require fully Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Rewrite 1. Original Text – Evidence may include, but is not limited to, documented operational and procedural controls exist and have been implemented. 2. Proposed Change – Evidence may include, but is not limited to, documented operational or procedure controls that have been implemented. b. R1.2 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Measures – Proposed Change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs. 2. Proposed Change – Evidence may include, but is not limited to, language in the physical security plan that describes the physical boundaries and how access is controlled. 3. Rationale – FERC Order 706 did not ask for egress access controls. The additional criteria at the end of the measure extend beyond what FERC has asked for, with minimal security benefit. c. R1.3 i. Requirement – Propose

change 1. Original content – Utilize two or more different and complementary physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 2. Proposed change – Utilize two or more different physical access controls to establish one or more Defined Physical Boundaries that restricts physical access to only those users that are authorized, where technically feasible. 3. Rationale – 'different and complementary' does not provide adequate guidance. The Measure R1.3 only references 'different. ii. Measure – only mentions 'different' access control methods with no reference to complementary (as included within the requirement). d. R1.4 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirement – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. 3. Rationale – The 15 minute criteria (Referenced in the 'Table of Compliance Elements,' page 21, R1 – High) provides greater clarity to satisfy alerting requirements. iii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs, or other evidence that documents that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access through any access point in a Defined Physical Boundary and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. e. R1.5 i. Requirements – proposed change 1. Original Text – Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 2. Proposed Change – Issue alerts within 15 minutes (to individuals responsible for response) in response to unauthorized physical access to Physical Access Control Systems. 3. Rationale – The 15 minute criteria (referenced in the 'Table of Compliance Elements,' page 20, R1 – High) provides greater clarity to satisfy alerting requirements. ii. Measures – proposed change 1. Original Text – Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs or other evidence that these alerts were generated. 2. Proposed Change - Evidence may include, but is not limited to, language in the physical security plan that describes the issuance of alerts in response to unauthorized physical access to Physical Access Control Systems and additional evidence that these alerts were issued, such as alert logs, cell phone or pager logs. f. R1.6 i. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." 1. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. ii. Requirements – Proposed Change 1. Original Text – Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual and date of entry. 2. Proposed Change – Log (through automated means or by personnel who control entry) of authorized individual's physical entry into each Defined Physical Boundary protecting applicable BES Cyber

Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the authorized individual and date of entry. 3. Rationale – The addition of authorized provides additional segmentation from R2 (Visitor Control) access requirements.
No
Table R2 1. R2.1 a. Applicability – Applicability wording of “Medium Impact BES Cyber Assets should be changed to “Medium Impact BES Cyber Assets with External Connectivity.” i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. 2. R2.2 a. Applicability – Applicability wording of “Medium Impact BES Cyber Assets” should be changed to “Medium Impact BES Cyber Assets with External Connectivity.” i. Rationale - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attack vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor’s name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor’s name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that ‘round-the-clock’ logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn’t introduce additional requirements.
No
Table R3 1. R3.1 a. Overall observations – EEI members felt that the shift from (pre-V5) maintenance on ‘mechanisms’ to the Draft 1 ‘systems’ expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered ‘tested’ in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted ‘prior to commissioning.’ Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective. 2. Compliance a. 1.5.2 – Evidence retention should keep the existing 90 day period for physical access logs as extending this to 3 years can create extensive commitment in storage media, particularly for video monitoring.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or

use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage.

No

2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence "The list could be sorted by BES Cyber System or source." It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. 4. 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. 5. 2.3 a. Requirement – As currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed.

No

1. 3.2 a. Requirement – Content Change i. Original content – Disarm or remove identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. 3.3 a. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. b. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). c. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria 3. 3.4 a. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. b. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. 3.5 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems and Associated and they do not appear to be Transient Cyber Asset related. b. Requirements – Append "to Medium or High Impact BES Cyber Assets or Associated

Protected Cyber Assets" to the end of the requirement. c. Measures – Content Change i. Original Text – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change - Evidence may include, but is not limited to, logs showing when Transient Cyber Assets were connected to Medium or High Impact BES Cyber Assets or Protected Cyber Assets.
No
R4 1. 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. 2. 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. 4.3 a. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. 4. 4.4 a. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. 4.5 a. Requirements – Content Change i. Original Content – Review a summarization or sampling of logged events every two weeks to identify unanticipated BES Cyber Security Incidents and potential event logging failures. Activate a response to rectify any deficiency identified from the review before the end of the next calendar day. ii. Proposed Change - Review a summarization or sampling of logged events every two weeks to identify BES Cyber Security Incidents and potential event logging failures. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008. b. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), signed and dated documentation showing the review occurred, and dated evidence showing that personnel were dispatched or a work ticket was opened to rectify the deficiency. ii. Proposed Change – Evidence may include, but is not limited to, documentation describing the review, any findings from the review (if any), and signed and dated documentation showing the review occurred. iii. Rationale – Since CIP-007 R4 should focus on Security Monitoring, ensuring the monitoring is adequately conducted (in advance of any incident response actions) should be at the core. Subsequent incident response actions are addressed within CIP-008.

No
a. Overall – EEI and its members struggled with providing alternate wording for this subrequirement. In both the original content and proposed change there exists a instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required.
No
1. R3 a. Propose switching High and Severe Columns as the High captures instance in which no methods were deployed, Severe captures instances in which incomplete methods were deployed. b. The initial paragraph in Severe is duplicated in High. 2. R4 a. Moderate – delete 'identify and implement methods to' b. High – delete 'identify and' 3. R5 a. High – The initial paragraph doesn't align with a requirement, propose striking.
No
1. Rationale R1 1. The initial sentence is fragmented, providing an incomplete framing for R1. Absent a complete sentence, proposing alternate language to better frame this rationale is difficult. Propose rewriting this sentence. 2. Regarding applicability to all registered entities – While EEI Members understand the need for all entities to have an effective process to respond to incidents within each organization, for the purposes of CIP-008 it would be best to establish applicability to entities with Medium and High Impact BES Cyber Assets/Systems, as those are the impact ratings in which Defined Physical Boundaries and Electronic Security Perimeters are required. 3. R1.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 4. R1.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 5. R1.3 1. Requirements ♣ The initial 'define' should be expanded to provide a complete sentence (i.e. An entities BES Cyber Security Incident Response Plan should include). 2. Measures – Content Change ♣ Original • Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communications processes or procedures. ♣ Proposed Change • Evidence may include, but is not

limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that address roles and responsibilities of; o BES Cyber Security Incident response personnel, o BES Cyber Security Incident handling processes or procedures, o Communications processes or procedures.
No
R2 1. 2.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist. 2. Requirements – Content Change ♣ Original Content • When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test. ♣ Proposed Change • When a BES Cyber Security Incident occurs, the incident response plans must be used and include recording of deviations taken from the plan during the incident. 2. 2.2 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – Since the measure frames this sub-requirement to identify, classify, and respond to BES Cyber Security Incidents targeting the ESP or DPB, it is appropriate to frame applicability to environments in which ESPs and DPBs (are required to) exist.. 2. Requirements – Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. 3. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 3. R2.3 – Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No
1. R3 1. 3.1 1. Applicability – Content Change ♣ Original Applicability • All Responsible Entities ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control and Monitoring Systems • Associated Protected Cyber Assets ♣ Rationale – The formal definition of BES Cyber Security Incident includes attempts to compromise the ESP or DPB, requiring Medium or High Impact BES Cyber Systems/Assets. 2. 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣

Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 3. 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.

No

1. R1 – Severe 1. 2nd paragraph, add 'types' to the end of the paragraph (…plan does not identify Reportable BES Cyber Security Incident types). 2. R2 – Severe 1. The second paragraph should be modified from "The Responsible Entity has not tested the execution of its BES Cyber Security Incident Response Plan" to "The Responsible Entity has not executed its BES Cyber Security Incident Response Plan" 2. Rationale – This paragraph aligns with R2.2 which requires activation or exercising the plan. The revised words better support requirement R2.2. 3. R3 1. High VSL (first paragraph) – Content change ♣ Original content • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. ♣ Proposed Change • The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 60 calendar days of completion. ♣ Rationale – This VSL combines the review (3.2) with the update (3.3) requirement, the 60 days support the 3.3 requirement.

No

• Overall 1. Propose renaming this Standard to "Recovery Plans for BES Cyber Systems" 2. The revised structure of CIP-009-5 documents requirements for backup media in both R1 and R2. Creating a requirement in which backup media requirements are consolidated (in-line with version 3) would provide a more concise means to identify media requirements. The requirements (as proposed) would be as follows: 1. R1 – Recovery Plan 2. R2 – Exercise of the Recovery Plan 3. R3 – Backup Media 4. R4 – Maintaining the Recovery Plan 3. References to 'implement' should be changed to 'exercise' regarding recovery plans to better capture activation of the plan vs. 'release and publish' efforts. 4. Actions required in advance of the implementation date (2.1, 2.2) should be removed from the standard(s) and included within the implementation plan. • Introduction 1. Purpose – Proposed Content Change 1. Original Content – Standard CIP-009-5 ensures that recovery plan(s) related to the storing of backup information are put in place for BES Cyber Assets and BES Cyber Systems and that these plans support and follow established business continuity and disaster recovery techniques and practices. 2. Proposed Change – Standard CIP-009-5 ensures that recovery plan(s) are put in place for BES Cyber Assets and BES Cyber Systems. 2. Applicability 3. Background • Requirements and Measures 1. R1 1. 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: ♣ Conditions for activation of the recovery plan ♣ Roles and responsibilities of the responders 2. 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. 3. 1.3 1. Requirement – Content Change ♣ Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality ♣ Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality ♣ Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: • Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 2. Measure – Content Change ♣ Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. ♣ Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. ♣ Rationale – Protection of BES Cyber System Information is addressed within CIP-011. 4. 1.4 – Correct

headers from ‘part’ to ‘Applicability,’ ‘Requirements,’ and ‘Measures’ 1. 1.4 ♣ The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that ‘The Commission does not believe that every change will necessitate verification of the backup and restoration processes’ from paragraph 740. ♣ Propose ‘new’ sub requirement applicable to High Impact BES Cyber Systems to require: • Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. ♣ Propose rewrite • Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. • Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. • Rationale – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. 5. 1.5 1. Requirement – Content Change ♣ Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. ♣ Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. ♣ Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.
No
1. 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
1. 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and

document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. 2. 3.2 1. Requirements – Content Change ♣ Original – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned. ♣ Proposed Change – Review the results of each recovery plan test or actual incident recovery within thirty calendar days of completion, documenting any identified deficiencies or lessons learned. 3. 3.3 4. 3.4 – Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit. 5. 3.5 2. Requirements – Content Change ♣ Original – Communicate all recovery plan updates to each individual responsible under R1.2 for the recovery plan efforts within thirty calendar days of the update being completed. ♣ Proposed Change – Updates to the recovery plan(s) shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of being completed. ♣ Rationale – The proposed change leverages 'pre-version 5' language which satisfies the intent of the requirement.

Yes

No

1. R1 1. Rationale – The current wording doesn't capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed "prevent unauthorized modifications to BES Cyber Systems." 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar

days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. R1 1. Rationale – The current wording doesn't capture the intent of FERC Order 706, paragraph 399: 1. We do not seek absolute assurances but rather are concerned that there be processes in place that permit a reasonably high level of confidence modifications do not have unintended consequence. 2. Suggest referencing this directive within the rationale, and ensure configuration management focus more on the spirit of the FERC Order rather than the currently framed "prevent unauthorized modifications to BES Cyber Systems." 2. R1.1 a. CIP-010-1 R1.1 should be replaced with CIP-003-4 R6 i. Rationale – CIP-010-1 R1.1 is too prescriptive. CIP-003-4 R6 is closer to a results based requirement and provides more flexibility to achieve the desired results. CIP-010-1 R1.1 greatly expands the scope of change control and configuration management (CIP-003-4 R6) beyond what was directed in FERC Order 706. FERC Order 706 paragraphs 397 and 398 directed "modifications to CIP-003-1 R6 to provide an express acknowledgement of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes." The concern was that some form of verification is performed to detect when authorized changes have been made. CIP-010-1 R2.1 addresses Order 706's concern for some form of verification to detect unauthorized changes. (CIP-010-1 R2.1 should delete reference to the baseline defined in CIP-010-1 R1.1.) FERC also did "not believe the changes will have burdensome consequences." CIP-010-1 R1.1 requires extensive and burdensome details tracking. Effective automated tools for detecting changes (authorized and unauthorized) are available to address Order 706's concern and some of these tools do not require the burdensome, prescriptive details as proposed in R1.1. 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 3. R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale

– Citing a “change advisory board” within the measure overly represents adequate evidence in support of the requirement. 4. R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 5. R1.5 1. Requirements – Propose content change ♣ Original Text • 1.5.1 – Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment, including a description of the measures used to account for any difference in operation between the test and production environments. ♣ Proposed Change • 1.5.1 – Prior to implementing any change from the existing baseline configuration in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and • 1.5.2 – Document the results of the testing and the differences between the test environment and the production environment. ♣ Rationale – Proposed rewording provide greater focus on the root requirements. 2. Measures – Propose content change ♣ Original Text – Evidence includes, but is not limited to, a list of security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test. ♣ Proposed Change – Evidence includes, but is not limited to, a list of security controls tested along with the date of the test, test results, and a list of differences between the production and test environments.

No

1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rationale • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we’ve removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Overall – There needs to be clear segmentation from ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rationale – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production

environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.3 4. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.

Yes

No

1. 1.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text – One or more methods to identify BES Cyber System Information. ♣ Proposed Change – Implement one or more methods to identify BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 2. 1.2 1. Overall – Correct column header labels within the table. 2. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 3. Requirements – Propose content change ♣ Original Text – Access control and handling procedures for BES Cyber System Information. ♣ Proposed Change – Demonstration of access control for BES Cyber System Information. ♣ Rationale – Additional wording frames this in a more complete manner. 3. 1.3 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems •

Medium Impact BES Cyber Systems with External Routable Connectivity • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • The additional qualifier of 'external routable connectivity' eliminates Medium Impact BES Cyber Systems that are not accessible outside of the BES facility, so information specific to these devices do not provide a means to compromise given the existing requirements for physical protection. This removes additional resources which could be better leveraged in other compliance efforts. • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed content change ♣ Original Text - Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. ♣ Proposed Change – Annually assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. 3. Measures – Proposed content change ♣ Original Text – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence to demonstrate that the action plan was implemented. ♣ Proposed Change – Evidence may include, but is not limited to, documented review, assessment results, action plan, and evidence of the status of the action. ♣ Rationale – Rewording allows for action plans which may be 'in progress' towards implementation, capturing instance in which remediation may rely on deliverables (not yet received) by vendors.

No

1. 2.1 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts. 2. Requirements – Proposed Change ♣ Original Content – Prior to the release for reuse of BES Cyber Asset media, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the media. ♣ Proposed Change – Prevent the unauthorized retrieval of BES Cyber System Information from BES Cyber Asset media prior to the release of BES Cyber Asset media for reuse. ♣ Rationale – While not directly changing the intent of the requirement, this rewording has been suggested to provide greater clarity of the root requirement. 2. 2.2 1. Applicability – Proposed Change ♣ Original Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems • Associated Protected Cyber Assets ♣ Proposed Applicability • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems • Associated Physical Access Control Systems • Associated Electronic Access Control or Monitoring Systems ♣ Rationale • Associated Protected Cyber assets were removed as they alone cannot (by definition) affect BES Reliability Operating Services without unauthorized access to Medium (or High) BES Cyber Systems. This removes additional resources which could be better leveraged in other compliance efforts.

No

R1 (Severe) – Propose removal of the first paragraph as it is mirrored within the subsequent paragraphs that better frame the violation.

No

The existing time frame of 18 months is too short, given the extensive enhancements within the standards as a whole, and particularly specific to the likely addition of numerous Low Impact BES Cyber Systems that may not have been considered in scope for previous versions. In the event that Low Impact assets are a component of the enforceable requirements on day 1, there is little doubt the implementation time would extend considerable beyond 18 months. References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. This occurs in the following

sections: 1. CIP-002 a. R2 b. M2 2. CIP-003 a. R3 3. CIP-008 a. R2.2 b. M2.2 c. R3.1 4. CIP-009 a. R2.1 b. R2.3 c. M2.3 d. R3.1 e. M3.1 f. VSL (High-R2) g. VSL (Severe-R2) h. VSL (Severe-R3) 5. CIP-010 a. R3.1 b. R3.2 6. CIP-011 a. R1.3 b. VSL (High-R1)
Individual
Andrew Z. Pusztai
American Transmission company, LLC
Yes
American Transmission Company (ATC) endorses EEI's comments on the proposed Definitions.
Yes
American Transmission Company (ATC) endorses EEI's comments on CIP-002-5 Standards. In addition, ATC is submitting comments for CIP-002-5 Attachment 1. Criterion 2.8 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLs and their associated contingencies' with wording of, '. . . as Facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more IROL violations', like the wording using in Criterion 2.11. Criterion 2.9 – (1) Use the term 'Planning Coordinator' rather than 'Planning Authority" to be consistent with the rest of the standard and current NERC practice. (2) Replace the less clear wording of '. . . as critical to the derivation of IROLS and their associated contingencies' with wording of, '. . . as FACTS that if destroyed, degraded, misused, or otherwise rendered unavailable, could cause the violation of one or more IROLs', like the wording using in Criterion 2.11. Criterion 2.12 – (1) Replaced the word, 'system' with 'common control system' to clarify that this criterion applies to a system triggered by a single (common) control, rather than a program (system) of many independent relays set to trip at the same frequency.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-002-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-002-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments regarding the VRFs and VSLs.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R5 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R6 of CIP-003-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-003-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-004-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-004-5 Standard.
No

American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-004-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R6 of CIP-004-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R7 of CIP-004-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-005-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-006-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R4 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R5 of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-007-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on VRFs and VSLs of CIP-008-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-009-5 Standard.

No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-009-5 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-009-5 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-010-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-010-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R3 of CIP-010-1 Standard.
Yes
No
American Transmission Company (ATC) endorses EEI's comments on R1 of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on R2 of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments VRFs and VSLs of CIP-011-1 Standard.
No
American Transmission Company (ATC) endorses EEI's comments on the proposed Implementation Plan for the CIP Standards.
Individual
David S. Revill
Georgia Transmission Corporation
Yes
In the definition of BES Cyber System, it should refer to "Transient Cyber Asset" instead of "Maintenance Cyber Asset." GTC also recommends that the definition include the phrase "at the discretion of the Responsible Entity" as follows: One or more BES Cyber Assets that are typically grouped together at the discretion of the Responsible Entity, logically or physically, to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. In the definition of BES Reliability Operating Services, GTC is concerned that this definition is overly complex and would be better served in a guidance document. GTC recommends the definition consist of the first sentence and move the remaining information to guidance as follows: BES Reliability Operating Services: BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). GTC is concerned that the definition of BES Cyber System Information is too broad and overreaching. GTC recommends that the drafting team research other information frameworks such as PII. Specifically, GTC recommends that the definition look at information in aggregate (such as multiple elements of a security configuration) rather than information minutia (such as a single IP address). GTC recommends that the drafting team consider revising the definition for Control Center. GTC is concerned that a single RTU that also operates a remote line switch does in fact "support real-time operations by a System Operator for two or more…transmission facilities, at two or more locations." In the definition of Defined Physical Boundary, the term "Electronic Access Control Systems" should be "Electronic Access Control or Monitoring Systems." In the definition of Electronic Access Point, GTC recommends the definition be as follows: "An interface on a Cyber Asset that controls routable or dial-up data communications between Cyber Assets" In the definition of Physical Access Control Systems, GTC disagrees with the need to change the definition as it existed in version 3. GTC recommends that the previous wording be used as follows: "Cyber Assets that authorize or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers." GTC also believes cameras should

be added to the list of excluded devices and those devices should be excluded if they are at or outside of the Defined Physical Boundary, not just AT the boundary. The definition of Electronic Access Control or Monitoring Systems is substantially the same as under CIP version 3. It has been interpreted by at least some regions to include the systems of Managed Security vendors, even if they only perform monitoring and alerting functions (no access control) and if they are a backup to the entity's own systems. This discourages entities from utilizing these services because it is extremely difficult to monitor and enforce a third party's compliance with the standards. The end result is a reduced use of these services which increases risk and reduces reliability. Consider specifically excluding vendor systems as long as they do not perform access control or at least if they both do not perform access control and are a backup to and entity's primary logging and alerting system. As written, the definition of External Connectivity would include communication between two of an entity's BES Cyber Assets if they are within different ESPs. This should not be included in the definition. The definition of Interactive Remote Access does not address how the word "Interactive" should be interpreted. This is an important element of the term because there is dispute about whether or not read-only access should be included in the definition. The definition should specifically include or exclude read-only access so that the industry has the opportunity to weigh in on the issue. In the definition of "Intermediate Device" the words "may" and "may be" should be changed to "is". Otherwise a device might be included if it is capable of providing those services even if it is not intended to do so and is not configured to do so. The sentence "Intermediate devices are sometimes called proxy systems is inappropriate". Certainly a proxy system could serve as an Intermediate device, but not all proxy systems would qualify. Conversely there are other devices (such as VPN termination devices) that are not generally thought of as proxy systems that could serve as an Intermediate device. Accordingly the sentence adds confusion instead of clarity to the definition. In the definition of Transient Cyber Asset item 2 should be expanded by adding Vulnerability Assessment. Devices used for a VA are perfect examples of the type of systems that should be included in this definition but do not clearly fall under any of the other categories.

Yes

We disagree with the need to modify the criteria from those already approved by industry in version 4 of CIP-002. We recommend the drafting team revert the criteria to those previously approved. Additionally, we are concerned that some of these criteria may in fact extend beyond the definition of BES that is in the process of being developed. This would create a situation where a NERC defined “BES Cyber Asset” may in fact not be part of the BES. GTC disagrees with the inclusion of “Transmission Owner” in criteria 1.3 and 2.13. The functional model indicates that the Transmission Owner has no real time obligations. As such, a control center used to perform the functional obligations of the Transmission Owner cannot, by definition, have a real-time impact on the reliable operation of the BES. Additionally, none of the functional obligations of the Transmission Owner, as described in the NERC Reliability Functional Model, could be performed by a control center. We do agree, however, that a Transmission Owner may, in fact, have a control center that is performing obligations of a Transmission Operator without being registered as such. We believe this case should be clarified in a footnote to the criteria and Transmission Owner be stricken. GTC is concerned that thresholds are being used inconsistently in Attachment I. Specifically, generation is only included as a Medium Impact if it is above 1500MW. However, generation control centers are included at a much lower threshold: 300MW. 300MW is used in regards to UFLS and UVLS schemes. However, we believe the importance of these schemes to the BES to be fundamentally different than simply the loss of a specific amount of load or generation. As such, we suggest the drafting team modify criteria 2.13 to only include generation control centers greater than 1500MW as a medium impact. Also, in section 1.2 of the Compliance Section, the word compliant is spelled incorrectly.

Yes

No

GTC is concerned with the manner in which the drafting team has chosen to handle the bookending of requirements throughout the standard. The phrase “initially upon the effective date” may lead to confusion in the industry as to exactly what is expected. Dictionary.com defines “upon” as “immediately or very soon after.” This could lead one to believe that everywhere this phrase is used, the approval must be made precisely on the effective date and that an approval obtained prior to the effective date would be considered non-compliant.

Yes
No
GTC is concerned that this requirement requires the implementation by policy of security controls for Low Impact BES Cyber Assets that are not required elsewhere in CIP-004 though CIP-011 (e.g. Configuration Change Management and Information Protection).
No
See response to question #4.
No
GTC believes that this requirement should be removed from CIP-003 and included as an element of the required training program in CIP-004. This would have the effect of eliminating a previously approved requirement, but GTC believes this is justified as the objective of the requirement is being met through including it in the required training program.
Yes
Yes
GTC is not sure that there is a strong reliability objective to this requirement as it stands and suggests that this language be combined with R1 and R5, eliminating R6.
Yes
No
The requirement should clarify that some roles may not include all requirement parts in their training program.
GTC notes that the guidance material appears to be out of sync with the requirement.
No
GTC disagrees with requirement parts 7.4 and 7.5 as they relate to Medium Impact BES Cyber Systems. The vast majority of Medium Impact BES Cyber Systems are field IEDs such as RTUs and Relays. The passwords on these devices are typically designed with safety of operations in mind and not security. As such, revocation of physical and remote access provides the only reliability benefit in the majority of cases and the revoking of individual credentials or shared account passwords provides no reliability benefit and may in fact harm reliability. Many of these devices require that the entire configuration be redeployed on the device (which typically requires a device restart) in order to modify the password. This has the unfortunate side effect of temporarily impacting situational awareness and increases risk to the BES. As such, GTC suggests that Medium Impact BES Cyber Systems be eliminated from the applicability on 7.4 and 7.5.
The applicability for the “Associated Physical Access Control Systems” is unclear. Are these PACS associated with the Low Impact BES Cyber Assets or those of Medium and High Impact BES Cyber Assets?
In requirement part 3.2, are “access control, logging, and alerting systems” the same as or something different than Physical Access Control Systems? If they are the same, GTC recommends consistent language. If they are different, please clarify.

In 1.2, "document" should be "documentation of" Requirement 1.4.1 should be more focused; more detail on what types of “security controls” are included is needed. Security controls are a key element of other parts of this standard as well and therefore need to be very clearly defined. Requirement 1.4.3 should be deleted. Documenting the test results is something you do to provide evidence of compliance; it does not promote reliability. If you do not document the test results you will not be able to show compliance with 1.4.2, but it is not fair for the same act to also constitute violation of 1.4.3.
How would an entity monitor for changes in physical location; does this require RFID of each asset? This requirement should allow flexibility between monitoring or annual validation, perhaps as part of the VA process.
Individual
Steve Karolek
Wisconsin Electric Power Company
Yes
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In the definition of "CIP Exceptional Circumstances", consider providing examples of impediment of large scale workforce availability such as a work slowdown, strike or pandemic.
Yes
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In High Impact Rating criteria 1.4 on page 15, the phrase "...that includes control of one or more of the assets..." should be changed to match the definition of Control Center, which requires the control of two or more assets. • Control Centers should be capitalized at the end of section 2.13 on page 17. • There should also be a column for LSE in the table provided on page 18. • On page 20, under the category "Balancing Load and Generation," Non-spinning reserve, the use of 'ramp rates' is typically associated with modeling programs not typically used as real time operation information and should be removed. • Managing constraints (page 21) has an extra bullet that should be removed. • Restoration of BES – 'coordination' all by itself lacks context and should include additional words to better frame the intent. • Inter-Entity Coordination and Communication – In additional to the recommend removal of 'communication' from the section, this should also include BA within the Operational Directives.
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 1.1 discusses changes that are "...intended to be in service for more than 6 calendar months..." It may be extremely difficult to document such intention to the satisfaction of an audit team. Wisconsin Electric Power Company requests that the Standards Drafting Team revisit this requirement and reword it to ensure it is actually auditable.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2 and Measure 2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. If the Guidelines and Technical Basis section will remain in the final published version of the standard, the table on page 18 should be updated to include the Entity Registration of Load Serving Entities with consideration of an "X" in the functional rows of "Dynamic Response", "Balancing Load and Generation" and "Controlling Voltage".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Measure 1, the bulleted items should be separated by ", or,". The requirement for designation to be made by a "high level official" is too vague. Designation of the CIP Senior Manager should be made by an officer of the company.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): If this requirement and measures are retained, the second measure should be further defined to identify acceptable (auditable) evidence that the ten topics were implemented. In the Guidelines and Technical Basis for Requirement 2, review the third bullet of section 2.4 and consider changing the phrase "ingress and egress" to the word "access" since monitoring and logging egress is not intended.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2 and Measure 2 contain the phrase "…initially upon the effective date…". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The wording of Requirement 3 could be interpreted to mean that there are two annual events to track, a review event and an approval event. Wisconsin Electric Power Company requests that the Standard Drafting Team consider wording changes to clarify that the annual review and approval is considered to be a single event.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The bulleted list in Measure 4 should be separated by ", or," between each bulleted item. The last bulleted item should define the periodicity of training as annual. Consider whether the word "contactors" in the second bulleted item should be changed to "contractors".
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 6, review the use of the word "change2" and consider changing this to "change". Also, in Rationale 6, review the use of the word "authoritv" and consider changing this to "authority".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Table R4, part 4.2 on page 17, delete the phrase "regardless of duration". It adds nothing to the meaning since there is a six month exception for certain addresses. Suggested new wording for this requirement would be: "Seven year criminal history records check in each county of residence, including any temporary residences where the individual lived away from a permanent residence while attending school for at least six months or while working for at least six months. A permanent residence is one which would be used when filing a state or federal income tax return. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed." Our rationale for this wording is that it clarifies that the county criminal court is the level of jurisdiction at which the inquiry must be made. This is distinct from the local municipal level, the state level or the federal level. It recognizes that some individuals travel to pursue education or employment and that they establish temporary residences in dormitories, apartments and motel rooms while away from a permanent residence. It allows individuals to seek, and employers to send personnel to, training or temporary work for up to six months without invoking a need to expand the scope of the PRA.
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The lists in Measures 6.1, 6.2, 6.3, 6.5 and 6.6 do not follow the conventions for either numbered lists or bulleted lists. Based on the context, Wisconsin Electric Power Company recommends that these be formatted as bulleted lists, with the bullet items separated by ", or,". The bulleted list in Measure 6.4 should have the bullet items separated by ", or,". In the measures for Requirement 6.4, we would appreciate clarification to explain the difference between the two bullet items, which are extremely similar.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The lists in Measures 7.1, and 7.2 do not follow the conventions for either numbered lists or bulleted lists. Based on the context, Wisconsin Electric Power Company recommends that these be formatted as bulleted lists, with the bullet items separated by ", or,". The bulleted list in Measure 7.5 should have the bulleted items separated by ", or,". The items in Measures 7.3 and 7.4 should be formatted as

bulleted lists, with the bullet items separated by ", or,".
No
Wisconsin Electric Power Company agrees that the requirement to revoke access when access is no longer needed is essential to the safe and reliable operation of the BES. We accept that we must establish effective and reliable systems to achieve that result and that we must be able to demonstrate our compliance with the requirement. We commit to establishment of an environment of a culture of compliance that strives for error-free results. However, in-service transfers and reassignments and out-of-service transitions are an area where many organizations have difficulty implementing effective and reliable controls. Not every such transaction begins with an individual informing their employer that they will be leaving service in 30 days. We can provide many examples if needed. We assert that planned, orchestrated out-of-service, reassignment and transfer events are less common than FERC suggests in Order 706, paragraph 461. And even fewer occur under the direct scrutiny and awareness of the security organizations responsible for compliance. In any larger organization, there is no single person or work group with complete situational awareness of every potential HR event. Because we are aware of this risk, we establish controls that deal with the planned, orchestrated events. We insert ourselves into existing automated information flows. We issue periodic awareness messages. We create tracking systems to time stamp events. We train supervisors and HR staff. We even add personnel to our organizations dedicated to NERC CIP compliance. However, this is an area of compliance that relies on habits and human memory, not automated systems that generate alerts and exception reports. It asks HR personnel and broadly dispersed supervisors to have high situational awareness of the impact of each personnel decision on authorization for access to NERC assets. Due to these compliance risks, we believe that the expectations established in the VSL for R7 are unreasonably high. In support of this position, we cite the Commission's own language in paragraph 461 which states in part, "...MOST organizations will know in advance..." (emphasis added), and "We understand that outlying elements may require some brief lag before denial of access is effective...". We believe this demonstrates the Commission's knowledge and understanding that error-free compliance is unlikely and that exceptions will occur. It is unfair to demand that reasonably anticipated exceptions should lead to sanctioned violations. We suggest instead that "Severe VSL" should read: "The Responsible Entity did not have a documented process for access revocation." And that "High VSL" should read: "The Registered Entity had a documented process for access revocation but failed to follow it for more than (some number of) personnel." And that the "Moderate VSL" should read: "The Registered Entity had a documented process for access revocation but failed to follow it for more than (some smaller number of) personnel." The measures for R7 should then include documents sufficient to demonstrate that the process was documented and followed, but achievement of the time threshold was delayed and why.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Measures 1.2 and 1.3, the words "and egress" should be removed. The current standard does not require logging exit transactions and no significant benefit accrues from establishing such a requirement. In Measure 1.6, the time of entry should be shown in addition to the date.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments

submitted by Edison Electric Institute for this question (with the following exceptions/additions): If these requirements are to remain in the standard, the requirement in Table R3 part 3.1 on page 18 would be better if split into two requirements, one for maintenance and one for testing. In Table R3 part 3.2 on page 18, in the applicability column, "Associated Physical Access Control or Monitoring Systems" should be changed to "Associated Physical Access Control Systems".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 2.3, the bullet items in the measures column should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In requirement 3.2, the bullet list items in the measures column should be separated by ", or,". In requirement 3.3, the measures should be a bullet list, not a numbered list, and the bullet list items should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): In Requirement 4.3, the numbered list items should be separated by ", and,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 5.6 has the potential to generate many TFEs and should include language stating that a TFE is not required for those devices where this is not technically feasible.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The measures for Requirement 1.3 should be written as a bulleted list with bullet items separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 2.3 and Measure 2.2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures for requirement 2.2 should be written as a bullet list with bullet items separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 3.1 contains the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would

not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures for requirement 3.1 should be written as a numbered list with ", and," between each bullet item. The measures for requirement 3.3 should be written as a numbered list with ", and," between each bullet item.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirements 2.1 and 2.3, and Measure 2.3 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 3.1 and Measure 3.1 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
The severity levels for Requirement 2 and Requirement 3 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): The requirements in Table R1, Part 1.1 on page 10, as a numbered list, should be separated by ", and,". The measures in Table R1, Part 1.1 on page 10, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.2 on page 11, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.3 on page 12, as a bulleted list, should be separated by ", or,". The requirements in Table R1, Part 1.4 on page 13, as a numbered list, should be separated by ", and,". The requirements in Table R1, Part 1.5 on page 14, as a numbered list, should be separated by ", and,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No

Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirements 3.1 and 3.2 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures in Table R3, Part 3.1 on page 29, as a bulleted list, should be separated by ", or,".
Yes
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): Requirement 1.3 contains the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year. The measures in Table R1, Part 1.1 on page 10, as a bulleted list, should be separated by ", or,". The measures in Table R1, Part 1.2 on page 11, as a bulleted list, should be separated by ", or,".
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question (with the following exceptions/additions): VSLs for Requirement 1 contain the phrase "...initially upon the effective date...". We are very concerned that this could be interpreted to mean exactly upon the effective date of the standards, which would not be practical due to the many instances of this wording throughout the standards. We propose that all initial compliance requirements be stipulated in the implementation plan, perhaps to have been completed during the calendar year the standards become effective and prior to the effective date. An effective date in January should require initial compliance in the preceding calendar year.
No
Wisconsin Electric Power Company has participated in the development of, and supports, comments submitted by Edison Electric Institute for this question.
Group
Seattle City Light
Kevin Cyr
Yes
"EAP" should be dropped from the Standards. EAP actually stands for "Extensible Authentication Protocol" which was officially coined by RFC 3748 back in 2004. Cyber security standards should use standard terminology and certainly should not make up terms that conflict with existing cyber security terms.
Yes
A bright-line approach does not contain hypothetical conditions. The approach outlined by CIP-002-5 Attachment 1 does not provide a “bright-line” procedure for categorizing cyber assets or systems. “15 minutes” is arbitrary to cyber security and is an invalid measure for categorization. To illustrate this, apply the CIP-002-5’s proposed guideline to different scenario. The card payment industry (PCI) doesn’t ask “If the misuse of a system can result in stolen credit card numbers within 15 minutes…” and the health care industry doesn’t ask the same question about the disclosure of personal healthcare information. The arbitrary nature of the proposed approach simply shifts the “voluntary

compliance" problem from asset categorization to cyber asset categorization. "Most of these criteria are similar to those already approved by the industry as part of Version 4" suggests that the criteria are fine because they were previously approved. The approvals of CIP v1, v2, and v3 show the flaw of this logic. Additionally, Version 4 has not been tested.
No
This requirement contradicts basic regulatory compliance principles and will lead to conflict between regulators and entities. During audit, the regulators will ask for evidence that all cyber assets and systems were identified and categorized. The entity cannot prove this if identification records aren't maintained for low impact cyber assets.
Yes
No
The severity levels are determined by, among other things, the number of low impact cyber assets that are categorized improperly. The entity is not required to keep records of low impact cyber assets. This approach will not work.
Yes
Yes
Yes
This requirement implies that to be compliant entities will need to maintain an inventory of job functions and the track the roles of all personnel at all times. This will add significant administrative overhead to entity operations without significantly adding to cyber security.
No
The measures imply that a hard-copy signature is necessary to demonstrate approval. Corporate emails, digital signatures, and other formats should be included. The CIP requirements should not dictate how an entity conducts internal approvals.
No
SCL seconds APPA's comment.
Yes
Yes
No
In addition to the new tracking implicitly required by CIP-003-5 R4, the entities will also need to track the access roles for all personnel. This adds an additional facet to track without adding value to the current awareness and training requirements. Eliminate the overlaps between CIP-003-5 R4 and CIP-004-5 R2 and simplify the approach.
Yes
No
This requirement is not effective from a regulatory perspective because it lacks decision criteria for evaluation. As long as the entities have discretion in how they evaluate the PRA results, they should also have discretion in determining what information the PRA should include.
Yes
No
The CIP requirements should not specify that the CIP Senior Manager has the ultimate authority over the access approvals for an organization's assets. This contradicts the segregation of duties concept and should be removed. A single person should not have authority over monitoring a critical business process while also having an operational role in the same process. Also, the CIP requirements should

not dictate how an entity chooses to set up its management structure and the associated authority related to internal business operations.
No
Regarding rapid removal of access, FERC Order 706 Paragraph 460 and 461 also states, “outlying elements may require some brief lag before denial of access is effective, in which case, the circumstances justifying such lag must be documented for audit purposes.” The proposed requirement does not address delays in access revocation and is not reasonable. Additionally, compliance with the proposed short revocation timelines will require highly matured access management programs and systems. Such programs don’t grow and mature overnight. A medium sized organization would require 3-5 years to implement access management processes and systems to meet this obligation.
Yes
No
Regarding R1.2, this requirement states that each cyber system or asset must have an EAP between itself and all its neighbors. If this is not the intent of the requirement, then it needs to include the term “externally routable.” Additionally, the language needs to be clear enough to allow for an isolated network to have multiple subnets or networks without an EAP at each hop. This point will become increasingly relevant with the growing popularity of virtualization. Regarding R1.3, this requirement obviously refers to firewall functionality and should use the proper terminology. According to Wikipedia, a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass is called a “Firewall.” Permissions on a firewall typically refer to console access, and Access Control Lists (ACL) are the rules that govern ingress and egress traffic. "Require explicit...permissions" and "including explicit criteria" hints that a stateful and/or application firewall is required. Network traffic cannot be allowed or denied based on “explicit” anything without inspecting the traffic. This requirement is technically inaccurate and vague. Regarding R1.5, this requirement is not aligned with the rest of the Standard regarding remote access and provides opportunities for worthless monitoring. The requirement should not dictate where the monitoring points should be installed for several reasons. First, encryption is required for remote access but this Standard allows for the encryption termination point to be located anywhere (this issue is further addressed under the relevant requirement.) For example, if the termination point is behind the firewall then you’ll be monitoring encrypted traffic (this is impossible.) Second, if the outside interface of the firewall is on a public network (or even a poorly governed private network) and the monitoring point is also on the outside interface then there won’t be any monitoring value without a corresponding internal monitoring agent. Placement of monitoring agents should be determined by a security practitioner that is knowledgeable about their unique network. Even with expertly selected placement locations of monitoring, successful implementations usually require tuning and experimenting with different monitoring locations. There is not a valid cookie-cutter approach to monitoring design, especially given the restraints of the other vague requirements of this Standard.
No
This requirement appears to be incomplete. The addition of encryption to the Standards is more than overdue but is unfortunately missing the mark. Encryption is of little to no value with a poorly designed implementation. First, allowing the encryption termination to occur outside of the firewall while disallowing direct connections to the target cyber asset means that unencrypted authentication traffic is allowed from outside the firewall (potentially on a public or poorly managed private network.) The requirement does not mention anything about encryption types or strengths. Additionally, the requirement does not address key management which is equally important as the encryption itself. Also, reference to a guideline published separately from the requirements is up until now, not a good idea as the regulators are very quick to point out that “NERC guidelines are guidelines, not requirements.” All applicable and allowable configurations need to be included in the requirement or provide entities with full discretion for their remote access implementations.
Yes
No
SCL seconds APPA’s comments.

Yes
Yes
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
No
SCL seconds APPA's comments.
Yes
Yes
Yes
Yes

No
SCL seconds APPA's comments.
Individual
John Tolo
Tucson Electric Power
No
TEP is concerned that there is not adequate definition of a "facility", and how this differs from a Critical Asset in prior versions.
No
It is TEP's opinion that the changes to the bright-line criteria from Version 4 to Version 5, particularly #2.7 requiring the aggregate of all lines would have a large impact .
No
It is TEP's opinion that the asset identification and categorization process defined in the Attachment and the Guidance is not clear. It appears to go from specific cyber assets to general systems or facilities to determine level. This would appear to result in an inventory of every asset at every facility rather than just those determined to have an impact level of high or medium. It is our opinion that this approach should be reversed. In addition, the guidance does not clearly define the steps required for the process of asset identification, resulting in a great deal of confusion.
No
Senior Manager approval should only be necessary for identified BES Systems or BES Cyber assets.
Yes
Yes
Yes
Agree with requirement, comment is regarding Guidance. Concern with Guidance on having a policy regarding Remote Access, specifically "Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating remote access."
Yes
Yes
Yes
Yes
Yes
Yes
No
Concern is with 2.10 – "Training on BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets", which is based on the FERC Order 706 paragraph 434: "clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets. CIP-004-1 should leave no doubt that cyber security training concerning a critical cyber asset should encompass the electronic environment in which the asset is situated and the attendant vulnerabilities. Any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security. TEPC does not feel that 2.10 adequately conveys the order. Suggested wording:

“Training on BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets to the extent a person with access could put critical assets at risk through their actions, whether intentionally or accidental.”
Yes
Yes
TEP would like to see additional guidance on denial criteria.
Yes
Yes
Rationale for R6 is confusing. Paragraph 4 addressing the quarter reviews states “individuals actually provisioned to a BES Cyber System”. Then it states that “focus is on the integrity of provisioning access rather than individual accounts on all BES Systems”. Please provide clarification on which method of review is intended.
Yes
TEP suggests using the term “access revocation” instead of “access removal” in the measures section of 7.1, 7.3, 7.4. We do not feel the definitions are the same and the intent is revocation.
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request that the intention expressed in the Rationale statement for R1.1 be clearly included in the Requirement which is vague as written. Suggest: “Define technical or procedural controls to restrict unauthorized electronic access so as Low Impact BES Cyber Systems are segregated from public or less trusted network zones.” Additionally, the concept of aggregation that is included in the Rationale is not defined elsewhere in the CIP Standards, which seems inconsistent. If this concept is to be considered here, it should be introduced in CIP-002. Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? For Requirement for R1.3, it is unclear why the Applicability for High Impact BES Cyber Systems does not include the reference to “with External Routable Connectivity” but it does for Medium Impact. What is the intended difference? Does this imply impacts to serial connectivity? If so, should the requirement clearly state that? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? The Rationale includes reference that the IDS must be separate from the Firewalls (2 distinct). If so, the Requirement should state that. From another point of view, if the intention is real time response detection, that could be stated without requiring that the method be IDS.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend removing from M2.3 the statement "Note that a UserID is not considered an authentication factor." If needed, add to definitions.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
TEP requests a clarification as to whether the 30 day window is in reference to the “Change Rationale for Requirement R2.3.
Yes
No
TEP feels that, for Requirement R4.5, a 2 week window for sampling of logged events is too burdensome due to the number of unique logging systems. A monthly process would be reasonable.
No
For Requirement R5.4, TEP is concerned that this applies to Low Impact BES Cyber Systems. In addition, the requirement contains the statement, “For the purposes of this requirement an inventory of Cyber Assets is not required.” How would the TFE be managed without a list of assets impacted? Has the impact of requiring TFEs for every device within every BES critical asset been determined?
Yes
Yes
Yes
No
For Requirement R3.4, TEP feels an update within 30 calendar days for “any organizational” change is unreasonable. The standard does not clarify whether these include both external and internal organizations as are referenced in R1.3.3. Additionally, it is often impossible to guarantee notifications of such types of changes.
Yes
No
For Requirement R1.4, TEP requests clarification of the statement “verified initially after backup”. Does this imply every backup, or when a new backup method is used? For Requirement R1.5, TEP does not feel a TFE process is warranted and suggests changing the wording to “Preserve data, to the extent reasonably possible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1.
Yes
No
For Requirement R3.4, TEP feels an update within 30 calendar days for “any organizational” change is unreasonable. The standard does not clarify whether these include both external and internal organizations as are referenced in R1.3.3. Additionally, it is often impossible to guarantee notifications of such types of changes.
Yes
Yes
No
TEP feels Requirement R2.1 would be particularly burdensome in the substation areas, and that the applicability to Medium Impact BES Cyber Sytems should be removed. Additionally , if this applicability remains, it is TEP's opinion that the TFE requirement does not work. Monitoring changes to a baseline configuration for a device generally takes place on a system (monitoring system) outside

the device (monitored device). Would the TFE apply to the monitoring system or the monitored device? Would the RE be required to have multiple monitoring devices if one did not work with a particular monitored device?
Yes
Yes
No
TEP is concerned with the apparent overlap of access controls for protected information between CIP-004 and CIP-011. Access controls stated in Requirement R1.2 seem to apply to the physical controls as well as electronic, but CIP-004 R6.3 and 6.6 also cover access control (authorization and handling as part of that).
Yes
Yes
Yes
Individual
Tony Eddleman
Nebraska Public Power District
Yes
Distribution Provider is not listed in the definitions, but it is modified from its current use in each of the CIP standards under the Facilities section. Distribution Provider should not be defined in these definitions – the impact is too broad and reaches beyond the cyber security standards. If you want to change the definition of a Distribution Provider, it should be done in a separate project not associated with the cyber security standards. Specifically, the last two bullets should be deleted on including a Transmission Protection System and a TO's restoration plan. These bullets are too broad and include systems which don't materially affect the reliability of the Bulk Electric System. In general, we understand why you are trying to move away from critical assets (CA) and critical cyber assets (CCA), but the change is too significant and doesn't provide a reliability benefit. We have invested significant effort and cost in our current documentation of CAs and CCAs. We understand how to identify CA and CCAs under our current standards, but we don't understand how to identify Cyber Assets and Cyber Systems as defined in the version 5. Recommend the drafting team follow the recommendations of the MRO NSRF (comments submitted separately) and retain the current CIP-002-4 bright line criteria in place of the proposed CIP-002-5. BES Reliability Operating Services introduces confusion and sets up a compliance trap. At a high level, it sounds reasonable, but trying to implement the concept is problematic. We will need a document to address each and every item identified in this definition to prove we are compliant and prove we have reviewed our systems in accordance with this list. The current bright line criterion in CIP-002-4 adequately addresses how to identify Cyber Assets and Cyber Systems and is significantly easier to implement. As an example, if a dynamic map board is used for situational awareness for the operators, is it a cyber system requiring protection? It appears it is a Cyber System. But, the operators still have screens on their computers for situational awareness. If a problem occurs with the map board and reduces their situation awareness, at what point is it a compliance issue? If a light bulb on the map board fails to light, do we have 15 minutes to change the light bulb before we have to report noncompliance to our Regional Entity? How do we know if the light bulb blew when it attempted to light or failed earlier – maybe we have already exceeded the 15 minutes? In a mitigation plan to prevent the light bulb from failing again, how do I prevent the light bulb from failing in the future? Will I be required to set up an identical map board for a test system? The cost is significant. It appears the only compliance solution is to remove the map board and reduce reliability by denying operators this additional tool due to these new compliance requirements and associated risk of a potential violation. This is only one example of many compliance traps introduced by the BES Reliability Operating Services definition. Each of the individual categories, while there are many identified, are still too broad and will require significant

documentation to an auditor why our system is or isn't included. We can't go down this path, because it opens up too many undefined situations.
Yes
As discussed in item one above, we recommend retaining CIP-002-4 and not implementing CIP-002-5. CIP-002-5 is confusing and will be difficult to implement.
No
We disagree with the SDT's comments during conference calls & webinars that entities will not have to have a "list" of LOW cyber assets. Audit teams will, especially early in the process, want to assess that how we evaluated each asset was correct with the intent of the standard. They will want to see how we checked each asset against the BES Reliability Operating Services to see that we didn't make a mistake. The audit teams will be checking for 100% compliance without any room for errors. We don't understand how we prove compliance without a list of LOW Cyber Assets. The shear scope of evaluating all cyber assets is daunting. Keeping these lists current seems like an enormous paperwork exercise. We question how this improves reliability when we will spend more time chasing paper than keeping up with current security issues & practices. The requirement to be 100% compliant and have documentation to prove 100% compliance at all times is unrealistic and drives registered entities to focus more on documentation and spend our customers dollars on trivial items instead of equipment improvements that will increase reliability. If a registered entity has a program implemented and misses minor documentation issues, the registered entity should be allowed to address the minor issues in a Corrective Action Program (CAP) and not be required to self-report the issues as potential compliance violations. The registered entity should document the minor issues in their own CAP and provide them upon request to the audit team during an audit. As an example, if you have several hundred individuals on an access list and have successfully added and removed the majority of them in the time periods specified, but missed a few of the removal dates by a few days, it's evident you have a program in place and implemented. The CAP would address how to correct the remaining items and further identify any repetitive or systematic issues.
No
Delete the "not to exceed 15 calendar months between approvals" in CIP-002-5, R2 and M2 and throughout version five of CIP-002-5 through CIP-011-5. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No

We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
Delete the "not to exceed 15 calendar months between reviews and between approvals". This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience! Also, please refer to item 6 above.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the other requirements is confusing - this is a compliance trap.
No
We are confused on which Cyber Assets and Cyber Systems the requirements in CIP-003-5 apply. In section 5. Background, under the Applicability section, the document refers to a table row to define the scope to which a specific requirement row applies. The only table provided in CIP-003-5 references VRFs and VSLs (i.e., an applicability table doesn't exist). The applicability section goes into detail on high, medium, low, and other Cyber Assets and Cyber Systems, but it isn't clear which requirements apply to which assets. General Comment affecting all the Version 5 CIP-002 through CIP-011 standards: Any requirement for "Low Impact Ratings" should be pulled from the various standards and collected in a stand alone standard specifically addressing low impact BES Cyber Assets and BES Cyber Systems. The current method of weaving the low impact requirements in with all the

other requirements is confusing - this is a compliance trap.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The requirement for Quarterly Security Awareness is excessive. There is a “yearly” training requirement, so why do quarterly awareness. Even nuclear does not require that level of awareness. Our teams are already required to read and be aware of so much information that this additional awareness requirement provides minimal if any value. Recommend a bi-annual requirement, and reduce the burden on entities. Having a blanket statement that must include vendors in our security awareness is excessive for them. This requirement forces us to track each vendor with access reviews of quarterly data, and requires the vendor who supports many customers to review each of those independently. We propose a change to include only vendors “on-site” be included in the quarterly awareness (or biannual as proposed above), with off-site/remote only being required to do the yearly training. This is consistent with nuclear practice, and is consistent with any associated risk.
No
We understand the point of defining specific roles that the SDT believes require training. However, we believe that there are too many categories that require training listed. It is conceivable that individuals could have responsibilities in all nine (9) of the areas listed in R2. This would require completion of nine (9) different training modules every year. This seems excessive, not to mention the burden on the individual responsible for upkeep of the training material to ensure its correctness and applicability.
No
In Table R4, delete, “including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more”. It’s impossible to prove we reviewed all locations where an individual has lived over the past seven years. We can threaten to fire the individual if they prove false or misleading evidence on where they have lived, but we have no control over the information they provide. Also, there isn’t a nation-wide system that can check an individual’s previous residences and confirm they have provided reliable information. If an individual does lie to us in attempting to obtain a job by covering up residence information, and we find out later, now we have to self report a compliance issue. This requirement goes too far by requiring all locations.
No
Delete the “not to exceed 15 calendar months between verifications” in Table R6 Part 6.5 and Part 6.6. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
The draft standard currently requires revocation of unneeded access by the end of the next calendar day. For most instances, when people change jobs, they continue to support their old position for at least 30-60 days, while the position is re-staffed or retraining of someone new can be completed. The guidelines state that “a review of access privileges must be performed”. The standard wording does

not state that at all, it states revoke, with evidence showing it was done. This wording in the standard must be changed to allow us to continue using the individual that was reassigned or transferred, as we deem appropriate.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Requirement 1.3 requires two factor authentications for physical access to HIGH Impact areas. In the measures, it states to provide evidence for how “ingress and egress is controlled by two or more different methods”. Two methods are not required for egress and this requirement for documentation must be changed.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The Measures section for Table R1, Part 1.1 references screenshots showing accessible ports of BES Cyber Assets as evidence, and this is infeasible. Obtaining the data into text files is fine, but to attempt to get screenshots of all these ports is an enormous amount of work. We understand the measures indicate this evidence “may include”, but an auditor will point to the measure and indicate for us to prove our compliance, we have to provide the screen shots. Please change the screen shots to text files.
No
In Table R2, Part 2.1, requires monitoring patches and updates for “all” software and firmware associated with BES Cyber System or BES Cyber Assets. This is a compliance trap. In a large Cyber System, the risk is great of missing a small piece of software embedded in a vendor’s product. What if a product is no longer supported or the vendor that developed the software/firmware is no longer in business? How do you comply with this requirement?
No
Table R3, Part 3.2 requires us to, “Disarm or remove identified malicious code.” Of course we want to do this, but what happens if we don’t get it all – are we in violation? Once a system is infected, it’s extremely difficult to clean; and, as we learned with STUXNET, we may not realize the total extent of the infection until later. We understand this requirement and agree it’s the right thing to do, but implementation will be difficult and then to wrap the compliance piece around the event will be almost impossible to prove compliance. Table R3, Part 3.3 requires signature or pattern updates within 30 days of availability of the updates. For remote locations, this is not realistic. A real-time system operating in the BES is difficult to update that quickly. The update process has inherent risks of inadvertently tripping an on-line device or piece of equipment. A generation unit may have a cyber system isolated from any external connectivity and the cyber system may only be available for updates during a planned outage. Please leave some operational flexibility for a registered entity to install the updates at a frequency consistent with the risks for the system. A suggested wording for the requirement is, “within 30 days or other time period documented as appropriate by the registered entity”.
No
Table R4, Item 4.3 is a compliance trap. At a minimum, please change, “next calendar day” to “next

calendar business day". Please provide more information on what this requirement is requiring. Table R4, Item 4.4 – why should we have to maintain records of disposition of event logs? If we can show 90 days of logs, providing records of disposition is unneeded documentation. By adding this into the Measures area, an auditor can require either this or something similar from us to prove we are compliant. Table R4, Item 4.5 – we don't understand this requirement. It appears to be requiring us to review a log that we are reviewing logs. Recommend this requirement be deleted in its entirety. This is unnecessary documentation.
Yes
We appreciate the wording change to include "the maximum complexity supported by the BES Cyber System". Thank you!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
In Table R1, Part 1.1, please remove "identify, classify" from the requirement. In Table R1, Item 1.2, please remove this requirement in its entirety. In Table R1, Part 1.3, please remove section 1.3.3.
No
Delete the "not to exceed 15 calendar months between executions of the plan(s)" in Table R2 Part 2.2. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
Delete the "not to exceed 15 calendar months between reviews" in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience! Table R3, Parts 3.2, 3.3, and 3.4 – Recommend combining these three parts in one and allow 90 days to update and communicate the changes. The current 30/60/30 time periods are confusing.
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
In Table R1, Part 1.5, our first and highest priority is to restore the real-time system to operations. While preserving data is desirable, it should not be the focus during a restoration. The requirement should plainly state restoring the BES Cyber System or BES Cyber Asset is the priority function and

preserving data is desirable, but not required at the expense or getting the system restored. As currently written, this is a threat to reliability, not an enhancement.
No
Delete the “not to exceed 15 calendar months” in Table R2 Parts 2.1 and 2.2. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
Delete the “not to exceed 15 calendar months” in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Table R1, Part 1.5 is not clear. If we add a disconnect to a one-line drawing in the Energy Management System (or other database change), is this change required to be tested prior to implementation? This requirement will significantly hinder any operational changes to support field crews real-time. This requirement will also add documentation requirements for changes to the Cyber Asset that don’t adversely affect the security controls. The additional testing requirements aren’t security related and should be removed from the standard.
No
Table 2, Part 2.1 has the potential to add significant TFE’s without a corresponding increase in security. This requirement will also reduce the reliability of the BES Cyber Systems by increasing the complexity/administration due to unnecessary software monitoring each system.
No
Delete the “not to exceed 15 calendar months” in Table R3 Part 3.1. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!

No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
Delete the “not to exceed 15 calendar months” in Table R1 Part 1.3. This requirement is a best business practice and should not be a requirement. This requirement will be very difficult to track and will result in numerous documentation errors for entities without any reliability benefits. This is a compliance trap. Since this phrase is included numerous times in the version 5 standards, compliance will have to track numerous different dates each year with a 15 month time bomb on each one. By forcing 100% compliance to the standards (reference comment above in item 3) each item would be a separate potential violation. Once per calendar year is sufficient for compliance and the entity should be able to define how a calendar year is implemented for their situation. Our industry is constantly challenged by the weather and other factors beyond our control. Forcing us to focus our attention on unnecessary documentation during an emergency significantly detracts from our ability to restore service to customers. Will there be an emergency during a period of time we are trying to update compliance documentation – absolutely - 100% chance based on experience!
No
VRFs and VSLs require 100% compliance which is difficult to achieve and maintain. Recommend a Corrective Action Program (CAP) be implemented by registered entities instead of requiring perfection on every item.
No
The implementation period should be phased for high, medium and low impact assets. Since the cyber security standards have changed significantly, registered entities need to make significant changes to existing programs, while maintaining compliance to existing standards. High impact Cyber Systems should be implemented first, followed by medium, followed by low. Our task of bringing in low impact Cyber Systems is significant and should not be attempted while trying to address high and medium Cyber Systems.
Individual
Mark B Thompson
Alberta Electric System Operator
Yes
The definition for Intermediate Device doesn’t specify where the device should be located, i.e., limit to secure networks.
Yes
The AESO agrees, but we may need to write a requirement in the Alberta version of the standard to designate the work required specifically of the ISO.
Yes
Wording changes may be required in Alberta to align with our concept of “annual”. Alberta Reliability Standards do not use the word “calendar” to imply a consecutive time frame.
Yes
Yes
Yes
Wording changes may be required in Alberta to align with our concept of “annual”. Alberta Reliability Standards do not use the word “calendar” to imply a consecutive time frame.
Yes

The use of the term “appropriate” makes it difficult to define which individuals need to have access to the policies.
Yes
Yes
Wording may have to be changed in Alberta to align with our concept of “days”, and we don’t use the word “calendar” to imply a consecutive time frame.
Yes
The AESO agrees with need for security awareness training. The Change Rationale states that the requirement to “ensure everyone with authorized access receives this awareness” differs from the R1 Rationale, which states that R1 “ensures that personnel who have authorized [access] maintain awareness of best security practices.”
Yes
No
Part 3.1 may be onerous because training will be required for every new hire in the applicability section, and the training program outlined in R2 and its parts will be quite extensive. Training groups of new hires within a certain timeline would be more practical.
Yes
The AESO will need to change the wording and/or requirements in parts 4.1, 4,2, and 4.4, to meet applicable Federal and Provincial laws in the Albert Reliability Standards version.
Yes
The AESO will need to change the wording and/or requirements in parts 4.1, 4,2, and 4.4, to meet applicable Federal and Provincial laws in the Albert Reliability Standards version.
No
The AESO suggests that the requirement for part 6.4 should read “…that individuals provisioned for unescorted physical access or authorized electronic access to BES Cyber Systems…” The original wording implies “unescorted electronic access”, which is not a valid concept.
Yes
Parts 7.2. and 7.3 state “end of next calendar day” which implies these requirements could take place on a weekend or holiday. This will cause additional expense for some companies as they will have to have IT and Facilities staff on-call 24/7 to handle any revocations.
No
Can there be a Low Impact BCA/BCS within the same ESP as a High or Medium Impact BCS? The Applicability in Parts 2.1, 2.2, and 2.3 all reference High, Medium, and Associated, but not Low. Is it then possible to require a VPN into an ESP for High & Medium, but have a direct interactive connection for a Low within the same ESP?
Yes
Neither should be checked, as the AESO does not comment on the VRFs and VSLs.
No
The applicability is confusing between Parts 1.2 and 1.3. Both have “Associated Electronic Access Control or Monitoring Systems” and “Associated Protected Cyber Assets” listed as applicable, however the requirements in 1.3 are more comprehensive than in 1.2.
Yes
Yes

No
The AESO believes that Part 1.2 will not stop something like Stuxnet from propagating through a network.
No
The Version 5 Implementation Plan refers to R1.1 in CIP-002 for planned changes - which reads; " 1.1. Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category." The Implementation plan then stipulates a 12 month time period for entities to become compliant with all applicable requirements within CIPs v5 in cases where unplanned changes have occurred, but there is no requirement addressing unplanned changes within the CIP-002 standard.
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Yes
MMWEC agrees with the comments submitted by APPA and NPCC.
Yes
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, MMWEC suggests for CIP-002 Attachment I - In 2.13, Change "(2) generation control centers" to "(2) generation Control Centers" (capitalize Control Center.) Indicate that Control Center is a defined term to avoid confusion with generation control rooms.
No
MMWEC agrees with the comments submitted by NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, –

Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
Yes
Yes
No
MMWEC agrees with the comments submitted by APPA and NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
Yes
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: “ other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.

No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by NPCC. Also, please clarify whether logged events must be reviewed for Medium Impact BES Cyber Systems.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in

frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by APPA.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
No
MMWEC agrees with the comments submitted by NPCC. In addition, regarding Applicability, MMWEC suggests the following change to CIP-003-5 through CIP-011-1, A. Introduction, section 4.2.4.4, – Append: " other than UFLS or UVLS systems configured to shed loads less than 150 MW." The intention of this change is to limit DP and LSE applicability to Registered Entities with systems configured to automatically shed loads greater than 150 MW. Although small loads may have a role in frequency and voltage support, these systems pose a low risk to the BPS as a target for cyber attacks. As written, the standard would impose on small entities a relatively high marginal cost of mitigation with little reduction in risk to the BPS resulting from a cyber security incident.
No
MMWEC agrees with the comments submitted by NPCC.
No
MMWEC agrees with the comments submitted by APPA and NPCC.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
The definition of "BES Cyber System Information" should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a "Schweitzer" relay (or even an "SEL 2030"), the information should not require special treatment. Refer to additional comments submitted for Question 49. The SDT should also re-think including data in the definition of Cyber Assets. Additionally, "suspicious" is not an auditable term and ought to be removed. The same is true for "attempt." It is not clear which "attempts" justify reporting. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. BES Cyber Security Incident: A malicious act that: • Compromises a BES Cyber System or BES Cyber Asset, or • Disrupts the operation of a BES Cyber System or BES Cyber Asset, or • Results in unauthorized physical access into a Defined Physical Boundary. BES Reliability Operating Services: we note the following: • "Identify and monitor flow gates" under "Managing Constraints" seems to be missing its bullet • We

recommend clarifying that the use of the word “Facility” means the NERC Glossary definition -- in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication” • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret. CIP Exceptional Circumstance: We request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. CIP Senior Manager: Replace “NERC CIP Standards” with “NERC CIP-002 – CIP-011 Standards” because CIP-001 is not part of this set of standards. Control Center: We are concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be affected by a broad definition of Control Center. In the proposed definition, the SDT uses the defined term “System Operator” which is “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” If the SDT’s intent was to limit Control Centers to BA, TOP, GOP and RC functions, we support the definition and request that the SDT make this limitation clear in the definition or in guidance. Intermediate Device: Recommended changes: “A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Yes

Attachment 1, Section 2.13 assigns a Medium Impact to "generation control centers that control 300 MW or more of generation." Control Center is a NERC-defined term; however, because "control center" is not capitalized in 2.13, it creates confusion because it could be interpreted that a typical control room of a combined cycle unit could be construed as a "control center” by the Regional Entity. The SDT should capitalize the term in 2.13 to make it clearer. We recommend adding a threshold for BAs similar to CIP-002-4. Change to “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12.” We do not agree with the inclusion of all Transmission Owner (TO) control centers. These may include local distribution "dispatch rooms" with visualization capability and minimal control of BES Facilities. We recommend removing “TO” from Attachment 1, 1.4 and 2.13. Alternatively, if TOs must be included, we recommend using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" (i.e. Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator”). The addition of a “Low Impact” rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit. In addition, Regional Entity audit resources would be better served if allowed to focus on more critical locations. We recommend this category be eliminated. Criterion 2.7 seems to have been modified to include some transmission substations operating at 200kV to 300kV. The present Version 4 bright-line criterion includes only those operating above 300kV. Because this includes substations interconnected to generators, it seems likely that 200kV substations newly identified as “Medium Impact” could include some generation facilities as well. This would require a

whole new level of regulatory compliance to facilities not included under the Version 4 Standards. There is no reason to believe the Version 5 criterion better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? In 2.12, "system" and "Facility" are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned.
No
For clarity, we request changing R1.1 from "Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation" to "Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation." For clarity and consistency with the previous suggested change, request changing M1 from "as required in R1 and list of changes to the BES)" to "as required in R1 and list of changes to the BES Elements and Facilities)". The word "intended" should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Part 4 needs clarification. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementing CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion framework. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. The SDT should consider an approach that would have documentation "requirements" in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards. We recommend replacing "30 calendar days" with "90 calendar days."
Yes
Recommend adding the following: "…has had its CIP Senior Manager or delegate review and update…"
No comment.
No
The SDT should re-think the use of a "CIP Senior Manager." In many organizations, there will not be one senior manager responsible for implementing the CIP Standards. For example, in some organizations, SCADA/EMS and Relay personnel report to one senior manager, but I.T., Security and H.R. personnel report to a difference senior manager (or managers). Yet, the SCADA/EMS, Relay, I.T., Security and H.R. all have roles in CIP compliance. A better approach would be for the Standards to require that a Senior Manager be designated for each Standard (or requirement), but it need not necessarily be the same Senior Manager for each Standard (or requirement).
Yes
Request clarification of the meaning of "implement" M2.2.
Yes

Suggested change: “Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Please see our comments in response to Question 6, above.
Yes
We recommend changing “30 calendar days” to “90 calendar days.” The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No comment.
Yes
Providing Security Awareness is useful and should remain in the Standard. However, the SDT should re-think the need to have a Security Awareness Program. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
Yes
Comments: Most of the requirements in R2 make sense. However, providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. We recommend removal of R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training. With respect to R2.10, it seems unnecessary to require training on the systems’ electronic interconnectivity and interoperability with other cyber assets. Generally, the personnel doing the “care and feeding” of those assets already know how they work and how they interconnect and interoperate. The personnel using those devices have no need to know about the interconnectivity and interoperability of the assets. Request clarification of whether personnel with access to only protected information need training/awareness.
Yes
Yes
For all R4 table entries, we recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2, we recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
The CIP Senior Manager should not necessarily have a role in R6.1, R6.2 and R6.3. There should, instead, be a particular person designated as the “gate keeper” for each cyber asset and physical

security area. For example, the SCADA/EMS manager is the logical person to grant access to the SCADA/EMS system, not necessarily the “CIP Senior Manager.” [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to a “gate keeper.” However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just create the “gate keeper” concept.] The Registered Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. In R6.1, we recommend changing “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except.” Also, change “minimum necessary” to “minimum the responsible entity considers necessary.” In R6.2, 6.3, 6.5 and 6.6, change “minimum necessary” to “minimum the responsible entity considers necessary.” For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For 6.6, we request clarification of whether variances noted in the verification would be required to be a self report. In the measure for R6.6, change “BES Cyber System information” to “BES Cyber System Information.”
No
In Part 7.1, the use of “at the time” of the resignation or termination is vague and ambiguous. For example, if a person informs the utility that his/her resignation is effective in three weeks, must the utility revoke access when informed of the resignation or when the resignation becomes effective? We recommend making the requirement seven days. We recommend moving the text in the footnote for 7.1 into the requirement. For Part 7.2, we recommend requiring only that the revocation occur as part of the next quarterly review. Those personnel have merely been reassigned or transferred. They do not pose a risk to the BES (as opposed to, for example, an involuntarily terminated employee). It makes sense that people deemed to be a risk (i.e. those terminated for cause) should have a very short timeframe for revocation. However, for people in good standing who are transferred or reassigned, the time frame has gone down from a seven-day permissible time frame to a single day. This seems an unnecessary burden that will cause utilities to incur costs needlessly (i.e., overtime pay to do revocations on Saturdays, as most people who resign or get reassigned or transferred would likely do so effective end of business Friday). Again, these costs and obligations seem reasonable for terminations for cause, but hard to justify for employees in good standing. Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the calendar quarter in which the resignation/termination occurs.” For Part 7.4, revoking a person’s overall access to cyber systems should suffice. In other words, if a person must be on your corporate network in order to gain access to critical cyber systems, revoking overall network access should suffice to meet the Standard (as opposed to revoking the person’s access to the various individual systems). If this language remains, we believe it should be revised as follows: “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within ninety (90) calendar days of the date of initial access revocation.”
No
There should be a “lower” and “moderate” VSL for R1 through R3 (e.g. For R1, a “lower” VSL could be if awareness reinforcement was done only two times in a year; a “moderate” VSL could be if awareness reinforcement was done only three times in a year). For R5, we recommend the following language: “Personnel risk assessments are not updated at least once every seven years. (5.2)” Also for R5, the “severe” VSL contains the following language: “The Responsible Entity did not have a documented process for personnel risk assessments.” Failure to have a documented process for PRAs should not involve a severe VSL. The important question is whether PRAs are being performed; not if there’s a documented process for performing them. In other words, if a utility can demonstrate it is performing PRAs (correctly and timely), it should not matter whether the utility has a documented process to perform PRAs.
Yes
For R1 there is an issue of auditability regarding Low Impact BES Cyber Assets. If an entity need not create a list under CIP-002, there is no way to ensure the technical and procedural controls have been applied. Request clarification for when Low Impact BES Cyber Systems are in the ESP with High/Medium BES Cyber Systems. Are such Low Impact BES Cyber Systems subject to 1.1 or 1.2? There is also some disagreement over the VRFs for this Standard. Currently, the VRF is set at Medium. For part 1.1, that VRF should not be Medium but should instead have its own VRF of “Low.” We propose the following wording change to Table R1, Part 1.1: Requirement: An Electronic Security Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access.

Measure: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. The Measures language proposed is similar to CIP-004-5 R1. We believe the use of the word “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
We recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset" to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset" because, as written, the requirement does not allow for the development of new technology. We recommend changing the Measure for R2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors."
No comment
Yes
We request clarification of Part 1.1’s Applicability because it does not identify which of High/Medium/Low BES Impact the Physical Access Control Systems are "Associated" with. We request Requirement 1.2 be updated to allow "escorted physical access." We propose the following wording change to Table R1 Part 1.1: Requirement: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measure: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. The Measure language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
Yes
Requirement 2.2 requires clarification. If the intent is to require that visitors sign-in once each day, the draft language does not clearly set forth that requirement. As currently written, the language could be interpreted to require entry/exit logs “on a per 24-hour basis.” Such an interpretation would mean a Registered Entity would have to retain a great deal of paper (where logs are maintained on paper). This is especially true for an entity on a six-year audit cycle (which will have to maintain 2,190 individual daily logs for each facility). Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis,"
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
No comment.
No
Request clarification on R1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while

the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
Yes
We request clarification of Part 2.2 because it requires creation of a “remediation plan.” However, if the entity applies the patch, no remediation plan should be necessary. We suggest wording similar to the following: "create a remediation plan or a plan to mitigate the vulnerability if the Responsible Entity opts to not apply a patch or update." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
Yes
The Standard should make an allowance in Part 3.3 for signature/pattern updates that create system problems/issues. In the Requirement for Part 3.4, the words, “…Transient Cyber Assets and removable media….” should read, “…Transient Cyber Assets or removable media….”
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Please clarify the Requirement for Part 4.3. Does it require that the failure be detected within a calendar day or that a response be implemented within a calendar day of a failure being detected? The Requirement in Part 4.5 for log reviews every two weeks is too frequent. We recommend monthly reviews (which is still more frequent than the 90-day reviews in the previous version of the Standards).
Yes
In Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.] Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No comment.
Yes
Yes
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
Yes
In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. We believe these times should coordinate with the plan in EOP-004-2 which allows 90 calendar days for update of the plan. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing up Information essential to BES Cyber System recovery, verify the media to ensure that the backup process was successful.”

No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported.
No
For Part 3.1, we recommend “and document any identified deficiencies or lessons learned” as that topic is addressed in CIP-009 R3.2. In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. We believe these times should be consistent with CIP-008-5 updates and, as stated in our response to Question 36, should be changed to 90 calendar days for update of the plan. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
No
This requirement will be very difficult to meet and will require many technical feasibility exceptions. We suggest the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems outweigh the cyber security benefit.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
No comments
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered.

Yes
Footnote 2 in 2.1 should be moved into the body of the Requirement.
No comments.
No
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Because Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. We also have the following overall comments: I. Black Start Issues There are several black start-related issues. First, in the current version of the Standards, a Registered Entity can have Critical Assets with no Critical Cyber Assets (CCAs). So, for example, a company may have black start units (i.e. Critical Assets) which have no associated cyber assets that use a routable protocol. As such, those black start units can be Critical Assets with no CCAs. As a result, the Registered Entity would not have to meet the NERC CIP requirements for the black start units. The same concept does not exist in the Version 5 Standards. In the Version 5 Standards, black start units will require CIP protections. That fact could have a chilling effect on entities. In other words, some entities may not bid their units into black start service because, by doing so, they would have to incur the expense of becoming NERC CIP compliant. In the ERCOT Region, black start service is not very lucrative and, therefore, some companies may refrain from bidding into black start service due to the expenses associated with being NERC CIP compliant (plus the fear of potential fines down the road). Additionally, many Blackstart units in the ERCOT Region are older, smaller units with very low capacity factors and limited revenue. Applying the “Medium Impact” CIP requirements on those units will result in the need for significant CIP investment and increased on-going operational costs as well as increased compliance risks. This may result in Generator Owners/Generator Operators not offering units for Blackstart service. It would also likely result in Blackstart units not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart service. With fewer units offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. We believe a Blackstart unit with no External Connectivity poses little or no risk to the BES and should be classified as Low Impact. We recommend the following modification to CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would remain in the “Medium Impact” category; however, Blackstart Resources without External Connectivity would move to the “Low Impact” category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through an Electronic Access Point. Another concern focuses on facilities downstream of the black start unit. For example, one company could be chosen to provide black start service from a generator, but a different company owns/operates the facilities along the cranking path. If that were the case, the transmission company would now have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. The same is true for facilities associated with the next-start unit. If the switch yard for the next-start unit is owned/operated by a company other than the one that won the black start bid, that next-start company may have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. Another question involves whether units that are black start capable must be NERC CIP compliant regardless of whether they are in the black start restoration plan. The reliability of the ERCOT system may be adversely impacted because units that have been updated to meet the NERC CIP Standards but not selected for Black Start service could be forced into mothball or retirement due to economics associated with maintaining NERC CIP compliance. Many such units are small, have small staffs and low capacity factors, do not run much during the year and may be running on the margin. If companies are reluctant to bid into the black start market due to the costs associated with being NERC CIP compliant, it could result in inadequate black start capability due to Generation Owners not bidding units into the black start market. Finally, we request clarity on

the inclusion of “next start units” in the black start path. As CIP-002 currently reads, it could be interpreted that they are not included in the black start path; consequently, clarification is in order. II. Other Issues • We recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • We request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • We request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Group
Florida Municipal Power Agency
Frank Gaffney
No
First of all, we thank the Standard Drafting Team for all of the hard work on what we believe is a very significant step forward on Cyber Security Standards. We believe that this is heading in the right direction. Having said that, this is the first draft and as such we have a significant number of comments that we hope will help improve the standards. Now, our comment to Question #1 is as follows: BES Cyber System – Maintenance Cyber Asset is not defined, suggest changing to Transient Cyber Asset. BES Cyber System Information – (1) Security procedures should not be on the list because it creates a conflict between CIP-011-1 that restricts access to the information and CIP-003-5 and CIP-004-5 that require general training and dissemination of those procedures. (2) BES Cyber System Impact is not defined. BES Reliability Operating Services – under Dynamic Response to BES Conditions, suggest adding Excitation Response. Under Balancing Load and Generation – suggest removing unit commitment since it will not meet the 15 minute window and it is an operations planning function and not a real-time operating service. CIP Exceptional Circumstance should include imminent danger to a BES Facility as a condition. CIP Senior Manager – the definition should exclude CIP-001, at least until it is retired with Project 2009-01 Control Center – (1) We assume that a Control Center is only a Control Center is used by an BA, TOP, GOP or RC. The definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” For clarity, we suggest adding this clarity to the definition. (2) The use of the word “facilities” in a fashion that does not mean “Facilities” will lead to confusion and ambiguity, especially since “facilities” is used later in the same sentence as meaning “Facilities”. FMPA suggests: “One or more sites hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation Facilities or transmission Facilities, at two or more locations”. Facilities should also be capitalized in the first bullet. Defined Physical Border is ambiguous. Specifically, are all spacial dimensions, horizontal and vertical, to be established as part of the boundary? In other words, it seems like the “roof” may no longer be required, e.g., 5 walls instead of 6 walls, but, vertical dimension requirements of walls / fences are ambiguous.
No
FMPA believes that a fourth category of risk impact be developed, a “De Minimus Impact” category that would consist of otherwise Low Impact BES Cyber Assets but that do not have routable protocol or dial-up access. We understand that there is concern about Low Impact BES Cyber Assets due to the risk of a coordinated attack. A coordinated attack is much more likely to BES Cyber Assets that have routable protocol or dial-up access than to those BES Cyber Assets with no connectivity. It is much more difficult and impractical to attempt a coordinated attack on BES Cyber Assets without connectivity. Recognizing this difference in both difficulty level and Low Impact (in other words, it wouldn’t be worth the effort because other attack vectors with similar levels of difficulty would have more impact), we propose adding a fourth impact category, De Minimus Impact. FMPA would propose that these De Minimus Risk BES Cyber Assets would not need to comply with the CIP standards because the costs would be unjustified. Bullet 1.2, a Control Center for any BA, even very small ones, being High risk is inappropriate. For instance, the entire load or supply of a small BA would fit into the “noise” of a large BA for supply and demand mismatch. Suggest changing 1.2 to parallel 1.3, e.g., a BA Control Center that includes control of one or more of the assets identified in criteria 2.1, 2.3, 2.4

and 2.12. Bullet 2.13 could then be used to accommodate smaller Bas Bullet 1.3, Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” Bullet 2.5, “Facilities” should be changed to “Elements”. The cranking path is not necessarily part of the BES. Bullet 2.6, is an autotransformer of 500 kV to 230 kV included? Bullet 2.7 is inconsistent in its terminology, switching between “Facility” and “Lines”. It seems that “Line” is intended. The focus also seems to be “at a single station or substation” where the focus ought to be a single BES Cyber Asset / System that controls multiple Lines. FMPA suggest changing the first sentence of 2.7 to read: “Multiple Transmission Lines operating at 200 kV or higher, but less than 500 kV, where the total weighted value of all BES Transmission Lines whose Reliability Operating Services would be adversely impacted within 15 minutes if a single BES Cyber Asset / System is rendered unavailable, degraded or misused exceeds a value of 3000.” Bullets 2.8 and 2.9, the phrase “at a single station or substation location” does not seem to add any value and can be a source of ambiguity. FMPA suggests striking the phrase. Bullet 2.12, the 300 MW bright-line seems arbitrary (albeit carried over from prior versions). In general, the system is more tolerant to loss of load than loss of generation and the 300 MW seems out of proportion with 2.1 of 1500 MW. The reasoning applied in the Application Guideline is flawed. UVLS and UFLS are only last ditch efforts if other events have already caused the system to be on the edge. So, how is that different from 2.1 if the system is already on the edge? The focus should be on how a malicious user can cause an Adverse Reliability Impact; hence, we suggest 1500 MW instead of 300 MW. Bullet 2.13, (1) Transmission Owners do not have Control Centers and should be struck from the bullet, e.g., the definition of System Operator in the Glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” (2) The term “control centers” should be capitalized in the phrase “generation control centers” to make it clear that it refers to the defined term “Control Center” In the application guidelines, when discussing the BES Reliability Operating Services, the bullets have associated with them the functional entity that typically provides those services. However, there are exceptions and the guidelines ought to reflect those exceptions; for instance, a TO may also provide UFLS. Also in the application guidelines, the word “facilities” is used in a fashion that does not mean “Facilities”, which creates ambiguity and confusion (e.g., Facilities by definition is part of the BES, whereas assets owned and operated by DPs and LSEs are typically not BES). Suggest using “elements”. The Application guideline discussion of bullet 2.13 of Attachment 1 is not consistent with the actual bullet.
Yes
FMPA agrees with the requirement but questions whether the standards actually meet the stated goal of the requirement to “not require discrete identification” of Low Impact BES Cyber Assets / Systems. There are numerous examples which seem to contradict this stated goal as described later in these comments and specifically to this requirement. How does one distinguish between a BES Cyber System and a non-BES Cyber System? Does this mean that we need to inventory all of our cyber assets and develop a test to distinguish between “Low” and “non-BES”, even though R1 says that “Low” does not “require discrete identification”? How are entities to prove to auditors that the identification and categorization was done without having an inventory, i.e., discrete identification? The VSLs seem to seem to imply that “Low Impact” needs to be discretely identified, e.g., what happens if an entity categorizes a Medium Impact as a Low Impact? In order to review correct categorization, doesn’t the auditor need to review Low Impact to see if they should have been categorized Medium or High Impact?
Yes
Yes
The Evidence Retention section of the standard should not refer to Rules of Procedure language that is subject to change. The sentence that states: “For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit” should instead reference the Rules of Procedure, Attachment 4C on the CMEP, Paragraph 3.1.4.2, e.g., “also refer to the Rules of Procedure, Attachment 4C … Paragraph 3.1.4.2”. In this way, it is possible to accommodate changes to the ROP language without needing the change

the standard.
Yes
No
“Implemented” is not the right word because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. Suggest changing to use the phrase “in force”, meaning that the policy is in force and able to be enforced, but not requiring enforcement of the policies in this requirement (implement includes enforcement), but rather enforcement is contained in ensuing standards. FMPA suggest rephrasing to: “Each Responsible Entity shall have in force one or more documented cyber security policies …” The standards are inconsistent in its use of BES Cyber Assets /Systems, e.g., R2, to be consistent with CIP-002-5, should use the phrase “BES Cyber Assets and BES Cyber Systems”. Alternatively, CIP-002-5 could just use BES Cyber Systems. The bullets are incorrectly numbered; they should be 2.1 through 2.10 and not 1.1 through 1.10
Yes
The grammar of the sentence is a bit off and it is not clear whether the CIP Senior Manager needs to approve each of the policies or not. Suggest moving the phrase “each of its cyber security policies” to after the word “Manager”, e.g., “Each Responsible Entity shall review and obtain the approval from its CIP Senior Manager for each of its cyber security policies …”
Yes
Yes
“Cyber Security Policy” should be “cyber security policies” to be consistent with R2 and R3.
Yes
There is an extra “2” at the end of the sentence within the standard.
Yes
See the discussion of Evidence Retention in response to Question 3 VSL to R5, should there be a time frame applied, e.g., failed to document … two delegations within the audit period, within a year? If three failures are spread over 30 years, e.g., one failure each 10 years, is that a severe violation?
Yes
“Implement” is ambiguous. If a process in “in force” but in one instance is not followed, is that a violation? The process has been implemented. Merriam-Webster’s has two definitions of “implement”, one of which is probably intended: 1: carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures 2: to provide instruments or means of expression for A process can meet both of these definitions. If enforced, a process can meet the first definition; if not enforced, the process can meet the second definition. FMPA assumes the SDT intends the first definition. FMPA suggests adding a footnote to specifically identify which definition of “implement” is intended.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 2.1, the measure and the requirement do not match. The requirement is to “define the roles”, the measure includes “and the training needed for each role”. Suggest adding this phrase from the Measure to the Requirement.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The phrasing of requirements that refer to tables is ambiguous with ambiguous reference of prepositional phrases. For instance, in this requirement, it is unclear if an entity that only has Low Impact BES Cyber Systems needs to develop training or not, i.e., does the prepositional phrase “that includes …” refer to “training program” or to “Responsible Entity” or to both? We suggest rephrasing: “Each Responsible Entity that owns applicable systems described in the Applicability column of Table ___ shall ___ in accordance with the applicable terms of Table ___” Such rephrasing should be done to all requirements that refer to a table associated with that requirement. In addition, measures should not include the word “must”. Measures are not enforceable

but are instead examples of evidence.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 4.2, the phrase “up to the current time” is problematic since it infers that 7 year criminal background checks need to be updated on at least a daily basis to cover “up to the current time”, This should be reworded to seven years prior to the last background check.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The flow of the bullets seems backwards and missing a job function analysis step. In addition, the word “minimum” implies an optimization that is impractical to achieve, e.g., do we want every individual account to be optimized to that individual, which is very difficult to administer and prone to error, or rather do we want to establish account groups based on job functional analysis with associated, appropriate levels of permission and assign individuals to these groups. The latter is easier to administer and less prone to errors, and follows established practices such as security clearance levels. FMPA suggests the following “flow”: 1. Job function analysis 2. “Account group” establishment with appropriate levels of permissions based on job function analysis with associated permissions 3. Assignment of individuals to the appropriate “account group” based on their position
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 7.1 is impossible for resignations. How is it possible for an entity to revoke access at the same time they receive a resignation? Footnote 2 does not help because it only applies to termination. For termination, the entity should know about the termination before the employee; however, for a resignation the reverse is true. FMPA proposes to create a new bullet specific to resignation and require revocation of access by the end of the next calendar day. Bullet 7.2, the urgency is out of alignment with the risk. Next calendar day means that if a re-assignment occurs on a Friday, that weekend work is required when that level of urgency is not justified by the situation / risk. FMPA suggest end of the next calendar week.
No
See the discussion of Evidence Retention in response to Question 3 The Severe VSL for R3 includes the phrase “The Responsible Entity did not fully implement its cyber security training program” which makes it a binary VSL and eliminates the High VSL described. For counts, e.g., R6, R7, should there be a time frame identified? E.g., 2 individuals within a year, within the audit period?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The requirement does not describe the overall purpose of the processes required. Are these processes to deny unauthorized access? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define technical and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the procedural and technical controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. Bullet 1.2 is ambiguous and implies another requirement. First, one does not “use” EAPs to control and secure, rather, EAPs are controlled and secured through use of some other means. Second, the requirement is to secure only identified EAPs,, e.g., is it a non-compliance if an entity misses an EAP, e.g., did not identify it? Third, the Measures are all to support the identification of EAPs and not to “secure and control” EAPs as required by the Requirement. And fourth, the ensuing bullets (1.3, 1.4) seem to be requirements to secure

and control EAPs; and hence, bullet 1.2 seems to create double jeopardy. FMPA suggests rewording bullet 1.2 to require identification of EAPs and not “secure and control”.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See the discussion of Evidence Retention in response to Question 3 The VSLs are binary, so, it seems that if one EAP is missed, it is a severe violation. Is this appropriate? FMPA encourages the SDT to develop non-binary VSLs.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 1.1 is ambiguous. How can physical access be restricted without a Defined Physical Boundary? Does this imply that Low Impact assets need to be enclosed in both horizontal and vertical dimensions? Does a fence of xx height suffice? Bullet 1.1 is over-ridden by the word “implement” in the parent requirement. In other words, 1.1 says that entities are to define operational and procedural controls. However, the parent requirement states that these are to be implemented. This means that the entity will need to have device-by-device evidence that the controls were implemented thereby not meeting the goals stated by the SDT that for Low Impact, the requirements are to be programmatic in nature and not require device-by-device compliance evidence. Suggest using a different word in the parent requirement than “implement” and then re-insert the word “implement” in the bullets as appropriate. The application guidelines act to embed a de facto standard requirement of 96 square inches that, if desired to actually be a requirements, must be specified in the actual Requirements of the standard and not in an application guideline that is not enforceable. Alternatively, a definition of a Physical Access Point could be developed with established thresholds that may vary between High, Medium and Low Impact and then the defined term used in the standard. FMPA is aware of challenges made by auditors to entity compliance surrounding issues like how thick does dry-wall need to be to constitute a wall. To avoid disputes between auditors and entities over what constitutes a Defined Physical Boundary, and what constitutes access points, FMPA encourages the SDT to develop bright-line criteria. Such criteria could be different for different risk impacts, e.g., for illustration purposes only: • High Impact might require 6 wall enclosure with every access of 96 square inches or larger opening defined as an access point with wall material of metal, concrete, or drywall of xx inches • Medium Impact may not require a roof, but, requires a fence or wall height of xx inches topped with a climbing deterrent such as barbed wire. • Low Impact video surveillance is sufficient. The standard is very ambiguous as to what is a sufficient physical boundary and will be open to debate between compliance and entities if such bright line criteria are not developed.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The note to bullet 2.2 that says “there is no need to document the escort or handoff between escorts” is inconsistent with the requirement of bullet 1.1 which states that visitors need “continuous” escort. How would one prove that escort was continuous without documenting the hand-offs? On bullet 2.2, what does the phrase “on a per 24 hour basis” mean? Does this mean that a visitor must be logged in and out on the same day and that if a visitor is there at midnight, then the visitor must be logged out at midnight on the prior day and logged back in the following day, or does this mean that military time is to be used when annotating the log?
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.1 is not limited to Medium and High Impact with the term “Locally mounted hardware or devices associated with Defined Physical Boundaries since Defined Physical Boundaries is not limited to only Medium and High Impact assets through its definition. This implies that all physical access controls, even those to Low Impact, are to be tested. Presumably, this includes padlocks used to control gates to fences. non-electronic door locks that control access to

substation control houses that contain Low Impact digital relays, etc. Such an interpretation would then require an inventory of those access controls, and presumably, to ensure a complete set, an inventory of Low Impact assets and their Defined Physical Boundaries. FMPA suggests adding to the end of the phrase “Defined Physical Boundaries associated with Medium or High Impact …”
Yes
See the discussion of Evidence Retention in response to Question 3 R1 has both a Long Term Planning and a Same Day Operations time frame listed because the separate bullets are different time frames. If a non-compliance occurs, wouldn’t Same Day Operations always trump Long Term Planning? If that is not the desired outcome, consider separating the bullets into separate requirements or apply the time frame on a bullet by bullet basis.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. On bullet 2.2. - (1) Suggest adding the phrase “addressed by the security related patches or updates” after the word “vulnerabilities” as clarification. (2) “Remediation” implies compensatory measures; the standard should not require compensatory measures because such measures may reduce reliability. Consider another term such as “palliative plan”, “alleviation plan”, or “assuagement plan”. On bullet 2.3, “A process for” is redundant with the parent Requirement and should be deleted and just start the sentence with “Remediate as identified in the plans of 2.2 …”
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 4.2 allows the entity to establish its own threshold criteria for what unauthorized electronic access or malware activity results in a real-time alert, is that a desired state? Bullet 4.3 implies redundancy, e.g., how will we know that event logging failed unless a redundant system tells us? Bullet 4.4 is a data retention requirement and does not belong as a requirement, but rather in the Evidence Retention section of the standard.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 5.4, if “implement” as used in R5 means to “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”, then, this bullet 5.4 would require a complete inventory of all Low Impact BES Cyber Assets to ensure that default passwords were changed …. To solve this, implement could be removed from the parent requirement and replaced with “have”, e.g., “have processes”, and then the bullets that require asset by asset / system by system implementation could re-insert the word implement. As such, what would likely need to happen is two bullets would need to be created for default passwords, one for High and Medium which would use the phrase “implement procedural controls” and another for Low Impact which would use the phrase “have procedural controls” to distinguish between a system by system approach for Medium and High and a programmatic approach for Low. Bullet 5.5.3 allows the entity to specify the amount of time between password changes, is this appropriate or should a bright-line be developed? For instance, High – 3 months, Medium – 6 months, Low – 12 months Bullet 5.6 allows the entity to specify the number of unsuccessful login attempts before an alert is issued, is this appropriate or should a bright-line be developed?
No
See the discussion of Evidence Retention in response to Question 3
No

See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to “identify, classify and respond to BES Cyber Security Incidents” on Low Impact systems? This “hidden” requirement is inappropriate. FMPA recommends making R1 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. This Requirement essentially implies that Low Impact assets need to have in place systems to monitor potential cyber incidents that are required of High and Medium Impact in CIP-007-5 in order to detect and respond to cyber security incidents. Otherwise, how is one to know “(w)hen a BES Cyber Se4curity Incident occurs”. This “hidden” requirement is inappropriate. FMPA recommends making R2 only applicable to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, and hence this is duplicative for Low Impact systems. Bullet 2.2, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire response for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.2 (an) Exercise …” Bullet 2.3 is an Evidence Retention requirement and should not be a requirement.
No
First, the question does not match the posted Requirement. The Requirement actually states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication”. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. See comments to Questions 34 and 35. FMPA believes that in order to make this requirement applicable to Low Impact systems, which implies that CIP-007 become applicable to Low Impact systems and this “hidden” requirement is inappropriate. Instead, standard CIP-008-5 should not be applicable to Low Impact systems, especially in consideration of the requirements of EOP-004-1 which require entities to analyze and report cyber security incidents.
Yes
See the discussion of Evidence Retention in response to Question 3
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. Bullet 1.4, what does the word “verified” mean, than the data is “retrievable”, or that all the data is verified? The intent seems to be that the data is retrievable, otherwise 2.2 seems duplicative.
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 2.1, “implement” is not the correct term and is duplicative with the parent requirement. How would one “implement” the entire recovery for a table top drill since no IT systems would be involved? “Exercise” or equivalent term is more appropriate, e.g., “R2 … implement a process for … 2.1 (an) Exercise …” Bullet 2.2 “current configuration” is not accurate. The back-up will not reflect the “current configuration” but the configuration at the time of the back-up.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15.
Yes
See the discussion of Evidence Retention in response to Question 3
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures

described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. The CIP Senior Manager (or delegate) should approve the baseline (1.1). Presumably, the baseline would be “reset” periodically to reduce the number of changes that need to be tracked, and the CIP Senior Manager (or delegate) should approve the new baseline (1.3). Bullet 1.3, the phrase “as necessary” does not seem to add anything and creates ambiguity. Suggest deleting the phrase.
No
Having to monitor all the assets associated under the Applicability section of Table R2 is a huge TFE generator based on the requirement. If the intent is to make sure that there have been no modifications to the device, it would seem appropriate that one could monitor other items and not just the configurations in order to meet the requirements of FERC Order 706, paragraph 397. FMPA suggests that there are methods, such as documented monitoring of logins, wherein if a device has not been logged into, the configurations need not be constantly monitored. Having a yearly requirement to verify configurations (via MD5 hash matching, for example) is an acceptable requirement, but having to constantly monitor the devices for any configuration change is going to be impossible for many devices, and create an unnecessary burden on entities while adding no value to the protection of the BES. Also, this requirement appears to add additional technical controls such as “white listing” above what is already called for in CIP-007 R3. We believe the intent should be to ensure that as part of change control, system configurations are checked to determine if any changes from the approved baseline configuration have occurred since the last authorized change. If detected, these changes should be investigated as per procedures covered under CIP 007-R3. See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. Bullet 3.2, what is an “active” vulnerability assessment? The term is ambiguous.
Yes
See the discussion of Evidence Retention in response to Question 3
No
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13. There should be recognition of law, e,.g., unauthorized people are only granted access in cases where the law requires divulging that information, such as public records acts, or a discovery process order by a judge. It would seem that access to BES Cyber Security Information should be approved by the CIP Senior Manager as a separate bullet under R1.
Yes
See comment on ambiguous reference to tables and improper use of the word “must” in Measures described in Question 15. See discussion of the ambiguity of the word “implement” discussed in response to Question 13.
Yes
See the discussion of Evidence Retention in response to Question 3
Group
Western Electricity Coordinating Council
Steve Rueckert
Yes
BES Cyber Asset. From an enforcement perspective WECC urges the SDT to revise the proposed “BES Cyber Asset” definition to exclude the criterion that limits BES Cyber Assets to those that would impact BES Reliability Operating Services within a “15 minute window.” The “15 minute window” is not in the interest of reliability. Misuse of a BES Cyber Asset may pose significant risks to the BES within 16 minutes, 15 hours or 15 days. Further, entities and regulators will be forced to speculate as

to which Cyber Assets would impact BES operations within 15 minutes. There are hundreds of scenarios under which the same Cyber Asset may impact the BES over and under 15 minutes. The proposed Standard does not point to any study nor provide a rational basis to support the “15 minute window” exclusion. To ignore BES Cyber Assets that are presumed to not pose impact to BES operations within 15 minutes, is contrary to FERC Order 706, and the Federal Power Act §215. The 15 minute window restricts entity discretion and disregards the FERC Order 706 which states that “implementing [CIP] Reliability Standards must be done on the basis of the specific facts and circumstances applicable in the individual case at hand.” To limit BES Cyber Assets to Cyber Assets that would impact BES Reliability Operations within 15 minutes is, therefore, over prescriptive. WECC also recommends eliminating the exception that excludes “Transient Cyber Assets” from the definition of a BES Cyber Asset. If any Cyber Asset satisfies the criteria put forward in the definition there is no rational basis to exclude that Cyber Asset from identification as a Cyber Asset. The SDT should provide clarification regarding the definition of “adverse impacts to BES Reliability Operating Services” in the context of identifying BES Cyber Assets. What is an “adverse impact”? Are “adverse impacts” included in the definition related to “High” and “Medium” impacts described in CIP-002-5 “Attachment 1, page 23”? BES Cyber System A BES Cyber System is defined as “one or more BES Cyber Assets that are typically grouped together, logically or physically to operate one or more BES Reliability Operating Services.” The SDT should provide clarification as to how to determine if Cyber Assets are “typically grouped together.” Specifically, in the context Cyber Security, the technology is rapidly evolving. Including the term “typically” excludes the integration of new technology within an existing BES Cyber System. Secondly, the proposed definition of a BES Cyber System may exclude Cyber Systems that directly impact BES Operations. The proposed definition of a BES Cyber System presumes that BES Cyber Systems are comprised of Cyber Assets that individually impact BES Reliability operations within 15 minutes. The proposed definition, therefore, does not consider Control Systems critical to BES Operations apart from the impact of individual devices comprising that system. Consequently, a Cyber System comprised of Cyber Assets that collectively impact BES Operations would not be identified unless individuals devices within that system are first determined to have separate impacts on BES operations independent of that systems The definitions of Version 5 CIP Security Standards does not include a definition for a device identified as a “Maintenance Cyber Asset.” The exclusion of “Maintenance Cyber Assets” from BES Cyber System contradicts the definition of a BES Cyber Asset. If a “maintenance cyber asset” qualifies as a BES Cyber Asset there is no rational basis to exclude that device from being identified as part of a “BES Cyber System.” Control Center The definition of a “Control Center” in the “definitions” is inconsistent with criteria proposed in CIP-002-5, “Attachment 1”. The proposed definition “Attachment 1” Section 1.4 requires the Generator Operator to identify BES Cyber Assets that impact Reliability Operating Services at a black start resource. WECC recommends that the definition of “Control Center” to include one or more BES generation or transmission facilities at a single location. Transient Cyber Asset The definition of a “Transient Cyber Asset” should be revised to include more specific criteria. Any Cyber Asset connected to a BES Cyber Asset or Protected Cyber Asset for 30 days or less may pose a significant risk to the BES. Any Cyber Asset capable of altering the configuration of or introducing malicious code to the BES Cyber System should be considered a BES Cyber Asset regardless of the duration of its connectivity. Electronic Security Perimeter Definition does not say clearly that this has to include ALL interfaces from outside the BES(s) being protected. Suggest change to: “The collection of all EAPs that permit communications to a BES system from a device not in that system.” Note that existing definition of EAP says “restricts” rather than "permits.” Unsure of the specific meaning of “restricts."

Yes

From an enforcement perspective WECC is concerned that the proposed categorization of BES Cyber Assets does not resolve ambiguity in previous CIP-002 versions, and does not address directives issued by FERC in Order 706. More importantly, however, WECC is concerned that proposed categorization will not serve BES reliability. In Enforcement’s experience with CIP-002 Versions 1, 2, and 3, entity identification of BES impacts has been a significant hurdle that entities fail to clear. Given the current uncertainty regarding the definition of “BES”, many entities have had difficulty identifying BES facilities that impact BES operations. The proposed Standard not only requires that entities identify impacts of individual cyber assets, but also qualifies BES Cyber Asset impacts as those that result in an impact to BES Reliability Operations within 15 minutes. This added criterion creates more ambiguity and does not provide clarification mandated by the Commission in Order 706. Based on Enforcement’s experience with the CIP reliability Standards currently in effect, there is no evidence that “categorization” will facilitate Cyber Security implementation. Presently, effective

Reliability Standards categorize Cyber Assets into three groups: Critical Cyber Assets, Cyber Assets in an ESP, and ACM devices. And, similar to proposed CIP-002-5 R1, current versions of CIP Reliability Standards assign a specific set of compliance obligations for each of these categories. In many cases, however, Entities have opted to afford the same protections to all three categories of Cyber Assets rather than develop separate compliance crosswalks for each category of Cyber Assets. In cases where entities have opted to treat each category of asset separately, Enforcement has observed increased instances of noncompliance, and less effective mitigation. Categorization appears to lead to inconsistent implementation of Security Standards. Even with a single CIP compliance manager, segregation of Cyber Assets tends to lead to a lack of coordination between business groups within the same organization. Consequently, it is difficult to detect and effectively mitigate violations that may implicate multiple categories of cyber assets. Mitigation of a CIP-006-1 R1 violation for Critical Cyber Assets, will not extend to ACM Cyber Assets under CIP-006-1 R1.8. WECC recommends that an entity identify Cyber Assets based on “use” or “operation” rather than ownership. A Cyber Asset owned by one entity, may be used by another. Consequently, if only the “owner” is required to assess that cyber asset’s impact, the owner will determine that it is not essential to its BES Reliability Operations. Further, the “owner” of a cyber asset may have physical access to the device, but the same “owner” may not have logical access to a device that is logically sited within another entity’s network. Consequently the “owner” will be unable to implement logical protections required under CIP-005, CIP-007, and CIP-010. If categorization of BES Cyber Assets is preserved, WECC recommends that the Requirement also require identification of “lower” or other BES Cyber Assets as some CIP Reliability Standards contained in proposed Version 5 apply to all BES Cyber Assets including those identified as “lower risk.” The first sentence in 2.7 may be ambiguous due to the Boolean property of the word "and": A clarification is requested to ensure proper understanding of this criterion. Is the second phrase, "and where the 'total weighted aggregate value' of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000" a qualifier for the first phrase, "Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation that is connected to three or more transmission stations or substations" or is it a standalone criterion. In other words, if the second phrase is a standalone criterion, the phrase "and where the 'total…" should be replaced by the phrase "or where the 'total…" which would retain the original intent of the SDT. On the other hand, if the second phrase was intended as a qualifier for the first phrase, the language should be amended to read "…connected to three or more transmission stations or substations, where the "total weighted aggregate value' of all BES Transmission Lines …" Either change that meets the original intent of the SDT would clarify this criterion and eliminate ambiguity that might later call for an interpretation. This is of particular concern given that there is a push from FERC and congress that more generation be inclusive in the application of cyber security controls. The wording of this measurement has had much debate and there is conflicting understanding on what this actually entails. The SDT has stated that this would be 1500 MW attached to a single DCS (for example). As currently written, this means that a single facility with multiple generation units at 1499 MW or less that are attached to separate DCS' would not reach the category of medium. An aggregation of generation capacity per facility should be considered. From a reliability perspective we suggest that the threshold in the Medium Impact category for generation should be 1,000 MW instead of 1500 MW and 300 kV instead of 500 kV for substations. Although the addition of "within 15 minutes" does lend itself to a "bright-line" criteria, it may be arbitrary in the event that a BES Cyber Asset or BES Cyber System is unavailable, degraded or misused and one or more BES Reliability Operating Service becomes "adversely impacted" at the 16 minute mark or longer. Why is an adverse impact happening within 15 minutes any less important to the BES than one happening in 20 minutes?

No

From an enforcement perspective WECC Recommends that the SDT create two Requirements: one for identification of BES Cyber Assets; the other for categorization of BES Cyber Assets. As written, the proposed standard would result in multiple repeat violations of the same standard. Multiple repeats of a standard tend to suggest a culture of noncompliance. Multiple violations of this requirement, however, may stem from different causes. Thus multiple instances of noncompliance with this Requirement may mischaracterize an entity’s compliance record and have consequences that impact the scope of subsequent audits and compliance investigations. From an enforcement perspective WECC disagrees with limiting an entity’s identification of BES Cyber Assets on “ownership” thereof. To date, there has been a great deal of controversy regarding “ownership” of individual devices. Entity

“use” or “operation” of a Cyber Asset, however, is easier to identify and is consistent with the purpose of CIP-002- requiring entities to identify Cyber Assets that are critical to their BES Operations. Further, to refocus BES Cyber Asset identification to emphasize “use,” responsibility at joint use facilities or jointly owned facilities is immediately identifiable. WECC recommends that the entity that operates or uses a Cyber Asset, is responsible for assessing that asset’s impact to its BES operations, and, if appropriate, identifying the Cyber Asset as a BES Cyber Asset based the role the asset plays in its BES operations. WECC disagrees with the provision that requires entities to categorize and identify BES Cyber Assets that have been “updated” or deployed within 30 days. Consistent with current implementation guidance approved by FERC, WECC recommends that the entity assess and identify BES Cyber Assets before implementation of a change or deployment. Deployment or reconfiguration of a BES Cyber Asset may pose a significant risk to the BES. A thirty day gap will not only delay identification of a BES Cyber Asset, but will also delay implementation of Cyber Security measures prescribed under CIP-003 through CIP-010. WECC strongly disagrees with the provision limiting “updates” to include only those Cyber Assets “that are intended to be in service for 6 months.” Regardless of intent, a device that satisfies the definition of a BES Cyber Asset or BES Cyber System must be identified and protected as such. A BES Cyber Asset connected for one month poses the same risk to the BES during that time as does the BES Cyber Assets connected for more than one year. Further, this language would preclude enforcement of CIP-002-5 R1 in cases where a device initially intended to connect a BES Cyber Asset for less than six months, remains connected, for a period of seven months. Because that entity “intended” a six month period of connectivity would Enforcement be able to Enforce CIP-002-5 R1? WECC recommends that the SDT removes any reference to an entity’s “intent” from proposed CIP-002-5 language. There appears to be a discrepancy between the Low Impact language of R1 "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification" and the "evidence of categorization" of Low Impact devices in M1. This discrepancy is derived from a strict interpretation of the R1 langauge: the entity must first prepare a comprehensive list of ALL Cyber Assets, then categorize appropriate BES Cyber Assets or BES Cyber Systems as High or Medium Impact according to the criteria in Attachment I, which then takes the BES ROS into account. Anything left over after the analysis process could be assumed as a Low Impact device, but it would still have been discretely identified by virtue of its position on the initial list. A more logical identification process indicates the entities should first identify any applicable BES Reliability Operating Services (ROS - as identified in the Guidelines and Technical Basis section, p. 18) relative to the entity's Registered Function(s), then identify and classify BES Cyber Assets and/or BES Cyber Systems associated with that BES ROS according to the criteria in Attachment I. As a practical matter, it seems that entities will follow the logical process as described above, but that approach does not address the "letter of the law" as stated in R1. The term “adversely impact” is not clearly defined. Please clairfy – is each cyber asset categorized EITHER alone OR as part of a BES system? Since the BES system concept is a major change for V5, more explanation wold be helpful.
No
WECC does not disagree with the requirement for the CIP Senior Manager or delegate approval There are clear definitions of the necessary bookends. However, we are concerned that given the recent NERC CAN on “annual” requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry.
Yes
Yes
Yes
The need for cyber security policies that address the BES Cyber Systems is prudent; however, it appears that the required topics to be addressed may not be holistic and/or fully appreciated without more description. For example, does Personnel Security include Training & Awareness policies? Would an entity know to include policies addressing Monitoring & Logging in the topic System Security? There does not appear to be specific policy requirements to address Application Security, provisioning, forensics or cryptography & encryption.
Yes
We agree with the proposed requirement. However, as noted in question 4, given the recent NERC

CAN on “annual” requirements, does this create a separate definition of annual for this requirement? If so, this may create confusion in the industry.
No
Individuals with access to BES Cyber Systems AND BES Cyber Assets should be made aware of elements of its cyber security policies appropriate for their job function AND degree of access. Additionally, The Requirement is unclear for the following reasons: 1. Rationale – R4 states: “The intent of the SDT is to ensure that the responsible entity takes sufficient measures to make its cyber security policy available and accessible to personnel. It is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.” However, the Requirement states: “… shall make individuals who have access to BES Cyber Systems …” It is unclear from the language of CIP-003-5 R4 whether then responsible entity must make some, most, or all individuals with access to BES Cyber Systems aware. 2. “… access to BES Cyber Systems …” will lead to confusion. Which type of access? To solve the above two concerns, R4 language should be “Each Responsible Entity shall make all individuals who have authorized cyber or authorized unescorted physical access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.”
No
M5 refers to documents, signed by the CIP Senior Manager, as possible measurements but not required documents. Documents, signed by an authorized person, should be required in R5 as follows: “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, approved (via signature), and shall specify the authority that is being delegated.”
Yes
Yes
Yes
WECC agrees with the apparent intent of the requirement. However, there is potential for registered entities confusion based on the current wording of this requirement. The rational states that the requirement "Ensures that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems maintain awareness of best security practices." yet neither the R1 requirement language nor the R1.1 table requirement make mention of this expectation. Furthermore, the change rationale for R1.1 states that such language was removed from the requirement. It would seem that if the expectation is to ensure that personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems were aware of best practices then this would be explicitly stated in the requirement section. Additionally, if awareness is provided only to personnel with authorized electronic access and/or authorized unescorted physical access, it could still be possible for personnel without appropriate awareness doing unrelated work on systems in other networks such as the enterprise network to infect systems in those networks, that might then be used to stage attacks against electronic security perimeters protecting BES cyber systems.
Yes
Yes
WECC agrees with the intent of R4. However, there are several concerns that could be addressed through modification of R4. Without requiring verification of credentials, eg. Government issued photo ID, how is the utility able to trust an employee's identity? It only states criminal record check and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries

and reasonable for both cyber security and safety. The criminal check record is private confidential information and this needs to be stored securely. It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). Contractors may not have 7 year history of criminal record, and also, in many cases, these contractors and/or vendors, have been working for them for many years. What if the utility cannot get all that info? What if the utility finds something from the criminal record of the contractor that has been with them for several years? In these cases, what should the utility do? Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require this permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIP Standards? Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity. Extended leave situations - such as a sabbatical, employee behavior/performance suspensions or maternal/paternal leave - are not identified as a reason for revoking or suspending access. Given the criticality of the environment being protected, reducing the privileges to only those who have a need for access as a part of current job duties should be maintained. These specific role changes perhaps could follow the requirements for transferred or reassigned personnel; however, it should be made clear in the requirement or Guidelines and Technical Basis section how to manage these common personnel situations. In the Guidelines and Technical Basis, there is a table that identifies that no action is required for death. WECC disagrees that no action should be taken. Revocation of access privileges for the deceased is an important action. Dormant accounts with privileges could be misused. By removing such privileges, the entity is reducing their overall attack surface as well.
Yes
No
WECC does not disagree with the purpose of the proposed Requirement. However, as noted in response to other questions WECC is concerned that given recent NERC CAN on “annual” requirements, a separate definition of annual specific only to CIP-002-5 R2 will create confusion in the industry. WECC also is concerned that escalating all access requests to the CIP Senior manager will not ensure reliability. The CIP senior manager may not be in a position to determine if the access rights granted are proportionate to an individual’s job function. Further, WECC Enforcement has observed that when asset owners are unable to remove access rights themselves, individuals maintain access rights beyond the point in time access to BES Cyber Assets is needed. Additionally, Part 6.1 doesn’t explicitly say “access to BES Cyber Systems” like it does in 6.2. Part 6.1 should be revised to: “The CIP Senior Manager or delegate shall authorize electronic access to BES Cyber Systems, except for CIP Exceptional Circumstances. Access permissions shall be the minimum necessary for performing assigned work functions.”
Yes
Yes
No
Part 1.5 states that the entity needs to establish a documented method for detecting malicious communications at each EAP. There is no additional comments in the Guidelines and Technical Basis section to clarify this requirement; however, the responsible entity could infer expectations from the measures column. Perhaps a better phrasing would be: "At each EAP, the entity shall document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity." Part 1.5 Measures include intrusion detection systems as a limit, which only alert on a signature firing; however, permit the packet to pass through the EAP. It is suggested to change Measures to be a minimum of intrusion prevention systems. An IPS alerts and denies a packet from passing through the EAP, which caused a signature to fire.
No
Part 2.2 “Requires encryption for all interactive Remote Access sessions to protect the confidentiality and integrity of each interactive Remote Access session.”, but this statement does not address end-

to-end encryption. Sometimes vendors access SCADA systems remotely via a third party remote access service, such as "logmein". Such sites may establish a secure tunnel between the vendor and the remote access service, and then another secure tunnel between the utility and the remote access service. In such a case, the remote access service has access to all the remote access traffic; that is, the encryption between the utility and the vendor is not end-to-end. It does not state anything about "Authenticating based on certificates". There have been a significant number of CAs compromised recently, and recent versions of Firefox trust approximately 50 CAs located at organizations all over the world. Secure authentication is necessary to ensure that encryption is useful. Relying on CAs outside of the US to authenticate remote access to critical national infrastructure is risky. In Part 2.3 there is discrepancy on the usage of multi-factor authentication. It states that for High and Medium Impact BES Cyber Systems, as well as the Associated Protected Cyber Assets "REQUIRES" multi-factor authentication. However, in CIP-007 R5.1, it simply states to "validate credentials before granting electronic access to each BES Cyber System" which does not state the need for multi-factor authentication. Multi-factor authentication needs to be carefully defined. US banks have been required to use two-factor authentication since 2006. While the meaning of the term is clear to security professionals, it has been interpreted in some cases by the banking industry to mean "mother's maiden name plus last 4 of social security number". Without clearly defining what is intended by multi-factor authentication, significantly weaker interpretations may be chosen. Regarding dialup connections to a specific BES Cyber Asset, the guidelines state "... examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use". Dial-back modems are easily defeated as revealed by a simple Google search. Remote enable or power up leaves a window of vulnerability unless combined with other defenses, such as modem BES cyber asset passwords. Policy requiring disabling after use is error prone.
Yes
Yes
Yes
Yes
Yes
No
The requirement states that the entity shall "Disable or restrict access to unnecessary logical network accessible ports". The "restrict access" option insinuates that access to any unnecessary ports must be restricted at the host and not at an access point to the network to which the host is connected (i.e. firewall). The wording does not explicitly eliminate an entity from assuming that perimeter firewalls restricting ports to an ESP network meets the R1 requirement. The addition of "from any network device, either local or remote to the cyber asset" would clarify the intent to require all networked hosts within an ESP to restrict access from any network device, regardless of location (i.e. end-point protection) to any unnecessary logical port.
No
The Security Patch Management requirements do NOT include any specific maximum timelines for vendor approved and recommended security patches/updates to be implemented. Requirement 2.2 requires a "timeframe" to be defined for a mitigation plan to address the vulnerability but again does not provide any specific timeframes. This type of vague language allows entities to keep delaying the implementation of vendor approved security patches/updates, creating significant risk to the network to which the device is connected, as well as the BES. Unpatched systems can create a situation where malware/Trojans can rapidly spread once any one system has been compromised (dominos or house of cards comes to mind). A requirement to test and implement relevant and approved patches on a regular basis (at least annually) would significantly reduce the exposure and risk to the BES. The requirements are acceptable and auditable except for the lack of required timeframe to address vulnerabilities.

No
The SDT should address the following to facilitate entity implementation: 1. How soon must the malicious code be removed under R3.2? 2. Who is responsible for identifying malicious code, malicious code prevention tool or any other source under R3.2? 3. Can the STD provide examples of “transient cyber assets”? Is the R3.4 referring to laptops, thumb drives, or any other media? 4. Enforcement recommends that R3.5 logging also require the identity of the person or entity connecting and using the transient device.
No
Part 4.2 - Currently CIP-007 version requires immediate notification or alerting. If immediate alerting is not required, please specify an acceptable timeframe in which staff must be alerted.
WECC supports the purpose of the requirement but notes that long passwords are primarily required to defend against offline password attacks. Increasing minimum password length from 6 to 8 characters is inadequate to address offline password cracking attacks, in the face of modern GPUs offering significant hardware parallelism and available on cloud computing services such as Amazon's EC2. Furthermore, without disabling LM hashes on Windows systems, any password of any length is easily cracked. This applies to all Window systems prior to Windows Server 2008.
Yes
Yes
WECC supports CIP-008-5, but suggests that the following questions need to be addressed. What happens if there is a third-party IT company that handles the utility’s cyber security incidents? Who should be doing what and who has the ultimate responsibility? For example, should the IT company handle everything from the beginning to the notification of the incident?
Yes
Yes
Yes
Yes
Yes
No
WECC agrees with the intent of R1, but offers the following improvements. Part 1.1 - This appears to be an asset inventory and not a true configuration baseline requirement. If a configuration baseline is to actually be achieved for the sake of assuring that the BES Cyber Asset can be monitoring for changes then this requirement should also include a system level baseline configuration action that can be achieved using tools like Tripwire. Of course, that would be where technically feasible. It is also noted that other than security patch level and available network ports there is no specific requirement to document the security controls. Although, it could be inferred that would be required as part of 1.1.3 and 1.1.4. Part 1.2 - Part 1.2 requires authorization of changes by the CIP Senior Manager or delegate but does not specify when. Unfortunately, some applicable entities may take this to the extreme, authorizing the change months after it occurs. Recommend Part 1.2 Requirement read: “Authorization prior to the change, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.”
No
WECC agrees with the purpose of CIP-010-1, but from an enforcement perspective, WECC recommends that in addition to R2.1, the SDT revise the requirement to require entities to document and implement an action plan to address current unauthorized changes and prevent unauthorized changes going forward. Part 2.1 – Similar to our comments above, we offer the following for Part 2.1.

Part 2.1 requires monitoring, documenting, and investigating the detection of any unauthorized changes but does not say when. Unfortunately, some applicable entities may take this to the extreme, documenting and investigating the change months after it occurs. Recommend Part 2.1 Requirement to read: “Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). Document and investigate the detection of any unauthorized changes within thirty (30) calendar days.” Suggest adding protections to the process for modifying cyber assets, in addition to monitoring for unexpected changes.

No

Impacts cannot be prescribed by the Standards, but must be assessed and determined by Enforcement pursuant to FERC Order 672. In some instances a “medium impact” or “minimal” impact may be appropriate. Regional enforcement staff does not have the authority to disregard FERC mandates that require it to assess impacts of noncompliance based on facts and circumstances of each case. WECC agrees with the language of Requirement R3, but offers the following improvements to Table R3 – Vulnerability Assessments. Part 3.1, Requirements, requires a paper or active vulnerability assessment but does not adequately define what is required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. The assessment must include, at a minimum, all of the following: 3.1.1: Enumeration (by name and cyber address) of all Cyber Assets of each BES Cyber System. 3.1.2: Enumeration of all enabled software ports and associated services for all Cyber Assets of each BES Cyber System. 3.1.3: Statement of which software ports and associated services of all Cyber Assets of each BES Cyber System are and are not required for normal and emergency operation. 3.1.4: Enumeration of community strings of all Cyber Assets of each BES Cyber System.” Part 3.2, Requirements, requires an active vulnerability assessment but does not adequately define what must be required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. The assessment shall include all elements defined in CIP-010 R3, Part 3.1.1 through 3.1.4. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.” Part 3.3, Requirements, requires an active vulnerability assessment but does not adequately define what must be required in the assessment. WECC recognizes FERC Order 706 paragraph 644, which leaves details to guidance. However, some applicable entities may take this to the extreme by doing very little in the assessment. Recommend the language be “Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the Cyber Asset. The assessment shall include all elements defined in CIP-010 R3, Part 3.1.1 through 3.1.4.” Part 3.4, Requirements, requires an action plan with planned date of completion but does not actually require completion. Furthermore, it doesn’t set a time limit to complete the action plan. Unfortunately, some applicable entities may take this to the extreme by setting the planned date of completion to an unreasonable date or not actually completing the plan by a reasonable date. Recommend the language be “Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. The action plan shall be completed no later than ninety (90) calendar days from the date of the assessment. Certain vulnerabilities identified in the assessment do not have to be remediated or mitigated if a subject matter expert determines the action will degrade availability, integrity, or confidentiality to an unacceptable level. In such cases, the responsible entity shall document why vulnerabilities were not remediated or mitigated within ninety (90) calendar days.” Without this type of clarity how are the auditors supposed to audit this requirement?. Without defined timeframe criteria the entity can keep rolling the same vulnerabilities from one year to the next without addressing the vulnerability. To effectively audit this requirement the auditors need timeframes. General - Vulnerability analysis looks for any weaknesses - it is more

than an audit of implementation against design.
Yes
No
WECC agrees with the language of Requirement R1 and CIP-011-1 Table R1 – Information Protection, Parts 1.1 and 1.2. However, we suggest the following for Part 1.3. Part 1.3, Requirements, requires an action plan but does not set a time limit for the date of completion. Unfortunately, some applicable entities may take this to the extreme by not implementing the action plan by a reasonable date. Recommend that the language to be "Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between assessments, assess adherence to its BES Cyber System Information protection process, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. The action plan shall be implemented within ninety (90) calendar days from the date of assessment."
No
WECC agrees with the language of Requirement R2 but not with CIP-011-1 Table R2 – Media Reuse and Disposal. The phrase "release for reuse" in Part 2.1 (Requirements) will lead to confusion and inconsistencies among entities. Furthermore, the language of Part 2.1 (Measures) and Part 2.2 (Measures) allows but does not require an applicable entity to generate and maintain records, without which applicable entity management and auditors will not be able to assess the performance of the requirements. Furthermore, the two Parts could be reduced to one with the following: "Prior to the physical removal of BES Cyber Asset media from a Defined Physical Boundary, the Responsible Entity shall implement a 7-pass media overwrite, degauss, or physically destroy BES Cyber Asset media. Each instance shall be documented within thirty (30) calendar days of occurrence."
Yes
WECC recognizes the issues related to the implementation of Versions 4 and 5 of the CIP standards and urges NERC to work towards a resolution that provide reliability to the BES while not forcing registered entities to undertake unnecessary expense and effort.
Individual
Don Jones
Texas Reliability Entity
No
No
In R1, we disagree with the statement that Low Impact BES Cyber Assets/Systems "do not require discrete identification." By definition, all BES Cyber Assets/Systems have the ability to impact BES Reliability Operating Services in a short period of time, including Low Impact BES Cyber Assets/Systems. There are relatively few Requirements that apply to Low Impact BES Cyber Assets/Systems, but in order to ensure compliance (and to audit compliance) with those requirements it will be necessary for those assets and systems to be identified by the applicable entity. What are the "required controls" referred to in M1?
Yes
Yes
Yes
Yes
No

In R4, we feel that if cyber security policy awareness is implemented through periodic training, there should be a periodicity requirement (e.g., annual).
Yes
Yes
No
In Part 1.1, it is not clear what “security awareness concepts” are intended to be included in the program. We suggest listing some concepts that should be included to provide a standard against which the program can be assessed.
No
In Part 2.1, consider requiring the role definitions to be reviewed on an annual basis. We are concerned that these definitions will become neglected and stale if there is no requirement to revisit them periodically.
No
In Part 3.2, we suggest modifying the requirement to read: “Require completion and documentation of the training specified . . ..”
Yes
Yes
No
In Parts 6.1 and 6.2, the Measure should not allow only a “sampling of accounts” regarding people with electronic access or automated physical access to BES Cyber Assets/Systems. The entity should maintain a complete register of this information, even though an auditor may only want to review a sample.
Yes
No
In Part 1.1, if there is no requirement for an entity to discretely identify Low Impact Cyber Systems, there is not any basis from which to determine what assets and systems this requirement applies to, or to audit this requirement. We believe that all BES Cyber Assets/Systems should be discretely identified in order to ensure that they are designed and operated in compliance with applicable requirements, and to facilitate assessment of compliance. In Part 1.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement. Part 1.5 should say “Detecting and recording malicious communications at each EAP.” The focus of this requirement should be on detecting and recording malicious communications, not on producing a “documented method.”
Yes
No
In part 1.3, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes

No
In part 3.1, consider reducing the testing and maintenance interval to 12 months. (What is the basis for 24 month interval?)
Yes
Yes
Yes
No
In Part 4.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
No
In part 5.3, we suggest adding a requirement to annually review the individuals who have access to shared accounts, to ensure that access authorizations are periodically reviewed and updated. In Part 5.4, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement. In Part 5.5.3, the required password change periodicity should be specified as at least annually. The entity should not be allowed to specify a time frame longer than 12 months. In Part 5.6, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes
Yes
Yes
No
In Part 1.5, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
Yes
No
In Part 3.3, the requirement should refer to Part 3.1 as well as Part 3.2 (regarding updating the recovery plan based on deficiencies or lessons learned).
No
In Part 1.1, consider adding that the “baseline configuration” includes any databases (including

version information) that support or interact with BES Cyber Assets/Systems.
No
In Part 2.1, remove “where technically feasible.” This language suggests that an entity may unilaterally decide that this requirement does not apply, without filing a TFE. If an entity cannot comply with this requirement, it should submit a TFE so that a proper determination of technical feasibility can be made. Alternatively, clarify that a TFE must be submitted to invoke the exception to the requirement.
No
In part 3.1, we feel that there should be some specification of a minimum set of security controls that must be implemented and tested, to provide a basis for assessment of compliance with this requirement. In Part 3.2, we feel that the 36-month interval between vulnerability assessments is too long and presents a reliability gap. Vulnerability assessments should be conducted annually on High Impact systems. Also, vulnerability assessments should generally be conducted on the primary or mirrored backup BES Cyber Systems, not on “test systems.”
Yes
Yes
Individual
Roger Fradenburgh
Network & Security Technologies Inc
Yes
Definition of “CIP Exceptional Circumstance” is, perhaps unintentionally, limiting by virtue of its “one or more of the following conditions” language. As written, conditions such as the threat of potential large-scale, cyber-related disruptions of the BES would fall outside of this definition. Suggest rewording using language such as, “Situations that involve actual or potential harm to life, property, or BES operations that require temporary suspension of one or more CIP operating procedures.” Replacement of defined term, “Physical Security Perimeter” with new term, “Defined Physical Boundary” will compel many Entities to undertake an extensive, time-consuming and, in our opinion, pointless project to replace all instances of the current term with the new one in policy and procedure documents, drawings, training material, etc. “Physical Security Perimeter” with new term, “Defined Physical Boundary” Rather than replace “Physical Security Perimeter,” the SDT should consider amending the current definition in a manner similar to how it has amended the term, “Electronic Security Perimeter.” Recommend revising definition of “Transient Cyber Asset” as follows: - Clarify what is meant by “directly connected.” Absent such clarification, there will be arguments about what it means. - Consider deleting third characteristic (“capable of altering the configuration of or introducing malicious code to the BES Cyber System”). It makes a “Transient Cyber Asset” sound like something to be feared and avoided if possible. We note that ANY cyber asset has the potential capability of changing a BES Cyber System’s configuration and/or of introducing malicious code to it. Change definition of “Electronic Access Point.” As written (“An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets”) the definition can be interpreted to mean an EAP’s function is to limit or hinder data communications. Recommend modifying to indicate an EAP’s function is to restrict routable or dial-up data communications to only those that are required for normal or emergency operations. “BES Cyber Asset:” Recommend deleting the second sentence (“This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services.”). It is confusing and seems to contradict the first sentence (“A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services.”). “Electronic Access Point:” Proposed definition (“An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets”) has several shortcomings the SDT should address. It is not clear whether or not the “Cyber Asset” can be a BES Cyber Asset or part of a BES Cyber System. CIP-

005-5 provides no help here, as it does not specify whether or not BES Cyber Assets and BES Cyber Systems must be within an Electronic Security Perimeter. The definition does not say what restrictions an EAP should place on dial-up or data communications, nor does it specify what “between Cyber Assets” means. We recommend the SDT consider basing its definition on the language in CIP-005-3 R1.1. We also recommend an explicit requirement that Medium and High BES Cyber Assets and Systems must reside within an ESP.
Yes
We believe that this new version of CIP-002 should include an analog of criterion 1.10 from CIP-002-4 Attachment 1 (Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.).
No
That the CIP Senior Manager must have “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” should be in the R1 requirement statement, not just the accompanying “Rationale” statement.
No
The policy topic list includes items an Entity with only Low Impact systems would (or should) not be required to have (e.g., Incident Response and Recovery plans). This should be corrected. In the mapping document, the SDT states security policy exceptions have been dropped from CIP-003 requirements because “The FERC Order 706 made clear that you could not take exceptions to the policy. As a result, it did not achieve a reliability objective to require individuals to maintain documentation about exceptions to their policy outside of the Standards.” This is incorrect. In paragraphs 376 and 377 (among others) FERC states that policy exceptions may not be used to except responsible entities from compliance with CIP Standard requirements, but the Order does not state policy exceptions are unallowable.
Yes
No
Four of the five of the “Evidence” examples in M4 would NOT demonstrate compliance with R4’s requirement that the Entity “make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.” Should either change R4 using words conveying that policies must be made available to such individuals –or– change the “Evidence” list to examples that would actually demonstrate compliance.
No
Suggest dropping the 1st sentence, “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards.” It conflicts with the 2nd, which states he or she may delegate much of the required authority for approvals and authorizations. What is meant by the statement, “The authority for subsequent delegations may also be delegated?” “Subsequent” means “coming after (something) in time,” or “later” and doesn’t seem to fit here. Is it the SDT’s intention that delegates appointed by the CIP Senior Manager may also delegate some the authority they have been granted, and that such “2nd tier” delegates may themselves delegate some of THEIR authority to “3rd tier” delegates, and so on? If so, this statement needs to be reworded to make that clear.
Yes
Yes
No
R2 and its included requirements should also be applicable to Associated Physical Access Control

Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets.
Yes
No
R4.2: We believe the requirement to perform a criminal check for any and all places of residence for the previous seven years has the potential to add considerable time and expense to the PRA process with little or no incremental benefit as compared to the existing Standard's seven-year criminal check requirement. We recommend dropping the "per place of residence" condition.
No
Grant of interactive remote access to Med and High BES Cyber Systems should be an explicit requirement. How can there be an explicit requirement in R7 to revoke this access if there is no corresponding requirement to authorize it?
No
R7.1: The SDT should clarify whether "at the time of the resignation or termination" means at the time the action is announced or at the time it becomes effective. R7.2: Suggested changing to, "For reassignments or transfers, revoke any and all unnecessary electronic and/or physical access to BES Cyber Systems within 30 calendar days of the date access is no longer needed." R7.3: The SDT should clarify whether the time limit (end of next calendar day) is meant to be tied to the date the resignation or termination action is announced or at the date it becomes effective. R7.5 The SDT should clarify whether the time limit (within 30 calendar days) is meant to be tied to the date the termination, resignation, reassignment, or transfer is announced or the date it becomes effective.
No
It is our understanding that SDT goals included making each Version 5 CIP Standard as "standalone" as possible. That being the case, we believe monitoring and logging requirements for Electronic Security Perimeters should continue to be addressed in CIP-005-5. When we first read the current proposed draft, we thought they were simply missing. R1.1: The word, "restrict" in, "Define technical or procedural controls to restrict unauthorized electronic access" is inappropriate, as it can be interpreted to mean, "put a limit on" or "hinder" where the presumed intention of the SDT is to prevent unauthorized access. Suggest replacing "restrict" with "prevent." Also suggest replacing "Define technical or procedural controls" with "Define and implement technical AND/OR procedural controls…" R1.1: The Application Guideline notes for Requirement R1 state that Entities should have "perimeter type security controls" that "segment low impact BES Cyber Systems from public or other less trusted network zones." However, since neither the Requirement statement nor the Measures statement contains such language, we believe there is a risk some Entities will feel they is no regulatory obligation to implement "perimeter type security controls" for low impact systems. The SDT should address this. R1.2: What is required for compliance with this requirement cannot, in our opinion, be clearly stated given the current definition of EAP. R1.2: It is not clear what's required for High and Medium systems that have neither external routable or dial-up connectivity. Recommend the SDT address this. R1.2: The phrase, "all routable" in the requirement statement, "Control and secure all routable and dial-up connectivity through the use of identified Electronic Access Points (EAPs)," is overly broad. Suppose two BES Cyber Systems (or two or more BES Cyber Assets) at a single facility (e.g. a transmission substation) communicate with each other using routable protocols but do not communicate with any "off-site" systems using routable protocols. What is the Entity required to do under that condition? Recommend the SDT address this. R1.5: We believe the requirement ("A documented method for detecting malicious communications at each EAP") is overly prescriptive and that the requirement should be written in a manner that allows the Entity to decide how to address Order 706's directive that Entities must use "two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter." (p 496). The use of and IDS or of similar measures could be suggested in the guidance section of the Standard.
No
Suggest changing, "Interactive Remote Access" to "Interactive Remote Access using routable or dial-up connectivity"

No
R1.1's requirement statement, "Define operational or procedural controls to restrict physical access" begs the question, "Restrict physical access to what or to whom?" Also, as noted for CIP-005-5 R1.1, we presume the SDT's intention is to require Entities to prevent unauthorized physical access. Suggest replacing with "Define and implement technical and/or procedural controls to prevent unauthorized physical access." NOTE: Use of "restrict" in R1.2, "Utilize at least one physical access control to establish one or more Defined Physical Boundaries that restricts access to only those individuals that are authorized" is okay, as the sentence includes information about what "restrict" is applied to ("to individuals that are authorized"). R1.2 and R1.3: Replace "restricts" with "restrict." R1.2 and R1.3: We note the Measures for these two requirements state that acceptable evidence includes descriptions of how both ingress and egress is controlled. However the requirements are, we believe, likely to be interpreted as requiring only that ingress be controlled. The SDT should resolve this apparent conflict. R1.6: Requirement should be to record time and date of entry, not just date (as in current CIP-006-3). In the "Guidelines and Technical Basis" section for R1, we believe the assertion that "two-factor authentication could be implemented using a single Physical Access Control System" violates the spirit, if not the letter, of FERC Order 706 p572. FERC Order 706 p562 states, "(the CIP NOPR) stated that use of a minimum of two different security procedures would, for example, enable continuous security protection when one of the security protection measures is undergoing maintenance and provides redundant security protection in the event that one of the measures is breached." Both "factors" in a two-factor authentication system that used a single Physical Access Control System would be rendered inoperable if the control system itself was inoperable.
No
R1.1: Should apply to all Medium Impact Systems R1.1: Change, "Disable or restrict access,…" to "Disable or prevent access,…" R1.2: Change, "Disable or restrict the use of,…" to "Disable or prevent the use of,…"
No
R2.2: Wording ("Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe") is very hard to follow. Suggest changing to: "Identify applicable security-related patches or updates within 30 days of their release from an identified source. Within that same 30 day period, create or revise an existing plan either to install the patch or update, or to otherwise remediate the vulnerability(ies) addressed by the patch or update. The plan shall include a defined time frame for its implementation." R2.3: We assume the requirement ("A process for remediation, including any exceptions for CIP Exceptional Circumstances") is meant to instruct Responsible Entities to implement the patch installation or remediation plan(s) required under R2.2. If this is true, R2.3 should so state in plain terms.
No
There should be a requirement, as there is in the current version of CIP-007, to test anti-malware signature or pattern update files prior to implementation. We note that in the "Application Guidelines" section, the SDT makes it clear this is their intent; however unless it is part of an "R" statement it will not be mandatory. R3.2: Should be subject to technical feasibility R3.5: As written ("Log each Transient Cyber Asset connection") the requirement may cause confusion as to what is meant by "each connection." The SDT should clarify whether it means each time a Transient Cyber Asset is physically or wirelessly connected to a BES Cyber Asset or to a subnetwork shared by BES Cyber Assets or each time a Transient Cyber Asset initiates a new logical connection (e.g., TCP) to a BES Cyber Asset.
No
R4.2 and 4.3 should apply to all Medium Impact BES Cyber Systems, not just those with external routable connectivity. R4.3: The SDT should clarify whether this requirement is meant to apply to individual BES Cyber Assets, to Cyber Assets that collect and analyze logs from many other Cyber

Assets, or both. R4.3: As written (“Detect and activate a response to event logging failures before the end of the next calendar day.”), requirement would allow an event logging failure to last for nearly 48 hours (12:02 AM Tuesday to 11:59 PM Wednesday, for example). Suggest changing this to something more stringent, such as “24 hours or less.”
No
R5.6: Suggest rewording as follows: “A process to limit, where technically feasible, the number of unsuccessful authentication attempts or to generate alerts after a predefined threshold of unsuccessful login attempts has bee reached.”
No
Should apply only to Medium and High Impact systems, along with any “associated” BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems. Why should a Responsible Entity with only Low Impact BES Cyber Systems be expected to define, implement, review, and test a Cyber Security Incident response plan when there are no corresponding requirements for monitoring, alerting, logging, etc. There’s not even a requirement to maintain an inventory of “Low Impact” systems.
No
Should apply only to Medium and High Impact systems, along with any “associated” BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems (as per our comments for R1, above). R2.1: Suggest rewording as follows: “When a BES Cyber Security Incident occurs, the incident response plans must be followed. Any deviations taken from the plan during the response must be recorded.”
No
Should apply only to Medium and High Impact systems, along with any “associated” BES Cyber Systems plus associated electronic and/or physical access control and/or monitoring systems (as per our comments for R1, above). R3.3: Recommend time limit on updates be changed from 60 to 30 days for consistency with R3.4. R3.5: We can think of no reasonable justification for allowing up to 30 days to provide response team members with already completed response plan updates. Recommend the allowed time be shortened to five (5) days.
No
R1.5: Preservation of what FERC Order 706 refers to as “forensic data” should by all means be subject to “if possible” conditions but should NOT be subject to “technical feasibility.” As written, it could compel an Entity whose control center burned to the ground to file a TFE. Suggest revising the requirement to preserve data for post-recovery analysis or to document why it was not possible to do so.
No
R2.1 and R2.3 are in conflict regarding what must be done on the effective date of the Standards: R2.1 directs Entities to “implement” recovery plans upon the effective date of the Standard by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise. R2.3 directs Entities to “test” recovery plans upon the effective date of the Standard through an operational exercise or an actual recovery response. The SDT should decide whether Entities should have the option of performing a tabletop exercise to implement/test their plans upon the effective date of the Standard and revise either R2.1 or R2.3 accordingly.
No
R3.1: Recommend removing “when BES Cyber Systems are replaced” as a condition requiring review of recovery plan(s). This condition is covered by R3.4. R3.3: Updating of recovery plan(s) should be triggered by any findings of deficiencies resulting from R3.1 plan reviews in addition to any findings of deficiencies or lessons learned from R3.2 test result reviews. R3.5: We can think of no reasonable justification for allowing up to 30 days to provide response team members with already completed recovery plan updates. Recommend the allowed time be shortened to five (5) days.
No
It is our view that R1.4, as written, represents a considerable weakening of existing CIP-007 R1

("Test Procedures"), which is generally interpreted to mean changes to the baseline configurations of Critical Cyber Assets should be tested prior to implementation, using production systems if necessary. We recommend modifying R1.4 to require an explicit test of a change's impact on security controls on one or more "test systems" that may, if no other option exists, be "production" systems. The "verification" step that follows implementation of the change on all systems to which the change is applied should in fact be performed on all of those systems.

Group

ACES Power Marketing Member Collaborators

Jason Marshall

Yes

The first two sentences in the definition of "BES Cyber Asset" are difficult to interpret. After considerable discussion among our staff, our understanding is as follows: the definition makes the distinction between when an asset is "rendered unavailable, degraded, or misused" and its actual "operation, mis-operation, or non-operation" under such conditions. If the asset impacts the BES "within 15 minutes" of its actual "operation, mis-operation, or non-operation," then it is a "BES Cyber Asset," regardless of how long since it was "rendered unavailable, degraded, or misused." We recommend editing this definition for clarity as it took a number of our staff numerous reads and discussion to arrive at this understanding that we are still not sure is what the drafting team intended. The distinction should be clarified. Also, we question the necessity of such a distinction and whether the value it adds is worth the confusion it produces. Additionally, it is unclear whether the "timeframe" referred to in sentence three applies to the "within 15 minutes" timeframe or the "regardless of the delay" timeframe. How does the responsible entity know if a BES Cyber Security Incident was malicious? Understanding if an act was malicious implies an understanding of intent. We do not believe that intent is something that can always be quickly and easily understood. Consider the recent case of the failure of the water pump at a Springfield, Illinois water utility that was initially attributed to hacking because it was accessed from a Russian IP address. It turned out it was accessed by a contractor on vacation in Russia at the request of the utility. Obviously, this example demonstrates intent takes time to determine. The Project 2009-01 Disturbance and Sabotage Reporting even stated this in their recent posting for the reason they decided not to define sabotage because intent is so difficult to determine. Thus, we recommend striking malicious from the definition. BES Cyber System includes the capitalized term Maintenance Cyber Asset. The capitalization is an indication that the term is defined in the NERC Glossary. Neither can we find such an existing definition nor is it the definition proposed in this standards project. Either the capitalization needs to be removed or the term needs to be defined. We recommend the latter. BES Reliability Operating Services should not be a NERC defined term. Many of these services are similar to the Policy 10 – Interconnected Operating Services that was never passed because industry could not agree on it. It is doubtful industry is going to agree on this broad definition that could apply outside the CIP standards. Furthermore, there are several issues with the definition. First, it is not clear what is intended by including contingency reserve in parentheses after spinning reserve. Contingency reserve can include spinning and non-spinning components as long as it can respond in 15 minutes to meet DCS. Spinning reserve does not necessarily relate to contingency reserve directly in that it can include unloaded on-line reserves that respond in more than 15 minutes. Furthermore, NERC has two conflicting definitions of spinning reserve: Spinning Reserve and Operating Reserve – Spinning. One definition limits the spinning reserve to what can respond in 15 minutes and the other does not. Second, it is not clear what is intended by including contingency reserve in parentheses after non-spinning reserve. Per NERC definition, non-spinning reserve is time limited but not necessarily limited to the 15 minute limit set in DCS and, thus, on contingency reserves. Thus, while some contingency reserves may be non-spinning, not all non-spinning reserves will be contingency reserves. Third, under the Managing Constraints section of the BES Reliability Operating Services definition, ATC is

identified. It should be removed. ATC is not used to manage constraints but rather to sell transmission service. That transmission service may never be used. While ATC is calculated using reliability components, it is not a reliability service but a commercial service. FERC even acknowledged that the MOD (ATC) standards were designed primarily "to ensure non-discriminatory allocation of transmission capacity among transmission market participants" in paragraph 30 of the order approving FAC-013-2 (137 FERC ¶ 61,131 Docket No. RD11-3-000). Fourth, the Inter-Entity Real-Time Coordination and Communication section of the BES Reliability Operating Services definition should be struck as it is just a supporting activity for all the other services. CIP Exceptional Circumstance should be modified to include a clause that other circumstances of similar nature and/or impact could be included as a CIP Exceptional Circumstance. Otherwise responsible entities could be put in a position of having to choose to violate some the CIP requirements because the SDT did not think of a particular exceptional circumstance that should have been included. CIP Senior Manager should be struck along with all references to CIP Senior Manager in the CIP standards. This definition and associated requirements dictate a corporate governance structure for no apparent reliability reason. A responsible entity should be free to have two, three, or more personnel oversee various portions of the CIP program. The responsible entity will still be required to meeting the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards. It is not clear that Control Center needs to be defined. EOP-008-1 (Loss of Control Center Functionality) was written without defining control center. We are concerned that this definition could cause confusion with EOP-008-1 and believe the definition needs to be coordinated with that standard. Reconvening the SDT that worked on EOP-008-1 may be necessary to accomplish this. For Interactive Remote Access, how do Cyber Assets used by the Responsible Entity differ from those used by employees? It is not clear why Responsible Entity is delineated in such a way. Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.

Yes

In the Background section, the SDT describes that the responsible entity will have a choice to evaluate BES Cyber Assets individually or collectively in a BES Cyber System. The opening paragraphs for High Impact or Medium Impact criteria need to be modified to make this clear. As written they do appear to provide a choice by stating "Each BES Cyber Asset or BES Cyber System". However, it does not make clear whose choice that is. The auditor might decide the choice belongs to them. Thus, these paragraphs need to be modified to make clear the choice belongs to the responsible entity. While similar and conforming changes need to be made to the Low Impact Rating as well, one additional change needs to be made. "All other BES Cyber Assets and BES Cyber Systems" should be changed to "All other BES Cyber Assets or BES Cyber Systems". Otherwise, there is no choice because both have to be included. This change would also conform Low Impact Rating to the Medium and High Impact Rating sections. While there are limitations on the TOP Control Centers such that not all TOP Control Centers will be included with a High Impact, there is no such limitation on the BA Control Centers. We recommend a similar limitation be place on a BA Control Center such that if the BA is not controlling assets that meet certain criteria in the Medium Impact they should not be included. There many small BAs that simply won't have a broad impact on the Interconnection and, thus, should not be included. Transmission Owner should be struck from Criterion 1.3. The Criterion states that it applies to Control Centers that are use to perform the functional obligations of the Transmission Owner and Transmission Operator. Per version 5 of NERC Functional Model, there are no functional obligations of a Transmission Owner that would be performed at a Control Center. Including Transmission Owner appears to be an attempt to address concerns regarding some RTO/ISO's Transmission Operator registration models that have been expressed in various forums by regulators. These concerns should not be addressed here in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. If the drafting team chooses not to strike Transmission Owner, we suggest splitting out Criterion 1.3 into two Criteria for clarity: one criterion for the Transmission Owner and one for the Transmission Operator. As Criterion 1.3 is written now, it could be interpreted as though the control of assets identified in criteria 2.2 and 2.5 – 2.12 only applies to the Transmission Owner. We believe the drafting team intended to apply these criteria limitations to the Transmission Operator as well. If indeed that is the intention, splitting them out would clarify the intent. Criterion 1.4 which obligates certain GOP control centers to be rated High

Impact includes criterion 2.12 as one of those reasons. 2.12 should be struck as it deals with UVLS and UFLS which are not GOP functions. We request that the drafting team clarify Attachment I or the associated requirements that BES Cyber Assets and BES Cyber Systems are not intended to be classified at more than one impact level even if they meet a criterion in multiple impact levels. We further ask the drafting team to clarify that the BES Cyber Assets and BES Cyber Systems that are part of a Control Center are not to be evaluated against other non-Control Center criteria. For example, if a GOP Control Center is used to control more than 1500 MW of generation, it would not be evaluated under criterion 2.1 but rather under criteria 1.4 and 2.13. As the criteria are written now, it is possible to interpret that the Control Center's BES Cyber Systems and BES Cyber Assets could qualify as both a Medium Impact under criterion 2.1 and, then, a High Impact under criterion 1.4. Criterion 2.3 creates an implied obligation on the Planning Coordinator (PC) or Transmission Planner (TP) to designate generation that is necessary to avoid BES Adverse Reliability Impacts. It is implied because there are not any requirements in any standard including the TPL standards that require the TP or PC to designate generation necessary to avoid BES Adverse Reliability Impacts. In fact, BES Adverse Reliability Impact is not even used in any requirements that pertain to the PC or TP. The implied obligation creates a compliance conundrum. Since it is only an implied obligation and not an explicit requirement, the PC and TP will never be required to meet it. How then, does the GOP or GO insure they get the information they need from the PC or TP? They have no recourse. Use of BES as a descriptor of Adverse Reliability Impact in Criterion 2.3 is redundant with the definition of Adverse Reliability Impact and should be struck. Criterion 2.3 focuses on the long-term planning horizon which is contrary to the standard. The standard focuses on reliability impacts caused on the BES in a 15 minute timeframe from the misuse, degradation or unavailability of the BES Cyber Asset or BES Cyber System. It does not make sense to subject BES Cyber Assets and/or BES Cyber Systems within a generator plant or GOP control center to these standards if a generator is identified as needed for reliability four years out but is not identified from year 0-3. For Criterion 2.5 regarding Cranking Paths, the last two bullets are confusing and the wording should be clarified. The graphic provided on page 26 in the Application Guidelines help with that clarification and the drafting team should consider adding this as an attachment so that it will remain with the standard. It is premature to base criterion 2.7 on the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index". It is still a work in progress. This document and approach is being developed under the purview of the Planning Committee's (PC) Reliability Metrics Working Group (RMWG). The PC has not approved any of the indexes. The only thing the PC approved was the approach and framework. At the December 2011 PC meeting, it was clear that the RMWG has additional work to do to finalize the indexes. Thus, it is premature to use any of these indexes in the "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" in a standard. At the very least, use of them should be coordinated with the PC and RMWG. Criterion 2.9 is redundant to Criterion 2.8. FACTs devices are Transmission Facilities and are covered in 2.8. Criterion 2.11 presumes that failure of an SPS or RAS would cause an IROL violation. This is not likely. An SPS or RAS may be implemented for a specific contingency for example. As an example, when that contingency happens, certain switching might need to occur or generation run back. These automated actions might enable a higher limit on an IROL associated with a transmission corridor. If the SPS was not available, the limit would likely be lowered but not necessarily violated. A violation would depend on actual system conditions at the time. Thus, the language should probably be change to something along the lines of impacts or enables higher IROL limits. Criterion 2.13 has control centers in lowercase. This would mean that the proposed NERC glossary definition does not apply. Is this the intent? If so, how would this meaning of control center be different?

No

We think Requirement 1 and associated Attachment 1 should focus on identifying the BES Facilities that are important and then the associated BES Cyber Systems and BES Cyber Assets. Otherwise, all BES Cyber System and BES Cyber Assets will have to be inventoried. While the Background section states "Requirement 1 only requires that discrete identification of BES Cyber Systems and BES Cyber Assets for those in High and Medium categories", we do not see how a responsible entity can demonstrate that it has correctly identified all High and Medium Impact BES Cyber Systems and BES Cyber Assets unless it has a complete inventory of all BES Cyber Assets and BES Cyber Systems. We can envision auditors asking for such an inventory. Part 1.1 needs to be further refined regarding what kinds of changes are included. By the NERC Glossary definition, Facility can include relay equipment associated with protecting a transmission line as part of the "set of electrical equipment that operates as a single Bulk Electric System Element". Thus, a change to a relay setting could be

could be inadvertently included. It should not be. We suggest the changes be limited to topological changes, generator interconnections and generator uprates and equipment retirements. While other changes such as permanent derates may allow that responsibility entity to lower the categorization of BES Cyber Systems and/or BES Cyber Assets, the reduction in compliance burden will cause them to do this. Thus, we don't need to increase their compliance burden by requiring them to do it for permanent derates.

No

Because regional entities already expect evidence to be signed and dated by persons of authority, there is no reason to have a specific requirement to have the CIP Senior Manager or delegate do this. The requirement is unneeded and the compliance auditor likely won't accept evidence for Requirement 1 unless it has been approved anyway by a person of authority. Thus, this requirement actually creates a form of double jeopardy that an entity could be held in violation of Requirement R1 and R2 for failure of the CIP Senior Manager or delegate to approve the list of BES Cyber Asset and BES Cyber Systems categories. Because there is no question dealing with other sections of this standard, we are adding comments regarding those sections here. We disagree with all the specificity in the applicability and facilities section for Distribution Provider (DP) and Load Serving Entity (LSE). These sections are not consistent with the Compliance Registry Criteria and will only cause confusion. There is no specific compliance registry criterion for including a DP that has been included in the Transmission Operator's restoration plan. Because NERC clearly states in their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2) that they will not enforce the standards against entities that are not registered, the standard simply couldn't be enforced against such an entity included in the TOP's restoration plan unless they were already registered. Furthermore, the Compliance Registry Criteria already allow NERC to register a responsible entity as a DP and LSE if that entity "owns, controls, or operates facilities that are part" of a required UFLS or UVLS program, special protection system (SPS) or transmission protection system. Since the DP or LSE with a required UFLS or UVLS program, SPS or transmission protection system, is already registered, how does this applicability section provide any more clarity? The DP or LSE will know whether they own or operate these facilities and simply will provide the appropriate response in any required CMEP submissions such as audits and self-certifications. If the responsible entity is not registered as an LSE or DP even if they own these facilities, then again NERC can't enforce these proposed CIP standards against the entity per their Rules of Procedure Appendix 5B Statement of Compliance Registry (see the first paragraph on page 2). In the Facilities section, we are concerned that non-BES Facilities will be included in the standard. Non-BES Facilities should not be included at this juncture given that the Project 2010-17 Definition of Bulk Electric System drafting team is just beginning its work on the second phase of defining the BES. Until this work is completed, non-BES Facilities should not be included and, then, they should only be included with significant justification. There should be a high bar for deviating from the BES definition particularly since it will be recent and have considered all issues facing the industry at that time. The application guidelines have not clearly identified all functional entities that might have some responsibility for the various BES Reliability Operating Services. For instance, in the Dynamic Response section, Special Protection Systems responsibilities are attributed to only TO but this could be a GO or even DP responsibility. UFLS and UVLS are only attributed the DPs but the TO could choose to implement these systems on the transmission system. Governor Response could also be a GOP responsibility. Another example would be the current and next day planning in the Situational Awareness section. It is only attributed to the TOP even though there are NERC standards that require the RC to perform next day planning. In the Managing Constraints section, the responsibility for interchange schedules is attributed to the TOP and RC. It should be attributed only to the Interchange Authority or Interchange Coordinator. In the Restoration of the BES section, the responsibility for off-site power for nuclear facilities is attributed to the TOP. In the NUC standard, it is actually attributed to the transmission entity which could be one of eleven functional entities. Since there many errors (we did not identify all of them) in attributing responsibility in this section, we suggest the drafting team completely review this section and update it or consider removing the responsibilities altogether as their purpose is not clear. We believe the statements beginning on page 23 and continuing on page 24 of the High Impact section of the applicability guidelines regarding TOP delegation to the TO should be removed. If the TOP has delegated some functions to the TO that would otherwise have been carried out in the TOP Control Center and might have resulted in additional TOP BES Cyber Assets and BES Cyber Systems being categorized as High Impact, this delegation should not have an impact on the TOs categorization of BES Cyber Systems and BES Cyber Assets. First, the TOP is still responsible and can't pass that

responsibility on through a delegation agreement. Thus, the TOP and TO will have to address this in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO. The TO likely owns these BES Cyber Assets and BES Cyber Systems, and they should be classified according to the criteria established for TOs in Attachment 1. Use of the term asset in the definition requires ownership by the responsible entity. If is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third, control Centers for TOs are not addressed in Attachment 1. Fourth, this appears to address some concerns regarding some RTO/ISO's TOP registration models that have been expressed in various forums by regulators. These concerns should not be addressed in piecemeal fashion but holistically in a forum covering all concerns and issues with the registration model. Fifth, there is nothing in the requirements that requires these BES Cyber Assets and BES Cyber Systems to be categorized in this manner. The application guidelines are not requirements and cannot modify the requirements. They can only help explain the requirements. However, these statements are fundamentally altering the requirements and how the attachment 1 criteria are applied. In the first paragraph on page 25 in the application guidelines, there is statement that indicates there may not be a Planning Coordinator for a given area. This statement is contrary to the Section 501.1.4 of the NERC Rules of Procedure. This section states that the registration process shall ensure that "no areas are lacking any entities to perform the duties and tasks identified in and required by the reliability standards". In the third paragraph on page 25 in the application guidelines, Category D contingency should be removed. The TPL standards only require a Planning Coordinator or Transmission Planner to document the impacts of Category D contingencies. There are no performance requirements for Category D contingencies. Thus, it is highly unlikely that any Planning Coordinator or Transmission Planner could ever justify the costs for reliability must run unit through Category D contingencies to its regulator, and, thus, there likely will not be any. In several places in the application guidelines (occurs on pages 26, 27, and 29), exceeding an IROL is discussed when the SDT really means violating an IROL. An IROL by definition has two components. It has a limit and a time constant called Tv. This time constant can be up to thirty minutes and usually is. The time constant is set based on how long the IROL limit can be exceeded without exposing the BES to an unacceptable risk. Thus, an IROL is only violated once the limit has been exceeded for a time greater than Tv. An IROL is exceeded but not violated when the time of the exceedance has not reached Tv. We suggest the drafting team modify the application guidelines in this standard and any other standard with the appropriate use of exceed or violate for the IROL consistent with this explanation. In the third bullet on page 29, the term regional load shedding requirement needs to be made consistent with the new UFLS standard. The UFLS program will be developed by the Planning Coordinator and not the Regional Entity. The NERC adopted version of the standard does not even require a regional version of the standard as was originally proposed.

No

The VSLs for R2 are not consistent with the requirement. Requirement R2 allows the CIP Senior Manager or delegate to approve identification and categorization of High and Medium Impact BES Cyber Assets or BES Cyber Systems. The VSLs drop the "or delegate" language which implies the CIP Senior Manager has to approve the categorization and identification. The "or delegate" language should be added back.

This requirement should be struck along with all references to CIP Senior Manager in the CIP standards. This requirement dictates a corporate governance structure for no reliability reason. An entity should be free to have two, three or more officers or personnel to oversee various portions of the CIP program. The responsible entity will still be required to meet the CIP requirements regardless. Furthermore, mandating a single CIP Senior Manager implies that potential for sanctions up to $1,000,000 per day per violation are not enough to get senior management's attention. This implication is totally contrary to the purpose of making standards enforceable by such sanctions. No other standards require identification of single senior manager and no reliability justification has ever been provided for why one is needed for the CIP standards.

No

We agree there should be "one or more documented cyber security policies that represent the Responsible Entity's commitment to the protection of its BES Cyber Systems and addresses" the required ten topics seem reasonable. However, the items that a "Responsible Entity should consider" for inclusion in its cyber security policy as stated in the Guidelines and Technical Basis section (application guidelines) of the standard appear to be written as requirements and the drafting team should consider moving them to R2 if auditors will ultimately treat them as requirements. This will

reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. Requirement R2 should also be modified to make it clear that an entity may write exceptions into their cyber security policies. FERC made it clear in Order 672 that only the requirements in a standard are enforceable and part of the standard. Thus, while the application guidelines make it clear the responsible entity can write in exceptions to its cyber security policy, the application guidelines are not enforceable and there is no way of ensuring that auditors follow them. Furthermore, we believe the fourth bullet in section 2.3 Remote Access regarding including language in contracts with vendors, consultants and contractors requiring them to follow the responsibility entity's cyber security policy should be modified. The bullet should apply to future contracts and not existing contracts to avoid the need to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. In addition, M2 bullet 2 says "Records that indicate the required ten topics were implemented." What exactly does "implemented" mean in this case? That the items the responsible entity should consider for each of the topics are included in the policy(ies)? This needs to be clarified.
No
What does "initially upon the effective date of the standard" mean? It could be interpreted that the cyber security policies would need to be reviewed and approved on the date the standard is effective which is not reasonable for a myriad of reasons. A couple of those reasons could include that the effective date could be a holiday or weekend or the CIP Senior Manager is not available (they could be incapacitated). Ultimately, we believe that the intent is for the cyber security policy to be in effect and approved by the effective date rather than on the effective date and to ensure that is has been reviewed recently particularly since the implementation plan is a minimum of 18 months. Then going forward subsequent reviews and approval would take place at least once per calendar year not to exceed 15 calendar months. If this intent of this requirement, there really is no way to ensure the review occurred recently without making the requirement retroactive which clearly cannot be done within a requirement. In addition, M3 bullet 1 implies that a Responsible Entity needs to have a "document management system." The word "system" could mean an application to manage documents. It could also mean a process for managing documents. Rather than leave it open to interpretation, we recommend eliminating the phrase, "from a document management system."
No
Awareness of a security program is covered in depth in CIP-004-5 and ensuring accessibility and availability of cyber security policies goes hand in hand with this. We recommend removing R4 from CIP-003-5.
No
Based on the assumption that there will be a CIP Senior Manager, we generally agree with the use of a delegate. We even believe it would be reasonable for a delegate to approve the cyber security policy. However, we do not agree with the use of "CIP Senior Manager" in this requirement based on our comments for R1 in question 6.
No
Based on the assumption that there will be a CIP Senior Manager, we agree with this requirement. However, we do not agree with the use of "CIP Senior Manager" in this requirement based on our comments for R1 in question 6. There is an extraneous number 2 at the end of the requirement.
No
We disagree with the VSLs for R2. More gradations could be provided based on the number of parts missed. Since there are 10 parts, there is plenty of room for four VSLs. The VSLs for R6 should consider using the numbers of days that documentation of the change to the CIP Senior Manager documentation is late. Use of number of days late is a common way to write a VSL and allows more gradations.
No
For Part 1.1, the rationale box does not appear to agree with the requirement. It states the need to ensure everyone with authorized access receives this awareness was removed. Yet, the requirement applies to the responsible entity and does not appear to exclude anyone with authorized access. Which is it? Furthermore, the rationale box should be more specific and use the full names of both types of access which are: authorized electronic access and authorized unescorted physical access. Otherwise, generically referring to authorized access could mean one or the other but not both, or it could mean both.

No
We agree with the concept that training should be role based. As an example, a system operator who is an end user of an EMS does not need most of the training identified in the various parts of Requirement 2. The system operator certainly does not need training on recovery plans for BES Cyber Systems but might need training on the visitor control programs and how malicious actors might use social engineering to gain access to the EMS. The problem we see with the requirements and it parts is that it does not make clear anywhere the need to identify what training each role would receive. Rather it only states that roles must be identified and then identifies training in the various requirement parts that apply to the main requirement which could be construed as applying to the whole training program including all roles. The paragraph references in the rationale boxes for parts 2.6 and 2.7 are inaccurate. Paragraphs 632-634, 688, and 732-734 refer to CIP-007 and CIP-009. There are no references to issues in CIP-004. While paragraph 413 does discuss CIP-004, it only describes what is in the standard and not any changes directed to the standard. In regards to Part 2.6 and storage media, the only mention in Order 706 of storage media is in paragraph 635 and it directs NERC to determine what it means to prevent unauthorized retrieval of data using storage media.
No
This requirement needs to be clarified that it only is intended to require appropriate role-based training for each individual with authorized electronic access or authorized unescorted physical access based on their specific job responsibilities and not the entire cyber security training program identified in R2. Use of the word “needing” is problematic. An entity cannot grant authorized electronic access or authorized unescorted physical access unless it is needed per CIP-007-5 R5. We suggest changing “each individual needing authorized electronic…” to “each individual with authorized electronic…” For consistency across the standards and clarity, we suggest every use of “authorized electronic or unescorted physical access” be replaced with “authorized electronic access or authorized unescorted physical access”. This will help to avoid similar confusion that arose in previous versions of the standard in which it was not clear if “authorized” applied only to electronic access or unescorted physical access. It will further make it clear that authorized electronic describes one type of access. Regardless of how it is written, it needs to be consistently used across that standards and it is not.
No
Part 4.2 may not be possible to complete. While we agree with the need to conduct seven year criminal history checks, obtaining all addresses may not be possible. The responsible entity can verify the current address or a recent address from reviewing a driver’s license but after that the responsible entity cannot with certainty verify that it has all of the former work, home and school addresses of the employee. The employee may not provide the addresses and the background check may not provide these additional addresses. The requirement needs to be clear that the responsible entity may request this information from both the vendor providing the background check and the employee but will not be held accountable for either party’s failure to provide a complete list of addresses. Part 4.3 could be problematic for a responsible entity and needs to be clarified that the responsible entity does not need to establish hard and fast criteria that must always be followed. Finding qualified personnel to work in these highly specialized fields is challenging enough without adding this additional constraint. Background checks may certainly reveal problems with an otherwise qualified person. While some of these problems would be obvious reasons to disqualify a person, others may simply require further research and explanation from the individual for why it is not a problem.
No
In general, we agree with the requirement but believe the requirement should be further clarified, perhaps in the measurement, that in no circumstance should a responsible entity be asked or required to show the personnel risk assessment for an individual to auditor and enforcement personnel. There are a myriad of reasons not to show the actual personnel risk assessment including privacy concerns and other applicable laws may prevent this.
No
The application guidelines on page 44 state that access authorization and provisioning should not be performed by the same person. While this is a laudable goal, it should be clear that small entities may simply not have the staff to accommodate this guideline. We suggest adding “where possible” to this statement.
No

It is not clear why resignations are separated from terminations in Parts 7.1, 7.3, 7.4 and 7.5. Resignations are voluntary terminations. We are unsure what the drafting team intends to accomplish by splitting them out. Where do retirements and layoffs fit in? Since there does not appear to be any different requirements on resignations and terminations, we suggest to use only the generic termination to avoid this confusion. Part 7.2 does not address the situation for phased transfers. For many entities, a transferred employee could continue to need authorized electronic access and authorized unescorted physical access for a long period of time to provide support particularly if a new employee is being trained. This could occur long after the transfer date. While the application guidelines do address this issue, they are simply not requirements and NERC is not bound to follow them. Thus, we suggest making Part 7.2 more generically state that the authorized electronic access and authorized unescorted physical access should be terminated once management determines it is no longer needed. We are a little surprised that the application guidelines state in the scenario table that no action is required to revoke access in the event of a death. While we agree there would be no immediate additional risk for obvious reasons, access should still be revoked at some point.
No
VSLs for Requirements R2 and R3 should have more gradated levels. For R2, there could easily be several roles which would allow for more than two VSLs. Since there are 10 parts to the requirement, four VSLs could easily be written based on the number of parts missed. For R3, more VSLs could be written based on the percentage of individuals that were not trained. The Severe VSL for Requirement R5 incorrectly includes personnel risk assessments (PRA). PRAs are dealt with in Requirement R4.
No
The requirements of Parts 1.2 and 1.3 make no mention of egress while the associated measures specifically mention it. Does the drafting team intend for there to be procedural or physical access controls regarding egress? If so, that is not clear in these standards at all and could set up a responsible entity for a compliance violation. We do not believe that egress controls should be necessary. Only ingress controls are necessary to prevent access to unauthorized individuals. Egress really only helps in knowing who is currently within the Defined Physical Boundary which might provide some value but the expense of installing egress physical access controls would likely far outweigh any benefit. It is unclear how the “operational and procedural controls” required in R1.1 differ from the “physical access controls” required in R1.2 and R1.3. Suggested methods for restricting physical access are given in the “Guidelines and Technical Basis” (application guidelines) section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. Also, regarding the application guidelines, it would be helpful if the section labeled “Requirement R1,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
We believe that this proposed requirement improves upon the existing requirements. However, we believe that individual point of contact could be confusing. We recommend changing it to escort and making it clear in the application guidelines that this would be the main escort with responsibility for the visitor but not necessarily someone who is with the visitor the whole time. Others could also temporarily escort the visitor. Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 2,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
Regarding the “Guidelines…” section, it would be helpful if the section labeled “Requirement 3,” was also sub-labeled for each of the sub-requirements. This would help link the suggested methods and commentary to the appropriate sub-requirements.
No
A visitor control program is intended to identify and log visitors to the Defined Physical Boundary (DPB). They cannot gain access due to other requirement such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training

requirements of CIP-004-5 compel a responsible entity's personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the DPB. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF.
No
On page 39 of the application guidelines in section 1.2, Component should be made lower case.
No
Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending "if less than three character types" to the end of the requirement for further clarity.
No
Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
No
EOP 4 in the Rationale box should be replaced with EOP-004. While Part 1.2 requires a process to identify Reportable BES Cyber Security Incidents, there is no indication of who is to receive these reports. There is only Part 1.3 that requires the responsible entity to identify internal and external staff to which to communicate the "incident". Does that mean the list of recipients is totally up to the responsible entity and could be null? If not, then the drafting team needs to identify the minimum list of recipients. In Part 1.3, we assume the drafting team means Reportable BES Cyber Security Incidents by the use of the term "incident". If this assumption is correct, please replace "incident" with "Reportable BES Cyber Security Incident".
No
The requirement in part 2.1 appears to apply to actual BES Cyber Security Incidents. However, the requirement states that deviations from tests should be recorded. Thus, "or test" needs to be struck. R2 Part 2.2 uses the phrase "initially upon the effective date of the standard." It is not clear as to the meaning of this phrase. It could be interpreted that the BES Cyber Security Incident response plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not reasonable. If the intent of this requirement is to do an initial implementation within some time period of the standard becoming effective, then the requirement should state a time period for this to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.
No
R3 Part 3.1 uses the phrase "initially upon the effective date of the standard." It could be interpreted that a review of each BES Cyber Security Incident response plan would need to take place on the date the standard becomes effective. Because Requirement R1 compels the development of the response plan, it does not make any sense to compel review of the response the same day the requirement of the response plan becomes effective. Rather the response plan review should be required the following calendar year after its initial approval. No application guidelines were written for this requirement. The drafting team should consider either writing some or making a statement that they are purposely omitted.
No
For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.

No
The stated rationale for Part 1.1 does not support the change and additional rationale needs to be provided. Paragraph 694 of Order 706 requires NERC to develop a specific requirement to implement the recovery plan. This requirement is not an implementation requirement but still a requirement for what to include in the plan. Thus, we do not see how the rationale supports the requirement. Part 1.2 should not require either names or titles. These are problematic in that the recovery plan has to change for every personnel move which includes transfers, terminations and promotions. A promotion of IT Analyst to Senior IT Analyst would necessitate an unnecessary change. A better approach would be to allow the use of generic roles such as analyst or even perhaps staff from department X. The requirement needs to allow some flexibility to avoid unnecessary paperwork that provides no reliability benefit. The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ.
No
Part 2.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the recovery plan(s) would need to be implemented either by responding to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise on the date the standard becomes effective. This is not practical for many entities and especially for smaller entities. Part 2.2 of CIP-008-5 R2 already requires BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Many of the same staff involved in the BES Cyber Security Incident response plans will likely be heavily involved in the recovery plans. The important part is that the recovery plan will be in place on the effective date per CIP-008-5 R1 and will likely have been tested prior to the effective date. Thus, the requirement should simply state a reasonable time period that can be met by limited staff for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Part 2.2 has potentially has a similar issue to Part 2.1 but is less clear. Rather than use the full term “initially upon the effective date of the standard” it just states that the test must be conducted initially. We assume the drafting team meant for this to be conducted on the effective date similar to Part 2.1. This makes completing this part and other parts mentioned in the previous paragraph even more impractical. The requirement should simply state a reasonable time period for the actual implementation or exercise to be completed after the effective date of the standard. Then going forward subsequent implementation would take place at least once per calendar year not to exceed 15 calendar months. Since Part 2.3 requires a full exercise in representative environment every 39 months and is required to be included per FERC directive, we recommend that it be limited to High Impact BES Cyber Systems. Conducting this test in a representative environment could get very expensive because responsible entities may have to purchase the appropriate equipment to set up a parallel environment. This is simply not practical or cost effective to do for every BES Cyber System. Is it really practically to set up a representative environment for every 500 kV substation or special protection system for testing?
No
Part 3.1 should be modified to require the first review of the recovery plan in the subsequent calendar year to the approval of the requirement. To accomplish this, the drafting team should strike “initially upon the effective date of the standard and”. CIP-009-5 R1 already compels the responsible entity to have a recovery plan and becomes effective on the same day as Part 3.1. Thus, the plan will already have been reviewed when it was developed and approved. Thus, it does not make sense to have a separate review in Part 3.1 on the effective date. For consistency with Part 3.3, R1.2 in Part 3.5 should be written as Requirement R1, Part 1.2.
No
The VSLs for Requirement R1 should include more gradations than two levels based on the number of parts missed. For Requirement R2 and R3, four VSLs could be written based on the number of days late for completing the task. This is a common way to write VSLs.
No
Part 1.1.6 could be redundant with CIP-007-5 Part 2.2. While CIP-007-5 Part 2.2 does not explicitly require documentation of the security-patch levels, demonstrating compliance with it ultimately will require such documentation. Thus, it becomes redundant with Part 1.1.6 of CIP-010-1 R1. If not redundant, it certainly sets up a high probability for double jeopardy because each compliance

violation of CIP-007-5 Part 2.2 will likely result in a violation of Part 1.1.6. Part 1.2 is unclear. Is this intended to require the CIP Senior Manager or delegate to authorize the process to develop a baseline configuration or is it intended to require the CIP Senior Manager or delegate to authorize deviations to the baseline? As a result, Part 1.2 needs to be clarified. As it is written now, the only clear requirement from Part 1.2 is the need to document baseline configuration deviations. Part 1.4.1 requires the responsible entity to identify the cyber security controls that could be impacted by the change. This appears to be the first use of cyber security controls in the library of CIP standards. As a result, the intent and meaning of the term needs to be further clarified.

No

Part 3.1 uses the phrase “initially upon the effective date of the standard.” It could be interpreted that the security controls for every applicable BES Cyber System and BES Cyber Asset need to be assessed on the date the standard becomes effective. This is not practical particularly for smaller entities. Several other requirements including Part 2.1 of CIP-009-5 and Part 2.2 of CIP-008-5 R2 already require significant action on the effective date of the standards. Part 2.1 of CIP-009-5 requires recovery plans to be implemented on the effective date and Part 2.2 of CIP-008-5 R2 requires the BES Cyber Security Incident response plans to be exercised on the effective date of the standard. Imagine the amount of personnel and effort necessary to complete all of these tasks on (not by) the effective date. Many of the same staff involved in the BES Cyber Security Incident response plans and recovery plans will likely be heavily involved in the vulnerability assessments. The requirement should simply state a reasonable time period for the vulnerability to be completed after the effective date of the standard or make it clear that the vulnerability assessment needs to be completed by the effective date and not on. Part 3.2 has a similar issue as Part 3.1 in that it appears to require a vulnerability assessment for all High Impact BES Cyber Systems on the effective date of the standard. We have the same issue with this requirement in that the same limited set of staff will likely be responsible for completing these assessments as the tasks compelled by several other requirements that must be complied with on the same effective date.

No

In general, the VSLs escalate violations to the higher end of the sanctions matrix too rapidly for minor violations. This could be fixed by writing VSLs for each level rather than just High and/or Severe VSLs in some cases. For example, if an entity fails to establish a single baseline on one applicable BES Cyber System or BES Cyber Asset per Requirement R1, it would be deemed a High VSL. If that is one out of one thousand BES Cyber Systems or BES Cyber Assets, this would seem excessive. Likewise, if an entity is one day late in updating their baseline configuration per Requirement R1, the violation would be deemed Moderate. This is not consistent with many other requirements in the CIP proposal which provide four VSL based on the number of days late.

No

The rationale for Requirement R1 indicates Requirement 4.1 was moved to the BES Cyber System Information definition. It does not reference which standards the requirement comes from. It needs to for clarity. Part 1.1 needs to be clarified. We believe the requirement pertains to ensuring BES Cyber System Information is either marked in some way to be clear it is BES Cyber System Information or recognized as such by the responsible entity’s personnel. However, we are concerned that requirement could be interpreted as needing to develop a method to ensure that all BES Cyber System Information has been found and there is no extraneous information. In other words, we are concerned the requirement could be interpreted as requiring the method to be some sort of search process. We think this problem would be solved providing some discussion of the intent of the requirement in the application guidelines. Part 1.3 needs to be modified. It requires the responsible entity to assess its adherence to its BES Cyber System Information protection process “upon the effective date of the standard”. This does not make any sense since the responsible entity will have just then been required to utilize the BES Cyber System Information protection process. What will they assess? This requirement should not require this assessment until the process has been in use for a year. Part 1.3 uses a term “protection process” that was not used previously in the requirement. For consistency with other requirements and clarity, we suggest that either that term be used in Requirement R1 instead of just the term process or that “protection” be struck in Part 1.3 and replaced with a reference to the main requirement.

No
We agree with the implementation plan concept that essentially bypasses the effective dates of version 4 of the standards for version 5. This will significantly lessen the compliance burden for responsible entities to avoid two separate transitions and avoid the confusion of preparing for version 5 while still preparing for version 4. We believe that some requirements should have delayed implementations plans rather than become effective on the same date as the remaining requirements. Some requirements are dependent on the completion of other requirements and do not make sense to implement until the other requirements have been in effect for some time. Consider Part 1.3 of CIP-011-5. It requires the responsible entity to perform an assessment of its adherence to the BES Cyber System Information protection process. However, the protection process is only required to be in effect the same day. What sense does it make to assess adherence to a process that was just started? The drafting team should perform a complete review of all the requirements for dependencies and determine an appropriate staggered implementation for them. The first sentence in the “Proposed Effective Date for Version 5 CIP Cyber Security Standards” on page 2 should be modified. It states the responsible entities must comply with the definitions on the effective date. Definitions have no compliance obligations. They simply become effective and help explain the requirements. We suggest 18 Months Minimum should be modified. Please change the “date of the order” to “effective date of the order” for clarity. FERC typically issues an effective date of their orders that is dependent on publication in the federal register and is different from the date the order is published. This will help provide clarity that the effective date of the order is the appropriate date to reference rather than the publication date. This will need to be changed across all the standards and the definitions.
Individual
Kevin Koloini
AMP
Yes
AMP agrees with the APPA trade association comments for the definitions.
Yes
Distribution Providers have not been applicable in the past to CIP-002. Adding Distribution Providers to the full gamut of CIP is a significant increase in the requirements for smaller organizations. Smaller organizations that may not currently have the resources for implementing many of the requirements, especially those that are recurring, time consuming and that require multiple policies and procedures. We need to draw the line somewhere. Adding these requirements to organizations that do not have in-house expertise or resources seems excessive when done on a recurring basis (once a year for many requirements as drafted). A NERC Alert for Distribution Providers may serve that function and the industry in a more economic fashion by reducing the time commitment and the required policies and procedures. Distribution Providers will still increase awareness, improve core competencies in security, and protect their equipment, but would not be required to perform the "paperwork" or "exercises" associated with the CIP standards as drafted. Please remove Distribution Providers.
No
The requirement is good. I believe it would be better if the language "within 30 calendar days" was removed. I believe there is a small percentage of changes that would occur for most organizations and for those that do have changes 30 days may not be enough time.
No
Why does this need to be a recurring requirement? Upon identification and categorization, there are typically no changes and those that do change are typically addends. All I am saying is that this requirement asks for every Responsible Entity to do an exercise even if a large majority of the entities will have a similar or identical result as the previous year. I don't see the point. Suggest: "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and upon Cyber Asset or Cyber System changes."
No
Yes

No
Proving implementation is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for implementation.
No
Extend the requirement's review period or make it event-based. I suggest 2-5 years for the review period.
No
I agree with the intent of the requirement. I believe that individuals should be aware. However, I feel that the auditing process will require training logs. Why not just make the requirement fit the implementation to make it easy for everyone. "Each Responsible Entity shall train staff that have access to BES Cyber Systems, maintain a log of awareness training and material, and maintain a list of staff who have access to BES Cyber Systems." Despite my suggestion, I feel this requirement is not needed.
No
Once the CIP Senior Manager has been given authority and responsibility, the CIP Senior Manager should be able to delegate without having to have a paper trail for each delegation, otherwise I feel the CIP Senior Manager is delegating authority and responsibility by naming another person. What is the result this requirement is going to achieve?
No
Remove the 30 day requirement and remove the delegations. Consider a simpler requirement where the CIP Senior Manager status changes. I believe this requirement can be eliminated and the rest of the requirements will still achieve a reliable result.
No
No
Proving the implementation happened is difficult without clear and simple expectations. I suggest removing implement from the requirements or explicitly describing the expectations for compliance beyond documenting the processes.
No
Eliminate the requirement or revise with the results in mind. As written, this is a requirement that has the potential to be highly violated and that may or may not prevent a physical or cyber event in whole or in part.
No
Eliminate the requirement.
No
Eliminate the requirement.
No
Eliminate the requirement.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No

Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the plans.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the programs.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Yes
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the plans.
No
Replace "and" with "or".
No
Yes

No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
Yes
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Proving that an implementation has occurred is difficult without clear and simple expectations. Remove implement or explicitly describe the expectations for compliance beyond documenting the processes.
No
Yes
Group
FirstEnergy
Doug Hohlbaugh
Yes
SUMMARY COMMENTS: FirstEnergy (FE) recognizes the dedicated work of the CIP Standards Drafting Team (SDT) in developing the proposed version 5 CIP standards. FE supports much of the SDT's work and changes offered by CIP V5. While we are balloting against the version 5 standards at this time, our voting position should not be viewed as a fundamental disagreement with the SDT's approach. However, we believe there is value in building on the version 4 CIP standards retaining certain key aspects of the standards which have already been implemented by hundreds of registered entities within industry. FE strongly supports further enhancements to the cyber security standards that improve reliability while providing compliance clarity and alleviating burdensome administrative tasks that do not improve reliability. As further described below, we propose the SDT: 1. retain the CIP-002-4 standard with slight modifications 2. continue to build upon its work for CIP-003-5 through CIP-011-5 3. develop a new standard for low impact critical cyber assets This proposal offers greater opportunity for the industry to deliver timely improvements needed in controls for medium and high impact cyber assets while further vetting any potential obligations for low impact cyber assets. Many

of the changes offered through CIP V5 are well received by FE. We appreciate that the SDT has tried to alleviate the need for TFEs where possible within the standards. As an example, CIP-007-5 R3 is a much needed improvement regarding malware prevention and no longer prescribes a specific technical method (anti-virus) as found in the existing CIP-007-3 R4 (which has historically generated a number of TFEs). We support the proposed table format which clearly shows the requirements and measures together and the additional insight and guidance offered by the Application Guidelines located in the back of each standard. The ability to classify BES Cyber Systems is also a welcomed change that helps simplify the maintenance of cyber asset lists subject to the CIP standards. Additionally, the proposal of new CIP-010-5 and CIP-011-5 standards more efficiently present obligations for configuration management, vulnerability assessments and information protection than the current CIP version standards. However, we encourage the SDT to retain certain existing terminology such as Critical Cyber Assets, Physical Security Perimeter over their proposed counterpart BES Cyber Asset and Defined Physical Boundary even if actual definition changes are warranted. FE is opposed to any instances of terminology name changes where no clear need is justified as the modifications will require significant industry resources to unnecessarily modify compliance procedures and processes. A significant departure from existing standards is moving away from determining cyber assets as “essential” to the Critical Asset that if “destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.” The introduction of BES Reliability Operating Services which if “misused” significantly increases the scope of cyber assets that could be subjected to the CIP standards. The NERC CIP standards should specifically define "Impact" as "The effect on the Bulk Electric System reliability if the essential asset is destroyed, degraded, or otherwise rendered unavailable." This is significantly different from whether an asset is "misused." If an asset has no external connectivity (i.e. not routable or dial-up), the assumption is that it cannot be misused by a remote attacker. However, it could be rendered unavailable -- which is why the assessment of "essential" is so important. As an example, an RTU -- if misused -- could have high impact on the BES. However, that same RTU -- if rendered unavailable (e.g. from a buffer overflow, loss of a communications circuit, or an ax to the chassis!) -- may have absolutely zero impact on the BES reliability. The term "misused" is therefore inappropriate in this context and should be removed from the language of the standards altogether. If that stays in the language, we'll have hundreds of new assets to manage under CIP that have little to no reliability impact if lost. We also suggest the SDT retain the concept of first identifying Critical Assets and then associated Critical Cyber Assets since the Attachment 1 Criteria listed in CIP-002-5 still refer to physical facility locations in most cases and are very similar to the NERC BoT approved “bright line” CIP-002-4 standard. In summary, we would like to see CA, CCA and PSP be retained terms with the definitions applied as suggested below. Therefore, we suggest retaining the CIP-002-4 standard with relatively minor adjustments to bring in some aspects of the SDT’s proposed CIP-002-5 standard. For instance, CIP-002-4 Attachment 1 could easily be adjusted to identify which criteria would qualify as high impact and medium impact in a similar manner as shown in attachment 1 of version 5. We are also supportive of other changes such as modifying version 4 Attachment 1 criterion item 1.7 to better match its version 5 counter-part criterion item 2.7 which lowers a threshold substation voltage level from 300kV to 200kV for qualification as medium impact facilities. The expansion of cyber protection to low impact devices, while warranting consideration, brings into scope many registered entities that have no CIP obligations today. The low impact requirements proposed by the SDT seem relatively benign on the surface and describe reasonable practices. However, they bring into question the ability to produce auditable evidence. For example, while it is indicated CIP-002-5 requirement R1 that BES Cyber Systems deemed to be low impact do not require discrete identification, yet it is unclear how the Compliance Enforcement Authority would be able to randomly sample whether or not an entity removed manufacture default passwords without an entity having a complete and thorough list of the devices. Producing such a list would not be insignificant and the reliability benefit requires further vetting in the proposed separate low impact standard. FE believes the low impact categorization is missing an important aspect regarding the connectivity of the cyber asset. Scope expansion beyond cyber assets with External Connectivity (routable and dial-up) greatly increases industry burden with questionable reliability improvement. Additionally, the FERC in Order 706 paragraph 285 states “CIP-002-1 provides that a critical cyber asset must have routable protocols or dial-up access … We do not find sufficient justification to remove this provision at this time. ” It is clear that, FERC did not explicitly direct NERC in its role as the ERO to expand coverage of cyber assets beyond those with external connectivity. However the Commission did direct the ERO to “consider the comment” made by an industry stakeholder that “argues that devices that use non-

routable protocols should also be considered as possible critical cyber assets." Therefore, FE believes that this subject requires further vetting in a separate standard focused on the controls required for low impact cyber assets. We would support a categorization as follows: 1. High Impact – CIP-002-5 Att. 1 High cyber assets regardless of connectivity. a. Essentially all the Control Centers described and regardless of connectivity. 2. Medium Impact – CIP-002-5 Medium cyber assets with External Connectivity 3. Low Impact – CIP-002 Att. 1 Medium cyber assets without External Connectivity and other BES (not captured in 1 or 2) cyber assets with external connectivity. The SDT spent a significant amount of effort describing the BES Reliability Operating Services to be evaluated in determining whether or not a cyber asset qualifies as a BES Cyber Asset. FE suggests that the BES Reliability Operating Services information be used solely as useful guidance in the Application Guideline section of CIP-002-5 that an entity could use to better assess if a cyber asset is "essential" to BES reliability and therefore subject to CIP standards and not be incorporated as an official NERC Glossary of Terms definition. In FERC Order 706 paragraph 284 the Commission in commenting about a stakeholder concern of too few critical cyber assets being identified indicates they share the concern but state: "However, there is no evidence that will be the case, and there is no formally accepted method for identifying critical cyber assets before us at this time. Therefore, we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." Based on FERC's comments, we do not see a need for the drastic departure from the existing definition of Critical Cyber Asset and believe that the references to BES Reliability Operating Services within the proposed CIP-002-5 standard only further confuses compliance expectations. GENERAL COMMENTS FOR ALL STANDARDS: Since the Comment Form does not offer opportunity to address miscellaneous items outside of the specific questions raised by the Standard Drafting Team (SDT), prior to addressing this Definitions question, we offer comments that apply to all the standards. In a similar manner, if we have feedback related to a particular standard that is not addressed by one of the SDT's questions, we include our feedback in the 1st question related to the subject standard. ♣ We ask that the team add clarity around the term "routable" because there could be misinterpretations in the industry. The industry standard seven-layer OSI reference model defines "routable" as "Layer 3 and above". We believe this should be clear in all definitions, requirements, and in any guidance that discusses the term "routable" throughout the CIP standards. ♣ Use of the term "real-time" – in several locations within the standard requirements, "real-time" is used. If the intent is to use the NERC Defined term, then this term should be capitalized within the requirements. ♣ Section B (Compliance), item 1.2 (Evidence Retention). The following statement causes confusion and should be deleted or clarified - "For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit." The section later implies that an entity need only keep evidence for three years, however, the preceding statement quoted above causes confusion; particularly in regard to a GO and GOP where scheduled audits are anticipated every six years. The standard should be clear on expectations. ♣ In many areas of the standards, requirement language contains the text "Initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between …" Any expectations of what needs to be accomplished to initially meet requirements should be clearly articulated in a standard's Implementation Plan and presents unnecessary requirement text. Although CAN-0012 "Completion of Periodic Activity Requirements During Implementation Plan" has already set expectations in this regard, we believe a clear Implementation Plan should address this matter within the CIP V5 standards. We offer proposed edits throughout the standards in regards to this topic. ♣ We suggest adding a definition in the NERC glossary for Annual defined as "A periodic activity occurring once each calendar year, not to exceed 15 calendar months between recurrences." This would alleviate the wordiness in each of these requirements, establish improved consistency across all standards having annual obligations and eliminate the need for CAN-0010. While both CAN-0010 and CAN-0012 indicate that an "annual" activity is met by performing the activity at least once per calendar year, each also refers to the not to exceed 15 months as the preferred approach. ♣ Section 4 (Applicability) and subsection 4.1 (Function Entity for Distribution Provider (4.1.2) and Load Serving Entity (4.1.6) contain redundant text with their counterpart Facilities (4.2) sections. We suggest streamlining the Functional Entity sections for DP and LSE to simply reference the information presented in the Facilities area. For example, rewrite item 4.1.2 to say "Distribution Provider that owns Facilities as described in section 4.2." ♣ The SDT implies that text from rational boxes will be moved to the guideline and technical basis section of the standard. We encourage the SDT to integrate this information into the existing guideline and technical basis information upon the second posting of the

standard so that we can see the complete guidance for each requirement. ♣ Violation Severity Levels – While we offer some comments on VSLs, in most instances we have not commented as it seems premature to comment in detail on VSLs until the requirement text is near final. As a general suggestion, it is useful when the requirement sub-parts are referenced within the VSLs listed in the VSL table. See standard CIP-004-5 as a good example of this practice. The SDT has not consistently used this format throughout the various VSL tables in other standards. Including the sub-requirement reference improves readability and ensures all parts of a given requirement are covered in the VSL table. ♣ The SDT should carefully review the table headings listed within each standard. In some cases each column says "Part" in each of the four columns instead of "Part, Applicability, Requirements, Measures". COMMENTS RELATED TO DEFINITIONS (Q1): 1. BES Cyber Asset – FE proposes the SDT abandon this definition and revert back to the existing Critical Cyber Asset term and its definition. 2. BES Cyber System – Change "Maintenance" to "Transient". We propose the definition be "One or more Critical Cyber Assets that are typically grouped together, logically or physically, and deemed essential to operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. 3. BES Cyber System Information – a. Break into bullet point for ease of reading as follows: "Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: ♣ security procedures developed by the responsible entity; ♣ network topology or similar diagrams; ♣ Security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports) of a BES Cyber System, Electronic Access Control System, and Physical Access Control System; ♣ BES Cyber System Impact designations; ♣ equipment layouts that contain BES Cyber System ; ♣ BES Cyber System disaster recovery plans; and BES Cyber System incident response plans." b. In the 4th bullet, we have removed of the phrase "floor plans that contain" since it is just one example of items that may contain BES Cyber System impact designations c. In the 5th bullet, we have removed the phrase "Impact designations" as protecting impact designations is now generally covered in our revised 4th bullet. 4. BES Reliability Operating Services – While we do not disagree with the details stated for each of the BES Reliability Operating Services, we do question the need for these items to be included in the NERC Glossary of Terms. Much of the same information is repeated in the CIP-002-5 Application Guidelines section. Since the only reference and use of the BES Reliability Operating Services is within CIP-002-5 we propose an alternate approach. FE proposes that the SDT 1) remove as an official defined term and 2) simply introduce the umbrella term (BES Reliability Operating Services) and the subcategories terms (Dynamic Response, Balancing Load and Generation, Controlling Frequency, etc.) in the Background section of the CIP-002-5 standard and refer to the CIP-002-5 Application Guide for more detailed information. This approach is analogous to how the terms "Associated Physical Access Control Systems, Associated Protected Cyber Assets and others are presented in the Background section of other CIP V5 standards. The BES Reliability Operating Services should only be viewed as guidance as how an entity may determine that a Cyber Asset is in fact a BES Cyber Asset (CCA). 5. Control Center – The definition, while similar to the version stated in the CCA Guideline Document (http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf) is not as succinctly written with the multiple "one or more" statements. We propose the following for the leading paragraph which is a hybrid of the two versions. "One or more facilities hosting BES Cyber Assets or BES Cyber Systems relied upon for performing any of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants and transmission substations. Functions that support Real-time operations of a Control Center include one or more of the following:" 6. Defined Physical Boundary – As stated above we propose that the PSP term be retained over DPB, however, the DPB definition should now be used. Also please add "or Monitoring Systems" after Electronic Access Control Systems. The definition should now read "The physical border surrounding locations in which Critical Cyber Assets, BES Cyber Systems, or Electronic Access or Monitoring Control Systems reside and for which access is controlled." 7. Electronic Access Points – We ask that the team add clarity around "routable" because there could be misinterpretations in the industry. The industry standard seven-layer OSI reference model defines "routable" as "Layer 3 and above". We believe this should be clear in this definition and in any guidance that discusses the term "routable". 8. Protected Cyber Asset – There is still some confusion as to how routable is defined? Please describe how "routable" should be interpreted. 9. Reportable BES Cyber Security Incident – change "Any" to "A" 10. General – Access management for vendors is a challenging area since there are occasions when immediate assistance is needed remotely from a vendor to get a malfunctioning system back to functionality. We assume that these cases are covered in the subrequirement language that includes exceptions for CIP

Exceptional Circumstances. We believe that immediate and emergency vendor support should be explicitly included in the definition for CIP Exceptional Circumstances.
Yes
General comments for CIP-002-5: 1) Purpose Statement: The purpose statement has a grammatical error and missing the word “the” in the second line between “to reliable”. We also suggest breaking the Purpose Statement into two sentences for ease of reading by adding a period after BES in the second line. 2) Applicability: 4.2.4.2 – Why is this needed? Since communication networks are now out of scope within the definition of Cyber Assets is this exemption still required? 3) Background: pg. 8 Real Time Ops: add wording to direct reader to BES Cyber Asset definition Evidence retention: 2nd sentence in opening par. should be reworded for clarity Evidence retention: How does 1st bullet fit in with entities on 6-year cycle? Attachment 1 Comments: Criteria 1.4 – We suggest adding 2.5 (a generation obligation) and removing 2.12 (not a generation obligation) Criteria 2.7 – This criteria has two embedded concepts separated by an “or” statement. During the Q&A session of the 1st NERC webinar conducted on 11/15, it appeared that the “or” is really intended to be an “and”. We suggest breaking these criteria into two bullet points for ease of reading. We propose: “Transmission Facilities operating at 200 kV or higher, but at less than 500 kV, at a single station or substation: ♣ connected to three or more transmission stations or substations; and ♣ with “total weighted aggregate value” of all BES Transmission Lines at a single station or substation operated at 200 KV or higher connected to other transmission stations or substations, including incoming and outgoing lines, exceeds a value of 3,000. The following “weight value per line” operated at the associated voltage value of a line will be used for the determination of the total weighted aggregate value.” Criteria 2.13 – The second reference to “control centers” should be capitalized to be clear it is intended to be proposed definition of Control Room (i.e. operating generation at two or more geographic locations) to avoid confusion with a control room(s) located at a single geographic generation plant location.
No
General – For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format. R1: Rational – Cyber Systems should be BES Cyber Systems 1.1 – what is meant by “intended”? for instance, what if you intended less than 6 months but it ended up being longer? We suggest replacing “intended” with “scheduled” 1.1 - also, we suggest that 30 days be extended to 60 days due to possible time needed to update the categorization
Yes
General – For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
R2 VSL - We do not believe that being late by 30 to 40 days is adequate since this a mere review of the list each year. We suggest changing the LOWER to “30 to 60 days”, then have 10 day increments for the rest of the VSL such as “60 to 70 days” for MEDIUM, “70 to 80 days” for High, and “80 to 90 days” for SEVERE.
Yes
General - For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format. We suggest removing the Applicability definitions on pages 7 and 8 since they are not used in CIP-003-5.
No
In M2, we do not agree with the 2nd example of evidence. How do you show the implementation of a policy? We suggest #2 be struck and reword the measure to “One or more documented cyber security policies that cover the ten topics specified in R2”. Also, in the guideline section in the first paragraph of page 20, the mandatory statement that says “must cover in sufficient detail” should not be in a guideline. If the team’s intent is to have certain minimum details covered in the cyber security policy, we suggest the team consider adding these minimum requirements within R2. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
Yes
For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No

1. We believe this requirement should only apply to High and Medium Impact BES Cyber Systems. Including all personnel who interface with Lower Impact BES Cyber Systems is unnecessarily burdensome with no significant reliability improvement. 2. R4 – The term “aware” is vague and our proposed revision to the requirement removes the ambiguity. We suggest a revision such that this requirement is clear that cyber security policies are made available to individuals given authorized electronic access or authorized unescorted physical access; and we suggest removal of “appropriate for their job function” since this gets into role-based training covered in CIP-004-5. We suggest that the requirement be rewritten to state - “Each Responsible Entity shall make available and accessible their CIP Cyber Security policy to individuals who have authorized electronic access or authorized unescorted physical access to BES Cyber Systems.” 3. M4 – We suggest removing the 2nd, 4th, and 5th bullets since they reference training which is outside the scope of the standard and requirement 4. We suggest that the Application Guideline include guidance for R4 since this is a challenging requirement to implement. 5. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
We suggest removing “The authority for subsequent delegations may also be delegated” since this just creates an endless loop. Also remove the 3rd bullet of M5, which is in regards to our suggested change. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
Yes
In regards to R6, the reference to footnote #2 needs to be reformatted as a superscript. For consistency with the format of the other CIP standards being proposed, we suggest the requirements be put into table format.
No
We propose that the VRF for Requirement R1 be modified to reflect a “Lower” VRF. The NERC VRF guideline document (http://www.nerc.com/files/Violation_Risk_Factors.pdf) indicates that a Lower VRF is “a requirement that is administrative in nature” and we believe this applies to R1 of CIP-003-5.
No
General CIP-004-5 comment: We suggest an addition in the applicability exception a new section: “4.2.4.5 Personnel associated with regulatory (e.g., Regional Entity, NERC or FERC) audit teams or investigations requiring access to BES Cyber System Information.”
No
2.2 - Should be eliminated. There is no way to talk about physical access controls and electronic access controls without talking about the security controls in place. This would be redundant with 2.3 and 2.4. 2.5 – We ask that the team clarify whether training on the visitor control program includes both electronic and physical access. Additional wording may be necessary in the requirement to make this explicit. 2.7 and 2.9 – We suggest switching 2.9 and 2.8 so that the requirements flow better since 2.7 and 2.9 deal with Cyber Security Incidents. 2.10 – The intended objective for item 2.10 is a bit unclear and what level of detail is required in regard to interconnectivity and interoperability. If the intent is a general “layman” understanding to the general population we can support, however, detailed training of IT staff that are knowledgeable and experienced in this area should not be the intent. FE requests that the SDT clarify this requirement.
No
R3 – The applicability includes other associated systems but R4 does not have these in the applicability. We ask the SDT to consider the need for consistency in applicability between the two. M3.1 – Measure 3.1 indicates that the date access was first granted would be evidence that may be needed for requirement 3.1. We ask that the SDT clarify in its guidance or compliance evidence retention section 1.2 as to the number of years the entity is required to retain this evidence. It should be clear that evidence is only needed for the last three years or since the last audit as stated in the evidence retention section.
No
4.4 – Add “Parts 4.1 through 4.3” at the end of the requirement 4.4 – measure should be consistent with the R5 Part 5.1 measure which allows the use of attestations from vendors and contractors
No
R5 – The applicability includes other associated systems but R4 does not have these in the

applicability 5.2 – In the measure, it is not clear the intent of “former” risk assessments. We suggest removing “former” since current assessments meets the intent of the requirement.
No
General – Access management for vendors is a challenging area since there are occasions when immediate assistance is needed remotely from a vendor to get a malfunctioning system back to functionality. We assume that these cases are covered in the subrequirement language that includes exceptions for CIP Exceptional Circumstances. We believe that immediate and emergency vendor support should be explicitly included in the definition for CIP Exceptional Circumstances. 6.1, 6.2, 6.3, 6.5, and 6.6 – the use of the term “minimum” is subjective and cannot be consistently defined across entities. We suggest replacing “the minimum” with “commensurate with what”. 6.2 and 6.3 – Remove “to verify unauthorized users do not have access” as this is not necessary for the entity to meet the requirement and it is up to the CEA to verify that the appropriate users have access. 6.1, 6.2, 6.3 - change from 'delegate' to 'delegate(s)' since it is likely that there will be more than one delegate to authorize all access.
No
7.1 - There may be times where access revocation may not be possible right away. In response to FE’s NOPR response suggesting that immediate be qualified as “as soon as possible” but not later than 24-hours, the FERC in paragraph 462 of Order 706 indicated that “the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible”. We encourage the SDT to revise requirement R7.1 to incorporate a “CIP Exceptional Circumstance” and revise the definition of CIP Exceptional Circumstance for “on the spot” terminations or resignations where the revocation may be forced to lag. Alternatively, allow for documentation of an “extenuating circumstance”, similar to 7.5, that required a lag not to exceed 24 hours for the revocation of access. The footnote should include resignations in addition to terminations consistent with 7.1. Also, footnote should be renumbered to #1. 7.2 and 7.3 – we suggest changing “next calendar day” to “next business day” due to weekends and holidays. 7.5 – We would find it very helpful if the team added some examples of “extenuating circumstances” in the guideline section of the standard.
No
R7 VSL – We believe the threshold violations are too low - it does not take into account the size of an entity and favors small entities. We believe that a percentage would be better such as up to 5% for LOWER, 10% for MEDIUM, 15% for HIGH, and 20% for SEVERE.
No
1.1 – Add “used” between “controls” and “to”. Measure 1.1 – Change “technical and procedural” to “technical or procedural”. Also, remove the last phrase “that exist and have been implemented since implementation should not be required for 1.1 since it only asks to define the controls. 1.3 – There are certain components that do not have the traditional "default Deny" platform. On these devices, an entity basically adds “deny or permit” statements as needed and their ability to get very granular for all in-bound and out-bound port specification is limited. We feel that as written this requirement would preclude existing technology from being used and cause unnecessary additional costs to replace them. We ask that the team remove the phrases “explicit inbound and outbound” from the requirements and have it worded as: “Require access permissions at each identified Electronic Access Point using routable protocols, including criteria for granting or denying those access permissions.” We believe that this change would meet the intent of the requirement. Also, to match the rewording of the requirement, we ask that the term “explicit” also be removed from the measure for 1.3. 1.4 – in general regarding TFE, will the NERC RoP’s TFE process in App. 4D be revised to be consistent with CIP V5 standards?
No
2.1 - The terms "Intermediate Device" and "directly access" are unclear. There are devices on the network between the Cyber Asset initiating Interactive Remote Access (e.g. corporate workstation) and a device within the ESP - are switches, routers, or firewalls sufficient as Intermediate Devices? In another scenario, if a proxy server authenticates the user and then grants Interactive Remote Access, is that proxy server sufficient as an Intermediate Device?. Is this considered direct access? We would appreciate it if the team clarified this language in the standard. The guideline and technical basis for R2 should include a link to the document referenced: “Guidance for Secure Interactive Remote Access”

No
The definition for Physical Access Control Systems explicitly excludes locally mounted hardware devices such as motion sensors, electronic lock control mechanisms and badge readers. However, its unclear if local panels containing programmable circuit boards would be considered part of the locally mounted hardware. Please clarify. General CIP-006-5 comments: Measure M1 statement preceding table: (grammar change) revise “Evidence must includes” to read “Evidence must include”. Table R1, Part 1.1 revise the Measure column to read “operational or procedural controls” for consistency with requirement language. Table R1, Part 1.1 revise the Measure column to strike the phrase “and have been implemented”. During the meeting it was raised that the statement is redundant with implementation wording in the M1 statement, however, it appears it may not be as the M1 statement reads “demonstrate implementation as described in the Measures column of the table.” Some were concerned that the statement “and have been implemented” raises concerns with the level of evidence required to show “implementation” of physical access controls related Low Impact BES Cyber Systems. Table R1, Part 1.2, replace “Utilize” with “Define and implement”. Table R1, Part 1.2 in the Measure column strike “and egress”. The requirement is to “restrict access” and there is no requirement expectation to track/control the egress of personnel who have unescorted physical access to Medium Impact BES Cyber Systems. Table R1, Part 1.3 in the Measure column strike “and egress”. The requirement is to “restrict access” and there is no requirement expectation to track/control the egress of personnel who have unescorted physical access to High Impact BES Cyber Systems. Table R1, Part 1.6 add the text “except during CIP Exceptional Circumstances” to the end of the requirement. FE believes a suspension of logs is warranted for the situations defined.
No
R2, part 2.1 revise the requirement to describe “visitors” as “known individuals or guests of the Responsible Entity” rather than just “individuals not authorized for unescorted physical access”. The reason for the suggested change is to alleviate any perception that a responsible entity may need to self report for this requirement in situations involving criminal theft or break-in within a Defined Physical Boundary protecting a BES Cyber System. FE suggests that the text with the parenthesis be revised to state “(individuals who are known or guests and not authorized for unescorted physical access)”
Yes
No
R1 Lower VSL, refers to Part 1.7, however, there is no part 1.7 in the requirements Table for R1. FE believes the 1.7 reference should be revised to Part 1.6. R1 High VSL, FE requests the drafting team remove the second item described in the High VSL text. The VSL describes an entity who failed to “initiate a response within 15 minutes” upon being alerted of unauthorized physical access into a Defined Physical Boundary. FE believes this VLS violates FERC Guideline 3 as stated in FERC’s June 19, 2008 Order on VLS. FERC’s Guideline 3 indicates VSLs should be consistent with the corresponding requirement and that the VSL should not expand upon requirement expectations. This portion of the High VSL refers to Part 1.6 which is related to logging physical entry into a Defined Physical Boundary. However, the VSL text does not appear to fit with any of the various rows of the requirements described in Table R1 (parts 1.1 through 1.6).
No
We suggest a change to the title of Table R1 to “Physical and Logical Ports” since “Services” is not included in requirements (part 1.1 and part 1.2) listed in the table. If “services” is brought back into the requirement for R1, we request the SDT to clarify its intent for “services”. 1.2 – We suggest a change to the requirement as follows: “Through technical or procedural controls, disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.
No
2.2 - It should be clear from the requirement that a remediation plan is not required if an entity planned on never installing a particular patch due to operational risk. If the remediation plan can state that the entity will 'have other layers of defense in place' then this should be explicitly clear and allowable in the requirement and measure. 2.3 – The requirement sentence is incomplete and we suggest the following wording: “Implement and document a process for remediation, including any

exceptions for CIP Exceptional Circumstances".
No
3.3 – We believe it should be clear in the requirement that the entity can evaluate malicious code protections for applicability and only implement the ones that apply to their specific environment. Activating every signature that gets released for an IPS device can impact the performance of the IPS and adversely impact the reliability of the BES. Furthermore, we believe that 30 days is too short of a timeframe for some entities. We suggest the following wording for 3.3: "Evaluate malicious code protections for applicability and potential adverse impact to the BES. Based on that evaluation, update applicable malicious code protections that are not expected to adversely impact the BES within 60 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns."
No
4.1 – For clarification, we suggest replacing the wording "Log generated events" with "For devices that can generate logs, log generated events…" 4.1.4 – We ask that the team add guidance and examples in the guideline and technical basis section regarding the phrase "potential malicious activity". 4.4 – In the applicability, we suggest changing "Medium Impact BES Cyber Systems at Control Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity" for consistency with the other subrequirements of R4. 4.5 – We are not sure of the justification for performing these reviews every two weeks. We suggest this time period be changed to "every calendar month".
No
5.1 – We propose deletion of this requirement as it appears to be redundant with CIP-005-5 R2.3 5.1 (Measure) – We ask the team for clarity around the use of the phrase "internal and remote paths". Is internal someone who is on the corporate network and getting into a CIP ESP and remote someone who is outside the corporate network (say on VPN)? Or is internal someone in the CIP ESP and remote is anyone on the corporate side connected into the CIP ESP via terminal servers and firewalls? 5.4 – For clarification, we suggest changing the Applicability and Requirements components of this part of R5. We suggest changing Applicability from "All Responsible Entities" to: "BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" We suggest changing the Requirements language to: "Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application. For the purposes of this requirement an inventory of Cyber Assets is not required." Without this change, it is unclear if the Requirements language may mean that such procedural controls are not needed when the cyber asset in question is, for example, a BES Cyber Asset. 5.5.2 – We suggest replacing "BES cyber system" with "BES cyber asset".
No
R2 SEVERE VSL - 1st section – We suggest changing "...did not identify a source or sources.." to "...did not identify sources...". In the 2nd section we suggest splitting these into two to make it clear; one should focus on the 30 day limit and one on not identifying. R3 HIGH VSL – The first section appears to duplicate what is stated in HIGH and suggest it be removed.
No
1.3 – We suggest removing 1.3.3 since this is covered in the proposed EOP-004-2 Event Reporting standard.
No
We suggest that 2.1 and 2.2 be switched so that the implementation comes before the incident response. 2.1 – We suggest rewording this requirement as follows: "For actual or simulated BES Cyber Security Incidents, the incident response plan(s) must be used and include recording of any deviations taken during the implementation of the plan." 2.3 – We suggest removing this subrequirement because this is dealing with retention of evidence already covered in the compliance section of the standard.
No
We believe that the Applicability of this whole standard should be to "All Responsible Entities" since it is requiring the development, implementation, and review of BES Cyber Security Incident plans. Therefore, the applicability of 3.2, 3.3, 3.4, and 3.5 should be "All Responsible Entities". 3.2 and 3.3 – We suggest the team consider moving these subrequirements under the umbrella of requirement 2

since they relate to testing and would seem to flow better in that requirement. 3.4 – We suggest changing the last phrase “that impact that plan” to “that impact the ability to execute that plan” to alleviate the burden of minor changes. Also, in many cases for large entities it may take longer than 30 days to update the plan and ask the team to consider 60 days.

No

1.3 – We suggest removing “protection” from the requirement and measure since protection of information is covered in new standard CIP-011-1. 1.4 – We suggest removal of the phrase “initially after backup” in the requirement since “ensuring the backup process completed successfully” already covers the intent. 1.5 – We suggest adding after “Preserve data” the following: “without impacting recovery efforts” to make it clear that recovery of critical information is of utmost importance and that if preserving data is possible after the recovery efforts, then 1.5 would apply. We therefore also ask that “where technically feasible” be removed. Lastly, we suggest the removal of “before proceeding with recovery” in the measure. Our suggestions align with FERC Order 706 Par. 708 in which FERC said in part “…recovery of critical cyber assets and the Bulk-Power System is of immediate critical importance, and information collection efforts should not impede or restrict system restoration.” General comments not specific to R1: ♣ We question why some of the subparts of the requirements in CIP-009-5 include “at Control Centers” in the applicability while others do not. For example, what would be the purpose of having a recovery plan per R1 for all Medium impact assets, but not require it to be implemented in R2. We ask the team to assure the applicabilities in CIP-009-5 are appropriate and consistent with the requirements. ♣ We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements. ♣ Purpose statement – we suggest the removal of the phrase “related to the storing of backup information” from the purpose. We believe this constrains the purpose of this standard since some information is not necessarily stored but continually changed and recovered. ♣ The headings in the columns on page 11 of 23 need to be adjusted as they all say “Part”. ♣ We ask that the guideline and technical basis section include the text of the referenced FAQs and CIPC guideline. ♣ We suggest the “Purpose” statement of the standard be changed. We suggest replacing '…plans(s) related to the storing of backup information are put in place for BES Cyber assets…' with '… plan(s) are in place for BES Cyber Assets…' ♣ We ask that the team attempt to make it clear in the standard on the use of the terms “recovery” versus “restoration”. In the “Disaster Recovery” world those have very different meanings and are not interchangeable.

No

2.1 – In the third bullet of the requirement, we suggest removing the term “full” and just use the phrase “with an operational exercise” in both the requirement and the measure. Incidents that occur usually only affect a portion of the system and only a portion of the recovery plan will be implemented. For example, testing 'failover' or 'restore-from-backup' of a small number of key EMS servers would be examples of partial exercises compared to a full test of all 100+ EMS servers all at one time (which is not possible for an entity without affecting the BES). 2.2 – We suggest removing the second word “any” and re-wording the phrase “backup media initially”. We suggest a rewording of the requirement as follows: “Test information used in the recovery of BES Cyber Systems that is stored on backup media (1) to ensure it is operational before use and (2) at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is still useable and reflects current configurations.” 2.3 – For consistency with other requirements and measures that mention periodic activities, we suggest changing the phrase “at least once every 39 calendar months” to “every 3 calendar years not to exceed 42 calendar months” in both the requirement and measure.

No

3.2 and 3.3 – We suggest combining these subrequirements into one subrequirement and allow 60 days for the review and update of the plan. We suggest the following wording for the new combined requirement: “Within 60 days of a test or actual incident, review the results of the recovery, document any deficiencies or lessons learned, and update the recovery plan based on any documented deficiencies or lessons learned.” 3.5 – The use of 'each' implies that we must prove that each person actually reviewed the updates. Suggest removing 'all' and 'each'.

No

General – Correct typo in first sentence of guideline and technical bases for R3; “note” instead of “not”. 1.1 – In 1.1.4, we suggest adding the word “installed” between “Any custom”. 1.1 (Applicability) – We suggest the removal of “Associated Protected Cyber Assets”. These are non-critical devices that happen to be in the ESP and believe the need to track the baseline configuration for these devices does not add any reliability benefit. 1.1.2 – In the guideline and technical basis section, we ask the team to add clarification with regard to “version” and the level of detail needed. And what is the expectation of applicability for appliances (e.g. HMCs) or for application ports (e.g. TCP/IP ports) where OS is not clearly defined like a Windows server? 1.1.3 – We are not clear as to the reason for the term “intentionally” and suggest it be removed. 1.2 – We suggest replacing the first phrase of the requirement “Authorization, by a CIP Senior Manager or delegate, and document” with “Document approved”. We believe it would be cumbersome and do not believe it is necessary to have the CIP manager or delegate in this requirement. From an overall policy standpoint per CIP-003-5 R5, this authorization and delegation is already covered in the “Configuration Change Management” portion of the cyber security policy. 1.3 – We suggest the removal of the phrase “and other documentation required by a NERC CIP Standard, including identification and categorization”. This phrase should be removed because this is adequately covered in other standards and may cause double jeopardy as a result. For example, identification and categorization of BES Cyber Systems changes is covered by CIP-002-5 R1 part 1.1. 1.4 – In 1.4.2, we suggest replacing the phrase “these required controls” with “the required cyber security controls” for consistency with the rest of the requirements in 1.4. 1.5 – We suggest striking the phrase “for Control Centers”. This is already captured in the High Impact BES Cyber System applicability since all High Impact systems are at control centers per Att. 1 of CIP-002-5.

No

2.1 – We suggest replacing “monitor for” with the phrase “utilize automated monitoring of”. This will align with the intent of the requirement as stated in the guideline section of the standard which says “the intent of R2 is to require automated monitoring of the BES Cyber System.”

No

3.1 and 3.2 - We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements. 3.3 – We suggest this requirement be made more specific as to when a modification requires an assessment. A broad requirement for an assessment for each and every modification is burdensome with no added reliability benefit for many of the modifications. FERC, in par. 547 of Order 706 made this clear and provided examples as follows: “…we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment. For example, we would anticipate that updating an attack signature file on the electronic access point would not require an active vulnerability assessment, but replacing the devices that comprise the electronic access point would require an active vulnerability assessment.” 3.3 – If our suggestion above for completely removing requirement 3.3 is not accepted, we suggest removing “Associated Electronic Access Control and Monitoring Systems” from the applicability for consistency with 3.2. Otherwise we would like clarification on the reasons for the difference.

We suggest adding references to the subrequirements for each VSL explanation in the Table of Compliance Elements.

No

Part 1.1 of Table R1, we suggest adding the words “evaluate and” between “to identify” so that the requirement reads “One or more methods to evaluate and identify BES cyber system information.” The proposed change is to better clarify the intent of the requirement. Part 1.1 of Table R1. The second bullet in the measure should not be included in this standard. The referenced training materials are covered in CIP-004, R2 Part 2.6 and not pertinent as a measure to this CIP-011 requirement. Heading of page 11 and 12 should be Part, Applicability, Requirements and Measures from left to right. Part 1.2 of Table R1, strike “procedures for” and replace with “of” in requirement to read, “Access control and handling of BES Cyber System Information”. The change is proposed to avoid any potential inadvertent interpretation that the requirement is merely assessing a documented procedure. The introductory R1 statement sufficiently covers implementation of a documented process. Part 1.2 of Table R1, add in Measures bullet 1 “BES Cyber System” and strike “in a manner” to read “Records indicating BES Cyber System Information that is stored, transported, and disposed

consistent with the documented process; Part 1.2 of Table R1, strike from Measures bullet 2 “with user access implemented on a need to know basis” to read “Records from an information management system containing electronic copies of BES Cyber System Information”. The text proposed for removal is not pertinent as a measure to this CIP-011 requirement and covered in CIP-004, R6. Part 1.2 of Table R1, add in Measures bullet 3 “BES Cyber System” and strike “with keys provided to only authorized individuals” to read “Hardcopies of BES Cyber System Information stored in a locked file cabinet”. The text proposed for removal is not pertinent as a measure to this CIP-011 requirement and covered in CIP-004, R6.Part 1.3 of Table R1, Strike the phrase “Initially upon the effective date” and the word “thereafter” so the revised requirement reads “At least once every calendar year, not to exceed 15 months between assessments …”. 1.3 – We suggest replacing “implement an action plan” with “initiate an action plan”. An action plan may take more than a year to complete and the requirement could be interpreted as requiring it to be completed annually. 1.3 - We suggest the removal of the phrase “initially upon the effective date of the standard and” because if the team intends for certain activities and requirements be completed by some date, then this should be clearly stated in the CIP Version 5 implementation plan and is not appropriate in the requirements.

No

General – We believe it would be helpful if the team added guidance or explicit language in the requirements with respect to media that is still in use but then the location becomes it is used in becomes “CIP-declassified”. Footnote “2” – We suggest that it would be more enforceable and mandatory if BES Cyber Asset Media was defined as stated in the footnote and be added to the NERC glossary of terms. 2.1 – We suggest changing the first part of the requirement “Prior to the release for reuse of BES Cyber Asset media…” to “Prior to redeployment of BES Cyber Asset Media outside the Electronic Access Perimeter…”. The ESP concept exists in the current wording of this requirement in CIP-007-3 R7.2 and therefore should be carried over into the proposed 2.1.

No

R1 VSL – The use of the term “periodically” in the HIGH VSL is not used within requirement R1 and should be removed. R2 VSL – We ask that the drafting team write the severity levels to be more granular with respect to the type of device being disposed. For example, it seems that not properly wiping a flash drive is not the same severity as not wiping a firewall.

No

We support the proposal to retain V3 while transitioning to V5 if the collective industry (Entities, NERC and FERC) achieve a timely approval of V5 prior to V4 becoming effective. However, the 18 month timeframe does not allow sufficient time to complete capital budget cycles and we suggest a 24 month implementation. Lastly, the SDT should consider a staggered implementation plan that would allow for focus on the high impact and medium impact items first, and then followed by the low impact items. This would ensure proper focus and attention is given to the more important items for BES reliability without distraction and attention being diverted to lower cyber asset issues. Lastly, references within periodic requirements that indicate “initially upon the effective date of the standard” should be moved into the Implementation Plan and removed from requirement language. This ensures clear prerequisite expectations upon the initial effective date of the standards and allows for more concise and clear requirement language.

Group

NERC Standards Review Subcommittee - ERCOT Region

Andrew Gallo, Chair

Yes

The definition of “BES Cyber System Information” should include only floor plans, diagrams, equipment layouts, etc. that clearly delineate the cyber assets in some way. In other words, if the diagram denotes a device as a “Schweitzer” relay (or even an “SEL 2030”), the information should not require special treatment. Refer to additional comments submitted for Question 49. The SDT should also re-think including data in the definition of Cyber Assets. Additionally, “suspicious” is not an auditable term and ought to be removed. The same is true for “attempt.” It is not clear which “attempts” justify reporting. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. BES Cyber Security Incident: A malicious act that: •Compromises a BES Cyber System or BES Cyber Asset, or •Disrupts the operation of a BES Cyber System or BES Cyber Asset, or •Results in unauthorized physical access into

a Defined Physical Boundary. BES Reliability Operating Services: we note the following: •"Identify and monitor flow gates" under "Managing Constraints" seems to be missing its bullet •We recommend clarifying that the use of the word "Facility" means the NERC Glossary definition -- in "facility operational data and status" under "Inter-Entity Real-Time Coordination and "Communication" •Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" •For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret. CIP Exceptional Circumstance: We request revision to "A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability." The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. CIP Senior Manager: Replace "NERC CIP Standards" with "NERC CIP-002 – CIP-011 Standards" because CIP-001 is not part of this set of standards. Control Center: We are concerned with the broadness of this definition. The SDT should consider the impact on small entities that will be affected by a broad definition of Control Center. In the proposed definition, the SDT uses the defined term "System Operator" which is "An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time." If the SDT's intent was to limit Control Centers to BA, TOP, GOP and RC functions, we support the definition and request that the SDT make this limitation clear in the definition or in guidance. Intermediate Device: Recommended changes: "A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network." Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Yes

Attachment 1, Section 2.13 assigns a Medium Impact to "generation control centers that control 300 MW or more of generation." Control Center is a NERC-defined term; however, because "control center" is not capitalized in 2.13, it creates confusion because it could be interpreted that a typical control room of a combined cycle unit could be construed as a "control center" by the Regional Entity. The SDT should capitalize the term in 2.13 to make it clearer. We recommend adding a threshold for BAs similar to CIP-002-4. Change to "Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12." We do not agree with the inclusion of all Transmission Owner (TO) control centers. These may include local distribution "dispatch rooms" with visualization capability and minimal control of BES Facilities. We recommend removing "TO" from Attachment 1, 1.4 and 2.13. Alternatively, if TOs must be included, we recommend using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" (i.e. Replace "Transmission Owner" with "Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator"). The addition of a "Low Impact" rating for every generation facility that does not meet the High or Medium Impact thresholds constitutes a significant change in the CIP Standards. This change forces every registered GO and GOP to adhere to approximately 40 requirements in the remaining CIP standards when, currently, those generators are not listed as Critical Assets. It seems unlikely that the cost to adapt existing corporate cyber security policies, cyber security awareness and cyber asset access management to these NERC CIP requirements will lead to a corresponding reliability benefit. In addition, Regional Entity audit resources would be better served if allowed to focus on more critical locations. We recommend this category be eliminated. Criterion 2.7 seems to have been modified to include some transmission substations operating at 200kV to 300kV. The present Version 4 bright-line criterion includes only those operating above 300kV. Because this includes substations interconnected to generators, it seems likely that 200kV substations newly

identified as “Medium Impact” could include some generation facilities as well. This would require a whole new level of regulatory compliance to facilities not included under the Version 4 Standards. There is no reason to believe the Version 5 criterion better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal? In 2.12, “system” and “Facility” are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned.
No
For clarity, we request changing R1.1 from “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation” to “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation.” For clarity and consistency with the previous suggested change, request changing M1 from “as required in R1 and list of changes to the BES)” to “as required in R1 and list of changes to the BES Elements and Facilities)”. The word “intended” should not be used in the requirement because it is not auditable. Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Part 4 needs clarification. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementing CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion framework. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. The SDT should consider an approach that would have documentation “requirements” in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is too complicated. In addition to the BES Cyber Assets classified as high, medium and low in CIP-002, the other standards introduce ten additional categories of assets to protect in various ways: •Associated Physical Access Control Systems •Associated Protected Cyber Assets •Associated Electronic Access Control or Monitoring Systems •Electronic Access Points (with External Routable Connectivity) •Electronic Access Points (with dial-up connectivity) •Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries •Transient Cyber Assets •Medium Impact BES Cyber Systems with External Routable Connectivity •Medium Impact BES Cyber Systems at Control Centers •Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some appear in the standards themselves and these categories may or may not be included in the definitions document. This approach is complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future interpretations, CANs, etc. The Standards should be revised so that CIP-002 defines all assets needing protection rather than being introduced throughout the Standards. We recommend replacing “30 calendar days” with “90 calendar days.”
Yes
Recommend adding the following: “…has had its CIP Senior Manager or delegate review and update…”
No
The SDT should re-think the use of a “CIP Senior Manager.” In many organizations, there will not be one senior manager responsible for implementing the CIP Standards. For example, in some organizations, SCADA/EMS and Relay personnel report to one senior manager, but I.T., Security and H.R. personnel report to a difference senior manager (or managers). Yet, the SCADA/EMS, Relay, I.T., Security and H.R. all have roles in CIP compliance. A better approach would be for the Standards to require that a Senior Manager be designated for each Standard (or requirement), but it need not necessarily be the same Senior Manager for each Standard (or requirement).
Yes
Request clarification of the meaning of “implement” M2.2.

Yes
“Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Please see our comments in response to Question 6, above.
Yes
We recommend changing “30 calendar days” to “90 calendar days.” The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
Yes
Providing Security Awareness is useful and should remain in the Standard. However, the SDT should re-think the need to have a Security Awareness Program. So long as the Registered Entity provides security awareness quarterly, the program adds no value and is merely another “compliance document” to maintain, review, update, etc.
Yes
Most of the requirements in R2 make sense. However, providing training on “physical access controls” is not necessary. The physical access controls are – generally – pretty straightforward (e.g. card key readers). It does not seem necessary to provide “training” on how to use a card key. The same can be said for training on electronic access controls. Most of those access controls merely involve two-factor authentication or something similar. The need to provide “training” on how to log on to devices is unnecessary. We recommend removal of R2.3 and R2.4 because they appear redundant to R2.2; alternatively, some explanation of the difference between R2.2 and R2.3/R2.4 should be provided. With respect to R2.8, it seems unnecessary to require training on recovery plans except for those very few employees who must implement the recovery plan. As currently worded, it is not clear whether only those who implement recovery plans must receive training. With respect to R2.10, it seems unnecessary to require training on the systems’ electronic interconnectivity and interoperability with other cyber assets. Generally, the personnel doing the “care and feeding” of those assets already know how they work and how they interconnect and interoperate. The personnel using those devices have no need to know about the interconnectivity and interoperability of the assets. Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement.
Yes
Yes
For all R4 table entries, we recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2, we recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of the CIP Standards. The additional language should spell out when this “grandfathering” expires (which will be when a new check is required).
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
The CIP Senior Manager should not necessarily have a role in R6.1, R6.2 and R6.3. There should,

instead, be a particular person designated as the “gate keeper” for each cyber asset and physical security area. For example, the SCADA/EMS manager is the logical person to grant access to the SCADA/EMS system, not necessarily the “CIP Senior Manager.” [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to a “gate keeper.” However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just create the “gate keeper” concept.] The Registered Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. In R6.1, we recommend changing “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except.” Also, change “minimum necessary” to “minimum the responsible entity considers necessary.” In R6.2, 6.3, 6.5 and 6.6, change “minimum necessary” to “minimum the responsible entity considers necessary.” For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For 6.6, we request clarification of whether variances noted in the verification would be required to be a self report. In the measure for R6.6, change “BES Cyber System information” to “BES Cyber System Information.”
No
In Part 7.1, the use of “at the time” of the resignation or termination is vague and ambiguous. For example, if a person informs the utility that his/her resignation is effective in three weeks, must the utility revoke access when informed of the resignation or when the resignation becomes effective? We recommend making the requirement seven days. We recommend moving the text in the footnote for 7.1 into the requirement. For Part 7.2, we recommend requiring only that the revocation occur as part of the next quarterly review. Those personnel have merely been reassigned or transferred. They do not pose a risk to the BES (as opposed to, for example, an involuntarily terminated employee). It makes sense that people deemed to be a risk (i.e. those terminated for cause) should have a very short timeframe for revocation. However, for people in good standing who are transferred or reassigned, the time frame has gone down from a seven-day permissible time frame to a single day. This seems an unnecessary burden that will cause utilities to incur costs needlessly (i.e., overtime pay to do revocations on Saturdays, as most people who resign or get reassigned or transferred would likely do so effective end of business Friday). Again, these costs and obligations seem reasonable for terminations for cause, but hard to justify for employees in good standing. Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the calendar quarter in which the resignation/termination occurs.” For Part 7.4, revoking a person’s overall access to cyber systems should suffice. In other words, if a person must be on your corporate network in order to gain access to critical cyber systems, revoking overall network access should suffice to meet the Standard (as opposed to revoking the person’s access to the various individual systems). If this language remains, we believe it should be revised as follows: “For resignations or terminations, revoke the individual’s user accounts on BES Cyber Assets (unless already revoked in accordance with R7.1 or 7.3) within ninety (90) calendar days of the date of initial access revocation.”
No
There should be a “lower” and “moderate” VSL for R1 through R3 (e.g. For R1, a “lower” VSL could be if awareness reinforcement was done only two times in a year; a “moderate” VSL could be if awareness reinforcement was done only three times in a year). For R5, we recommend the following language: “Personnel risk assessments are not updated at least once every seven years. (5.2)” Also for R5, the “severe” VSL contains the following language: “The Responsible Entity did not have a documented process for personnel risk assessments.” Failure to have a documented process for PRAs should not involve a severe VSL. The important question is whether PRAs are being performed; not if there’s a documented process for performing them. In other words, if a utility can demonstrate it is performing PRAs (correctly and timely), it should not matter whether the utility has a documented process to perform PRAs.
Yes
For R1 there is an issue of auditability regarding Low Impact BES Cyber Assets. If an entity need not create a list under CIP-002, there is no way to ensure the technical and procedural controls have been applied. Request clarification for when Low Impact BES Cyber Systems are in the ESP with High/Medium BES Cyber Systems. Are such Low Impact BES Cyber Systems subject to 1.1 or 1.2? There is also some disagreement over the VRFs for this Standard. Currently, the VRF is set at Medium. For part 1.1, that VRF should not be Medium but should instead have its own VRF of “Low.” We propose the following wording change to Table R1, Part 1.1: Requirement: An Electronic Security

Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access. Measure: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. The Measures language proposed is similar to CIP-004-5 R1. We believe the use of the word “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
We recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset" to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset" because, as written, the requirement does not allow for the development of new technology. We recommend changing the Measure for R2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors."
Yes
We request clarification of Part 1.1’s Applicability because it does not identify which of High/Medium/Low BES Impact the Physical Access Control Systems are "Associated" with. We request Requirement 1.2 be updated to allow "escorted physical access." We propose the following wording change to Table R1 Part 1.1: Requirement: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measure: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. The Measure language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
Yes
Requirement 2.2 requires clarification. If the intent is to require that visitors sign-in once each day, the draft language does not clearly set forth that requirement. As currently written, the language could be interpreted to require entry/exit logs “on a per 24-hour basis.” Such an interpretation would mean a Registered Entity would have to retain a great deal of paper (where logs are maintained on paper). This is especially true for an entity on a six-year audit cycle (which will have to maintain 2,190 individual daily logs for each facility). Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis,”.
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
No
Request clarification on R1.1. is this at the BES Cyber System level or at the Asset level or can the

Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
Yes
We request clarification of Part 2.2 because it requires creation of a “remediation plan.” However, if the entity applies the patch, no remediation plan should be necessary. We suggest wording similar to the following: "create a remediation plan or a plan to mitigate the vulnerability if the Responsible Entity opts to not apply a patch or update." What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
Yes
The Standard should make an allowance in Part 3.3 for signature/pattern updates that create system problems/issues. In the Requirement for Part 3.4, the words, “…Transient Cyber Assets and removable media….” should read, “…Transient Cyber Assets or removable media….”
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Please clarify the Requirement for Part 4.3. Does it require that the failure be detected within a calendar day or that a response be implemented within a calendar day of a failure being detected? The Requirement in Part 4.5 for log reviews every two weeks is too frequent. We recommend monthly reviews (which is still more frequent than the 90-day reviews in the previous version of the Standards).
Yes
In Part 5.2, the CIP Senior Manager or delegate should not have to authorize the use of administrator, shared, default, and other generic account types. The “owner” of the asset (e.g. the SCADA/EMS manager) should be able to authorize the use of such accounts. [We realize that, under the Standard, the CIP Sr. Mgr. can delegate the responsibility to someone else. However, doing so simply creates another document (the delegation) to maintain, review, revise, etc. It makes more sense to just let the asset owner authorize the use.] Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
Yes
Yes
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
Yes
In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. We believe these times should coordinate with the plan in EOP-004-2 which allows 90 calendar days for update of the plan. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing up Information essential to BES Cyber System recovery, verify the media to ensure that the backup

process was successful.”
No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported.
No
For Part 3.1, we recommend “and document any identified deficiencies or lessons learned” as that topic is addressed in CIP-009 R3.2. In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. We believe these times should be consistent with CIP-008-5 updates and, as stated in our response to Question 36, should be changed to 90 calendar days for update of the plan. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
No
This requirement will be very difficult to meet and will require many technical feasibility exceptions. We suggest the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems outweigh the cyber security benefit.
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
Yes
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it

very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered.
Yes
Footnote 2 in 2.1 should be moved into the body of the Requirement.
No
Overall comment to all proposed Standards: I.Black Start Issues There are several black start-related issues. First, in the current version of the Standards, a Registered Entity can have Critical Assets with no Critical Cyber Assets (CCAs). So, for example, a company may have black start units (i.e. Critical Assets) which have no associated cyber assets that use a routable protocol. As such, those black start units can be Critical Assets with no CCAs. As a result, the Registered Entity would not have to meet the NERC CIP requirements for the black start units. The same concept does not exist in the Version 5 Standards. In the Version 5 Standards, black start units will require CIP protections. That fact could have a chilling effect on entities. In other words, some entities may not bid their units into black start service because, by doing so, they would have to incur the expense of becoming NERC CIP compliant. In the ERCOT Region, black start service is not very lucrative and, therefore, some companies may refrain from bidding into black start service due to the expenses associated with being NERC CIP compliant (plus the fear of potential fines down the road). Additionally, many Blackstart units in the ERCOT Region are older, smaller units with very low capacity factors and limited revenue. Applying the “Medium Impact” CIP requirements on those units will result in the need for significant CIP investment and increased on-going operational costs as well as increased compliance risks. This may result in Generator Owners/Generator Operators not offering units for Blackstart service. It would also likely result in Blackstart units not being maintained in a manner appropriate to support Blackstart service because of the additional on-going cost, thus removing them as a future option for providing Blackstart service. With fewer units offered for Blackstart service, ERCOT may not have enough Blackstart Resources to effectively restore the ERCOT BES after a complete or partial system blackout event. We believe a Blackstart unit with no External Connectivity poses little or no risk to the BES and should be classified as Low Impact. We recommend the following modification to CIP-002-5, Attachment 1, to ensure the continued reliability of the ERCOT portion of the BES: “2.4. Each Blackstart Resource with External Connectivity identified in its Transmission Operator's restoration plan.” Blackstart Resources with External Connectivity would remain in the “Medium Impact” category; however, Blackstart Resources without External Connectivity would move to the “Low Impact” category. The Blackstart Resources in the Low Impact category would have the appropriate physical and cyber protection controls as listed in the current CIP Version 5 draft standard. Our understanding of CIP Version 5 draft standards is that External Connectivity is defined as having Routable or Dial-up connections through an Electronic Access Point. Another concern focuses on facilities downstream of the black start unit. For example, one company could be chosen to provide black start service from a generator, but a different company owns/operates the facilities along the cranking path. If that were the case, the transmission company would now have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. The same is true for facilities associated with the next-start unit. If the switch yard for the next-start unit is owned/operated by a company other than the one that won the black start bid, that next-start company may have to incur the cost of becoming CIP compliant even though it is not compensated for those expenses. Another question involves whether units that are black start capable must be NERC CIP compliant regardless of whether they are in the black start restoration plan. The reliability of the ERCOT system may be adversely impacted because units that have been updated to meet the NERC CIP Standards but not selected for Black Start service could be forced into mothball or retirement due to economics associated with maintaining NERC CIP compliance. Many such units are small, have small staffs and low capacity factors, do not run much during the year and may be running on the margin. If companies are reluctant to bid into the black start market due to the costs associated with being NERC CIP compliant, it could result in inadequate black start capability due to Generation Owners not bidding units into the black start market. Finally, we request clarity on the inclusion of “next start units” in the black start path. As CIP-002 currently reads, it could be interpreted that they are not included in the black start path; consequently, clarification is in order. II.Other Issues •We recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will

make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. •We request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. •We request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5.
Individual
Nathan Mitchell
American Public Power Association
Yes
BES Cyber System Change: Replace Maintenance Cyber Asset with Transient Cyber Asset Justification: Maintenance Cyber Asset is not defined. BES Cyber System Information Change: Define “BES Cyber System Impact” Justification: It is assumed when the SDT uses the capitalized BES Cyber System Impact it is referring to CIP-002—5 Attachment 1 “Impact Categorization of BES Cyber Assets and BES Cyber Systems.” The SDT needs to make this clear in a BES Cyber System Impact definition. CIP Senior Manager Change: Replace: “NERC CIP Standards” with “NERC CIP-002 – CIP-011 Standards” Justification: CIP-001 Reliability Standard is not part of this set of standards and has not been approved for inclusion in EOP-004-2. This will give clarity to the limit of the definition. Control Center Proposed Definition:”One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:” Comment: APPA is concerned with the broadness of this definition. The SDT should consider the impact on small entities. Many dispatch centers or control rooms will be drawn into compliance by an overly broad definition of Control Center. In this definition the SDT uses the defined term: System Operators which from the glossary is: “An individual at a control center (Balancing Authority, Transmission Operator, Generator Operator, Reliability Coordinator) whose responsibility it is to monitor and control that electric system in real time.” If the SDT’s intent was to limit Control Centers to buildings that house a System Operator with 24/7 staffing and include BA, TOP, GOP and RC functions, then APPA supports the definition and requests that the SDT make this limitation clear in the definition or in guidance. If this is not the intent of the SDT then APPA does not support the broader definition of Control Center. APPA points the SDT to our comments in Question 2 on CIP-002-5 Attachment 1 which conflicts with this limited scope of Control Center where 1.3 and 2.13 of Attachment 1 include TO control centers in the High and Medium Impact Rating. APPA is also concerned with the use of the term “facility” in the definition due to the fact that a generator control room may control multiple generators on the same site. This control room could be interpreted to be a Control Center if the current definition is approved. Therefore, APPA supports the comments of the Florida Municipal Power Agency (FMPA) on replacing the term “facility” with the term “site” to provide clarity that a Control Center controls generators or transmission substations at multiple locations. APPA recommended definition: “Control Center: One or more sites used for real-time operations by System Operators on a 24/7 basis to perform the Functional obligations of the RC, BA, TOP or GOP. These sites also host a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions for two or more BES generation facilities or transmission facilities, at two or more locations: (Continue with bullets in proposed definition) Reportable BES Cyber Security Incident Comment: APPA is concerned with the conflict between CIP V5 Reportable BES Cyber Security Incident and EOP-004-2 Reporting of Cyber Security Incidents. The SDT should coordinate with EOP-004-2 SDT to make sure there is no overlap of standards.
Yes
4. Applicability 4.1.2 Distribution Provider 4.1.6 Load-Serving Entity Comment: APPA is concerned with the new inclusion of DPs in the version 5 standards and with the qualifiers proposed for LSE in the Applicability section. APPA believes that this inclusion of this broad group of entities will draw in small entities with no operational capabilities and cause them to go through a paperwork drill of proving they either do not provide BES Reliability Operating Services or they do not have cyber assets associated with this equipment. APPA recommends that the SDT develop a simple method for DPs and LSEs to prove “No Impact – owning no BES Cyber Assets or BES Cyber Systems” therefore are clearly exempt from CIP-002-5 – CIP-009-5 and CIP-010-1 – CIP-011-1. APPA points to the comments of the Florida Municipal Power Agency (FMPA) which describes a “De Minimus Impact” category as an exclusion alternative. The SDT should discuss these alternatives as a way to address the burden on

small entities. Attachment 1 1. High Impact Rating 1.2 BA Control Centers Change: Add Threshold for BAs similar to CIP-002-4. Change to “Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority that includes control of two or more of the assets identified in criteria 2.1, 2.3, 2.4, 2.12” Justification: Some small BAs do not control multiple assets and designating all BAs would be burdensome to small entities. 1.3 TO/TOP Control Centers Change: Removal of Transmission Owner or Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator” Justification: APPA members are in strong opposition to the inclusion of "ALL" Transmission Owners (TO) control centers. These may include local distribution "dispatch rooms" that have visualization capability and minimal control of BES Facilities. APPA recommends the removal of TO from Attachment 1, 1.3 and 2.13 If TOs must be included APPA recommends using the qualifier similar to what the SDT drafted in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)." 2.13 TO/TOP Control Centers not included in High Impact Rating Change: Removal of Transmission Owner, or Replace “Transmission Owner” with “Transmission Owner, assigned by agreement, the functional obligation of a Transmission Operator” Justification: APPA members are in strong opposition to the inclusion of "ALL" Transmission Owners (TO) control centers. These may include local distribution "dispatch rooms" that have visualization capability and minimal control of BES Facilities. APPA recommends the removal of TO from Attachment 1, 1.3 and 2.13 If TOs must be included APPA recommends the qualifier given in the guidance: "agreements where some of the functional obligations of a Transmission Operator [are] delegated to a Transmission Owner (TO)" Change: Add to 2.13: (3) Balancing Authority control centers that control 300 MW or more of generation. Justification: If the SDT accepts the change proposed by APPA in 1.2 above, limiting the High Impact BA control centers then those not included in the High Impact Rating, but control more than 300 MW of generation should be included in 2.13. This will limit the burden on small BAs that do not control major flows in an interconnect. APPA points to the comments submitted by AECI and NRECA, which propose an additional criteria that will include Control Centers that “do not use protected data connections.” This proposed approach should be discussed by the SDT as an option for addressing the 706 directives, and reducing the burden on small BAs.
No
Requirement R1, 1.1 of CIP-002-5 Change: Replace “30 calendar days” with “90 calendar days” Justification: The SDT uses a number of different calendar days for reporting throughout the CIP standards. APPA recommends one consistent time of 90 calendar days.
Yes
No
R1 VRF/VSL Comment: APPA is concerned that a Responsible Entity will need to produce a list of Low Impact BES Cyber Assets to prove they have not “incorrectly categorized BES Cyber Assets at a lower category.”
Yes
Yes
Yes
No
Change: In Measure M4 second bullet: Replace: “Documented records that policies have been provided to contractors where access to BES Cyber Systems is authorized” with: “Policies are accessible to contractors when access to BES Cyber Systems is authorized.” Justification: This Measurement imposes a documentation and records retention burden, which is above and beyond the cyber security benefits to compliance. APPA suggests the above change so contractors have the same access to the policies, but the responsible entity does not have to prove they have given each contractor (individual) a copy of the policy. Change: In Measure M4 fifth bullet: Add: “Training is not required in R4, but would be acceptable evidence of compliance” Justification: APPA suggests the above qualifier to M4 fifth bullet since the measure implies the need for training, when the requirement specifies only awareness.

Yes
No
Comment: APPA recommends changing “30 calendar days” to “90 calendar days” to be consistent throughout the CIP standards.
Yes
Yes
Comment: APPA agrees with this programmatic approach to a culture of cyber security requiring all Responsible Entities to have a Security Awareness Program.
Yes
Yes
Yes
Yes
Yes
No
R7 Access Revocation Change: Replace “by the end of the next calendar day” with “within 30 days.” Justification: APPA believes that the Requirement in Table7 Part 7.2 for “reassignments or transfers” is extreme compared to the threat of cyber attack on the system by someone being transferred or reassigned for reasons other than disciplinary action. Even the SDT in their Change Rationale stated an objective; “to prevent a person from accumulating unnecessary authorizations through transfers.” This is not a threat to BES reliability it is only a cleanup activity and Responsible Entities should be allowed more than one calendar day to complete and show compliance. APPA suggests 30 days which is consistent with Part 7.5.
Yes
No
Electronic Security Perimeter Comment: APPA agrees with the SDT comments in their Change Description and Justification calling for “Entities are to document perimeter type security controls”. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by an Electronic Security Perimeter Procedure will improve cyber security. However, APPA does not see this same programmatic approach in the Requirement and Measures in Table R1 Part 1.1. Therefore, APPA proposes the following wording change to Table R1 Part 1.1: Requirements: An Electronic Security Perimeter Procedure that defines operational or procedural controls to restrict unauthorized access. Measures: Evidence may include, but is not limited to, an Electronic Security Perimeter Procedure that describes the operational or procedural controls and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to provide a listing of Low Impact BES Cyber Systems and proof of protection on each individual device. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets.
Yes
Yes

No
R1. Physical Security Plan Comment: APPA agrees with the SDT comments in their Change Description and Justification calling for “programmatic protection controls as a baseline”. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by a Physical Security Plan will improve cyber security. However, APPA does not see this same programmatic approach in the Requirement and Measures in Table R1 Part 1.1. Therefore, APPA proposes the following wording change to Table R1 Part 1.1: Requirements: A Physical Security Plan that defines operational or procedural controls to restrict physical access. Measures: Evidence may include, but is not limited to, a Physical Security Plan that describes the operational or procedural controls and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the plan. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel the use of the term “implemented” without further description may be interpreted to mean a Responsible Entity will need to show how each Low Impact BES Cyber Asset is physically protected. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. Comment: Table R1 Part 1.2, In the Requirement it specifically states that a Responsible Entity should “restrict access.” APPA interprets this as meaning to allow only authorized individuals into (ingress) the restricted areas. However, the Measures states both “ingress and egress is controlled.” Cyber security is not enhanced by logging out (egress) authorized personnel. APPA recommends removal of the word “egress” from the Measures and the SDT should give guidance that ingress logging is all that is required for compliance. Additional Requirement: APPA recommends the addition of a requirement in R1 that addresses the issue of Physical Access logs similar to the requirement in CIP-007 R4.4 for Cyber System event logs. APPA Proposed Requirement: Retain BES Physical Access Ingress logs identified in R1.6 for at least the last 90 consecutive calendar days. Justification: APPA is concerned with the need to retain 3 years of logs as proof of compliance, when current standard language and audit practice is for entities to show a process requiring retention of logs and showing the auditor that entities have the current 90 days of logs at a minimum.
Yes
Yes
Yes
Yes
No
R2: Security Patch Management Comment: In Table R2, Part 2.2 the Requirements state “create a remediation plan or revise an existing remediation plan.” APPA believes the term "remediation" should be changed to "mitigation or compensatory measures", since remediation implies that a patch or update is required to be applied. In some cases it may be known through testing that a particular patch interferes with the operation of the system. Applying a patch in these cases may reduce reliability.
Yes
R4: Security Event Monitoring Comment: In Table R, Part 4.2 the Requirement states; “Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert.” APPA feels this is a fill in the blank requirement that Registered Entities will need guidance on developing a threshold for generating alerts. Question: In Table R4, Part 4.3 was it the intent of the SDT to require duplicate logging capability with the statement; “Detect and activate a response to event logging failures?”
No
R5: System Access Controls Comment: APPA points out to the SDT when requirements are applicable to All Responsible Entities including Low Impact BES Cyber Systems these requirements must address “programmatic protection controls” as commented previously. We feel this approach to a culture of cyber security requiring facilities with Low Impact BES Cyber Systems to be covered by programmatic

plans or procedures will improve cyber security. However, Table R5, Part 5.4 calls for “Procedural controls for initially changing default passwords,” in the Requirements, but in the Measures the first bullet says; “Demonstration showing default vendor passwords have been changed, sampled on a locational basis.” APPA recommends the following changes to the Requirement and Measures: Requirement: System Access Control Procedure for initially changing default passwords…” Measures: Evidence may include, but is not limited to, a System Access Control Procedure that describes the process for initially changing default passwords when new devices are deployed and additional evidence to demonstrate that this procedure was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel showing default vendor passwords have been changed will require a Responsible Entity to identify all Low Impact BES Cyber Assets. This would be a major burden to Responsible Entities and may imply the need for a list of all Low Impact BES Cyber Assets. APPA understands that High Impact BES Cyber Systems may need to undergo more stringent compliance requirements. If the SDT feels it is necessary to conduct sampling of changed vendor passwords, Requirement R5 Part 5.4 should be split into two Parts; one for Low / Medium Impact BES Cyber Systems and one for High.

Yes

No

R1: BES Cyber Security Incident Response Plan Specifications Comments: APPA is concerned with the possibility of violations of Requirements in CIP-008-5 conflicting with Requirements in EOP-004-2. APPA understands that CIP-008-5 is the “Incident Response Plan” and EOP-004-2 requires the development of an “Operating Plan for Event Reporting.” However, CIP-008-5 Table R1, Part 1.1 requires a process to “identify, classify, and respond to BES Cyber Security Incidents” while EOP-004-2 R1.1 requires; “A process for identifying events listed in Attachment 1.” APPA recommends the SDT revise the Requirement and Measure in Table R1, Part 1.1 to remove the terms “identify” and “classify.” Table R1, Part 1.2 requirement of a process to determine if an incident is a “Reportable BES Cyber Security Incident” is in direct conflict with Event Reporting Reliability Standard EOP-004-2. APPA suggests Part 1.2 be removed and coordinated with the EOP004-2 SDT. Table R1, Part 1.3.3 requires definition of “Internal staff and external organizations that should receive communications of the incident.” EOP-004-2 R1.3 requires “A process for communicating events in Attachment 1 to the ERO, the RC… and other appropriate entities.” APPA suggests Part 1.3.3 be removed and coordinated with the EOP004-2 SDT.

No

R2: BES Cyber Security Incident Response Plan Implementation and Testing Comments: In Table R2 Part 2.2 the Requirement states “initially upon the effective date” which implies that date is the only time this plan can be implemented. APPA suggest replacing the term “upon” with the term “by.” This will allow Responsible Entities to implement the plan prior to the effective date and be in compliance. APPA recommends that Table R2, Part 2.3 be removed or clarified. If the intent of the SDT was to require records retention for compliance that is covered in Section C1.2 Evidence retention and Part 2.3 should be removed from the standard. If it was the intent of the SDT to require Responsible Entities to have a “Procedure” for retaining Reportable BES cyber Security Incidents then the Requirements and Measures need to be reworded. APPA offers the following revision for Part 2.3 Requirement: Procedure for retaining relevant documents related to Reportable BES cyber Security Incidents for three calendar years. Measures: Evidence may include, but is not limited to, a records retention procedure that describes retention of Reportable BES cyber Security Incidents for three calendar years and additional evidence to demonstrate that this plan was implemented such as, but not limited to, the signature of the CIP Senior Manger on the procedure. APPA points out to the SDT that the Measures language proposed is similar to CIP-004-5 R1. We feel showing records retention of all documentation for Reportable BES cyber Security Incidents will be a major burden to Responsible Entities.

No

R3: BES Cyber Security Incident Response Plan Review, Update, and Communication Comment: In Table R3, Part 3.2, 3.3, and 3.4 require different times for updates; 30 and 60 calendar days. APPA believes these times should coordinate with the plan update requirement in EOP-004-2 which allows 90 calendar days.

Yes
No
R1: Recovery Plan Specifications Comment: Table R1, Part 1.5 - The requirement to "Preserve data where technically feasible" may impede the timely restoration of a BES cyber asset that is required for the reliable operation of the BES. For example, if an entity is required to create an image of an affected hard drive for forensic analysis or to send the device to a laboratory for analysis, this may interfere with the restoration of the system. Suggest changing the wording to "Actions to preserve data where such actions do not interfere with the restoration of the function of a BES Cyber System."
No
R2: Recovery Plan Implementation and Testing Comment: Table R2, Part 2.2 the Requirement states; “to ensure that the information is useable and reflects current configuration.” APPA believes the statement should read “to ensure that the information is useable and reflects currently approved configuration based on the CIP-010-5 Part 1.1 or 1.2 as appropriate.”
No
R3: Recovery Plan Review, Update, and Communication Comment: In Table R3, Part 3.2, 3.3, and 3.4 require updates within 30 calendar days. APPA believes these times should consistent with CIP-008-5 updates and as stated in Question 36 should be changed to 90 calendar days for update of the plan.
Yes
No
R1: Configuration Change Management: Comments: In Table R1, Part 1.3 the Requirement states; “identification and categorization of the BES Cyber System, as necessary.” APPA believes the statement “as necessary” gives the Responsible Entity the option to self identify those BES Cyber Systems that apply to this requirement. Therefore, APPA recommends the removal of “as necessary” from this sentence. In Table R1, Part 1.4.2 and 1.4.3 use the term “verify” and “verification” where the version 3 CIP-007 R1 uses “test.” APPA would like clarification from the SDT why this change was made and why the Requirement does not match up with the Measure which uses the term “test.”
No
R2: Configuration Monitoring Comment: APPA recommends the SDT go back to the drawing board on this requirement. This requirement is next to impossible to do physically and it will be a compliance nightmare with constant technical feasibility exceptions. Even the first words of the requirement are “Where technically feasible.” APPA strongly suggests that the SDT remove this requirement and address the FERC Order 706 directive in a cost benefit analysis that the cost of putting these controls on all High and Medium Impact BES Cyber systems far outweigh the cyber security benefit. APPA cannot recommend to its members an affirmative vote on the CIP standards if this requirement remains as written.
No
Comments: In Table R3, Part 3.2 the Requirement states; “perform an active vulnerability assessment in a test environment.” APPA requests the SDT define at a minimum a “vulnerability assessment.” Also, what is the difference between an “active” and “passive” vulnerability assessment.” The SDT needs to clarify what a “test environment” is compared to a “production environment.” APPA suggest the following change to the Measurements that may clarify the intent of the SDT:”Each entity must define the test environment reflective of the requirements as laid out in CIP-010 R1.4.” In Table R1, Part 3.4 the Requirement states; “action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of the action plan.” This requirement will be hard to prepare for audit since it will require a continuous update of the execution status in case of a spot check. APPA recommends removal of the statement;” including the planned date of completing the action plan and the execution status of the action plan.” from the requirement.
Yes
Yes

Yes
Yes
No
Implementation Plan: Change: Remove: “18 Months Minimum” Add: “24 Months Minimum” Rationale: CIP Version 5 will impact an increased number of Responsible Entities who are not included in the Applicability of the CIP Version 3 or Version 4 standards. Twenty-four months is needed to allow for sufficient operational planning and budgeting activities to successfully implement Version 5. In most cases, twenty-four months will allow for two budgeting cycles to deal with the organizational and financial considerations of Version 5 for those Registered Entities (many of which are small) who have not previously dealt with the myriad of CIP asset issues. We understand that 18 months was proposed to facilitate the potential avoidance of implementing Version 4 however, Registered Entities may need the option of using this additional six months to successfully implement Version 5 to avoid non-compliance issues. Again, many of these entities are small and have not previously needed to deal with cyber asset issues to the degree Version 5 will likely require.
Individual
Greg Rowland
Duke energy
Yes
• Overall comments o There are many capitalized terms in this document that aren’t defined terms, and aren’t proposed to be defined terms, so their capitalization should be removed. (These definitions (as well as the ones on NERC’s website) need a thorough review and revision.) o Throughout—Terms and especially acronyms used but not defined in this document are not all defined in the NERC Glossary of terms. (CIP, NERC, BES, EMS, SVC, and DMZ (see more on DMZ below)). Also, inconsistent use of acronyms--SVC, ATC and AVR are defined upon use in the document most of the other acronyms used are not. The NERC Glossary of Terms is now outdated with terms like Critical Cyber Asset. o Throughout—some definitions include parenthetically noted acronyms, such as Electronic Security Perimeter (”ESP”). Others, such as Protected Cyber Asset (PCA??) are not. Be consistent, with a preference from this entity to publish acceptable (industry-wide) acronyms to assist in communications between entities, regulators, auditors, etc. o Page 8 “Intermediate Device”: The definition of “Intermediate Device” uses the acronym “DMZ” to describe a “DMZ” network. Both the acronym and the term “DMZ network” should also be defined. (Please do NOT use the common, but incorrect term “Demilitarized Zone” (a physical area where military activity is banned, usually between two opposing forces), but rather the more accurate and effective “Demarcation Zone” (A line defining the boundary of a buffer zone or area of limitation) to define the acronym DMZ!) • BES Cyber Asset – More guidance should be provided on how the 15-minute time criteria is to be be applied. Need to define or better clarify the meaning of the phrase “adverse impact” so that the threshold is understood. “Adverse impact” could mean many different things. For example, the NERC-defined term “Adverse Reliability Impact” means “The impact of an event that results in Bulk Electric System instability or Cascading”. • BES Cyber Security Incident – Third bullet should be reworded to include attempts to gain physical access into a Defined Physical Boundary. • BES Cyber System – “Maintenance Cyber Asset” should be “Transient Cyber Asset”. • BES Cyber System Information – The phrase “BES Cyber System Impact Designations” should use a lower case “I” on the word “impact”. • BES Reliability Operating Services o Lead-in paragraph – “Operating Services” is not a defined term and should not be capitalized. o Balancing Load and Generation – Unit Commitment is not a real-time activity and should be deleted. Also under Load management, Demand Response, and Manually Initiated Load Shedding, the “Ability to identify load change need” is not a real-time activity and should be deleted. o Managing Constraints – ATC is a forward-looking business concern and shouldn’t be on this list. Also, “Interchange schedules” raises many questions. For example the IDC is a NERC tool; so what entity (or entities) are responsible for its protection? “Identify and Monitor Flowgates” is planning horizon work and shouldn’t be on this list. o Restoration of BES – Blackstart restoration bullet should be reworded as follows: “Blackstart Resources and Cranking Paths as identified in the Transmission Operator’s restoration plan.” o Situational Awareness – “Situational Awareness” is not a defined term. It’s unclear what is meant by the phrases “unplanned changes” and “Change management”. “Next Day planning” is not real-time and should be struck from this list. o Inter-Entity

Real-Time Coordination and Communication – The ISN is a virtual NERC tool that they manage. Who is responsible for identifying and protection? Also RCIS? • CIP Exceptional Circumstance – Strike the phrase “Cyber Security” in order to make this more broad. • Transient Cyber Asset – How does the 30-day clock work? What does “directly connected” mean? Does it matter if the device is shut down every night? What if it’s physically disconnected for one minute and then reconnected?
Yes
• Under 1.4, 2.12 should be 2.13 • 2.5 needs to be replaced with the language of 1.5 from CIP-002-4 Attachment 1, as follows: “The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.”
Yes
It is important to retain, and if possible, more clearly delineate the provisions for dealing with Low Impact BES Cyber Assets and BES Cyber Systems (i.e. “do not require discrete identification” and “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.”).
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
1. The rationale for R2 should be reworded from “…contains the proper policies…” to “…covers the required policies…” 2. Consider whether the role-based training approach adequately addresses Order 706 paragraph 435, where “any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions could, even inadvertently, affect cyber security.”
No
Measure 3.1 - Delete the phrase “the date access was first granted”, since this may not be available for all individuals currently having access.
No
4.1 – should the word “initial” be retained? The word “Initial” here could indicate that this new requirement must be done for existing individuals who already have access prior to V5 becoming enforceable. Consider rewording or a grandfather clause. 4.2 - “Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more.” Does six months apply to just the school

requirement or “resided and been employed” “Been employed” can be construed many different ways especially if a company covers many areas and locations. Clarify this to ensure it will be clear that it covers where the person actually worked… not where the corporate office is.
Yes
No
R6.1, 6.2, 6.3, 6.5, 6.6 – These requirements introduce the phrase “minimum necessary” regarding access permissions. Demonstrating compliance could become controversial and overly burdensome. Consider using Version 4 language phrases such as “need-to-know” and “confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities.”
No
R7.1 - Need further clarification to allow for situations where people are out for a period of time (suspension, sickness, etc.) and then determine while that person is still out that they are being terminated or not returning. Access should be allowed until the determination is made they are not coming back – not as of the last day worked.
Yes
No
R1.1 - Measures should be “technical OR procedural controls” to match language of requirement. Propose removal of “and have been implemented” from the end of the measure statement to avoid tracking compliance on a ‘per-device’ basis, otherwise this would support the need for tracking this information for low impact BES Cyber Systems. R1.2 - Modify the applicability column to frame applicable Cyber Systems/Cyber Assets as those with External Routable Connectivity or dial-up connectivity. Also modify the requirements column to exclude ‘all routable and dial-up connectivity’ as the focus should be ‘external routable or dial-up’ connectivity (as covered within the proposed Applicability change). R1.3 - Although 'Deny by Default" is included in the Guidelines and technical basis it should be put back in the language of the requirement and only have criteria for granting access. R1.4 - There were various interpretations of ‘non-Interactive Remote Access,’ which implies this requirement may need some additional clarification, may look to merge R1.4 with R1.2. “where technically feasible” – Make clear that this is a TFE-able section?
No
R2 - Not all requirements make sense for both routable and dial-up connectivity - perhaps split out requirements? Have one set for expectations for routable connectivity and another set of requirements for dial-up? R2.1 - Applicability should include External Routable or dial-up connectivity as a filter. Suggest rewording to support placement of an intermediary device that may not be part of an ESP. R2.2 - Where does encryption supposed to start/stop - suggestion is to specify that encryption doesn’t need to extend past the intermediate device…otherwise it renders the IDS unable to evaluate the potential for malicious traffic.
No
Classifying instances where no documentation of compliance exists as severe is appropriate; instances in which a minority of non-compliance controls were identified within a primarily compliant program should be assessed a VSL with respect to the finding. VSLs addressing ‘each identified EAP’ and ‘all Interactive Remote Access’ should be assessed as a sliding scale to consider whether lower/moderate/high may be more applicable.
No
Conceptually we are good with this section with only editorial comments noted below: 1. Page 11, Part 1.2 “Measures” states “the physical security plan that describes the physical boundaries and how ingress and egress is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs.” a. This measure implies a requirement to log egress from Defined Physical Boundaries (DFBs) for “Medium Impact” BES Cyber Systems. The registered entity feels that this requirement goes above and beyond existing systems and installations to restrict access to cyber assets by controlling and logging ingress only. The additional system complexities and costs to add additional hardware and system capacity to log egress to a number of facilities across service areas by all NERC members

is considered onerous and does not address any perceived or real risks where individuals vacate a protected area. 2. Page 12, Part 1.3 Measures a. Entity has the same comment on egress logging as above. Particularly, when access is now restricted for High Impact based on multi-factor access controls. 3. Page 13, Parts 1.4 and 1.5 Requirement statements require real-time alerts to be issued to individuals responsible for responding to unauthorized physical access. a. The intent of the drafting committee regarding required responses is not clear and could range from each entity defining the parameters of the actual responses, or that there is some undocumented implication that CIP-008 requirements should be used, based on prior versions of the standards. 4. Page 14, Part 1.6 Requirement statement "Log (through automated means or by personnel who control entry) of physical entry into each DPB…" a. This statement implies that self-logging cannot be done by personnel entering the DPB. In the case of an authorized individual accessing a DPB by two different physical locks and keys (providing the 2 different access controls to a High Impact DPB) there is implication that this access point must be manned by a second party to conduct the logging. If this is the intention of the drafting team, the registered entity feels this is not operationally or cost effective to implement by the industry. If this is not the intent of the drafting team, the registered entity requests clarification of the written requirement.

Yes

No

Page 18, Part 3.2 Requirement states the entity must "Log dates, time, and duration for failures or outages of access control, logging, and alerting systems." • Suggest for clarity that this statement be changed to use the defined term "Physical Access Control Systems" in place of "access control, logging, and alerting systems", words which are contained in the definition of "Physical Access Control Systems".

Yes

No

• Table R1 o R1.1 Requirement – Suggest changing language to "Disable or restrict access to unnecessary logical network accessible ports". This removes the need to document the justification for all enabled ports while still requiring the need to demonstrate that ports have been reviewed and limited. o R1.1 Measures – Suggest changing language to "Evidence may include, but is not limited to, documentation that only necessary ports remain enabled". o R1.2 Requirement – Suggest adding the following sentence to the end: "Restriction of physical ports can be achieved technically or procedurally via policy".

No

• Table R2 o R2.1 Requirement – Agree with EEI recommendations. o R2.2 Requirement – Agree with EEI recommendations. o R2.3 Measures – Agree with EEI recommendations.

No

• Table R3 o R3.3 Measures – Agree with EEI recommendations. o R3.4 Requirement – Suggest changing language to "Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to any Cyber Asset listed in the Applicability section". o R3.4 Measures – Suggest changing language to "Evidence may include, but is not limited to, an inventory of Transient Cyber Assets or removable media and the methods used to detect, deter, or prevent malicious code." o R3.5 All – Suggest deletion of this Requirement in full. Logging, especially that without any form of review, provides no assistance in the protection of BES Cyber Systems and is not explicitly required in Order 706.

No

• Table R4 o R4.1 Requirement – Agree with EEI recommendations. o R4.2 Requirement – Agree with EEI recommendations. o R4.2 Measures – Agree with EEI recommendations. o R4.3 Requirement - Agree with EEI recommendations. o R4.3 Measures - Agree with EEI recommendations. o R4.4 Measures - Agree with EEI recommendations. o R4.5 Requirement - Agree with EEI recommendations. o R4.5 Measures - Agree with EEI recommendations.

No

• Table R5 o R5.1 Requirement – Suggest changing language to "Authenticate user account access before granting electronic access to each Cyber Asset within the Applicability section, where

technically feasible." o R5.2 All - Agree with EEI recommendations. o R5.3 All - Agree with EEI recommendations. o R5.5 Requirement - Agree with EEI recommendations.
No
Agree with EEI recommendations.
No
We are good with this standard in general. Suggest the following improvement: Page 11 Part 1.2 Requirements statement a. This requirement does not provide guidance to a Registered Entity in terms of the reporting process for an incident that has been determined to be a "Reportable BES Cyber Security Incident". Suggest that language be added to point to current or drafted standards and requirements such as CIP-001-1a R4 or EOP-004.
Yes
Yes
Yes
No
1. Requirement 1, Part 1.3 (page 10) stating "One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality". Comment is that the "protection" requirement could be construed as being redundant with CIP-011 and put responsibility entities in double jeopardy regarding compliance to two standards rather than just one. I believe the intent of protecting the information is also reflected in Part 1.4 of this same standard (page 11). 2. Requirement 1, Part 1.5 (page 11) is not a good requirement. It states "Preserve data, where technically feasible, or analysis or diagnosis of the cause of events that triggers activation of the recovery plans(s) as required in Requirement R1." This requirement is much too specific and I believe misses FERC Order Section 739's and 740's stated intent "give responsible entities a high confidence level that their backups will actually restore the system as needed". These FERC Order Sections should be and in my opinion are covered in Part 1.4, not in this new requirement. If anything, this new requirement should state that the responsible entity should conduct and document a root-cause analysis to attempt to identify the reason a system had to be recovered. There is real value in that, but not in a requirement to preserve data (but with no requirement to do anything with it!) As well, some system failures are obviously not data related and this practice again would be of no real value to preventing future impacts to the BES.
Yes
Yes
Yes
No
• General Comment – Still poorly written and difficult to understand. Needs a Technical Writer to correct tense, language use, match grammar to intent, etc. • Page 8/bullets 2&3: What is the difference here between these two? • Page 10/middle column-1.1.4: Should the last word be 'Asset' instead of 'Entity'? Seems confusing… • Page 11/middle column: Why Sr. Mgr. for baseline deviation approval? Too far removed from the daily working details. Should be line mgr/supv. • Requirement asks for physical location to be part of the baseline. Recommend to replace with "unique identifier". • Recommend to allow using minimum security baseline documents/templates as a baseline configuration vs actual point in time view of configuration on actual asset being a baseline • Not clear if such baseline needs to be changed every time an update is performed (e.g. every time new patch levels are released). Recommend instead to allow baseline that states "patch levels need to be up to date (no older than XYZ) days" that would allow for more consistent process.
No
Recommend to specify how frequently the changes to the baseline need to be monitored. Also,

recommend to add criteria for distinguishing between different levels of deviation (high risk vs. low risk change/deviation) and appropriate response based on the level.
No
• Page 18/3.3/middle column: What is “CIP Exceptional Circumstance”? This is undefined and new. Why is this being introduced, and what is the intent? • Recommend to replace wording “…the controls are implemented correctly and operating as designed” with less subjective language, such as “verify against minimum baseline”. • Need definition on “CIP Exceptional circumstances” under requirement 3.3
Yes
No
Agree in full with EEI recommendations.
No
Agree in full with EEI recommendations.
No
Agree in full with EEI recommendations.
No
We believe that due to the extensive changes in Version 5, more than 18 months will be required. We propose 24 months, and the effective date should not be on January 1, due to the added degree of difficulty with a year-end roll-out.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
BES Cyber System Definition: Is the drafting team going to provide more guidance on how a "system" is to be determined by registered entities? Do all assets included in a system have to reside in the same physical location? BES Cyber Asset Definition: Is this definition intended to replace the definition of Cyber Asset? Drafting team needs to provide clarification on the statement "The timeframe is not in respect to any cyber security event or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES". How does this statement apply to assets that don't necessarily operate the BES, but produce real-time information that could affect real-time BES operational decisions (e.g. ATC/AFC calculation engines)? Also, is it the drafting teams intent that this definition include auxillary assets related to facilities where the assets reside (e.g. Fire systems, HVAC, Halon system, etc.)? BES Reliability Operating Services Definition: Related to Balancing Load and Generation [Manually Initiated Load Shedding], is it the drafting teams intent that this include load shedding resulting from opening non-BES circuits? Related to Monitioring and Control [SCADA], is it the drafting teams intent that the SCADA system be categorized into an impact category as a whole, or broken up into seperate BES Cyber Systems? Related to Inter-Entity Coordination and Communication [Scheduled Interchange], how does the drafting team expect registered entities to handle third-party BES Cyber Assets associated with scheduling interchange transactions (e.g. OATi). What is the drafting team's expectation for securing BES Cyber Assets that are used by multiple entities and maintained and operated by a common external vendor or service provider?
No
No
Drafting team needs to address change in categorization from higher to lower impact, if registered entities portion of BES is modified or changes.
Yes
Yes
Yes

Yes
Yes
No
This is an ambiguous requirement. Drafting team needs to expand on expectations for making individuals aware. Does this require distribution, training, posting on company website etc.?
Yes
Yes
Yes
Yes
No
If training is role-based then why is the applicability to High and Medium BES Cyber Systems. This implies that anyone with access to these assets needs all of the training specified in 2.2 thru 2.10 and takes away the basis of a role-based training program.
Yes
Yes
No
The applicability is confusing here and does not align with applicability for the PRA program.
No
How does the drafting team expect registered entities to prove that "Access permissions are the minimum necessary to perform assigned work functions?" This introduces an entirely new concept for revoking access when an employee's work functions change and could become overly burdensome?
Yes
Yes
No
Part 1.3 has an applicability which considers routable connectivity for Medium Impact assets, but not for High Impact assets. Part 1.5 includes this consideration for both classifications. Is there a reason for this inconsistency?
Yes
Yes
Yes
Yes
No
Drafting team needs to clarify whether an outage of a Physical Access Control System is a violation of the standard. R3 seems to allow for this type of occurrence; however it is unclear.
Yes

Yes
Yes
Yes
No
Drafting team needs to clarify whether part 4.1.2 applies locally at the device level. This is unclear. R4.2 is too generic. There will be inconsistency across the regions in how this requirement is implemented.
No
The applicability is inconsistent on part 5.4. Is "All Responsible Entities" meant to represent all asset classifications?
Yes
No
Is "All Responsible Entities" meant to represent all asset classifications? Is it the drafting teams' expectation that separate incident response plans be developed for different asset classifications?
Yes
No
Why does the applicability change from all Responsible Entities to High and Medium Impact?
Yes
No
Is it the drafting team's intent that a separate recovery plan be developed for each BES Cyber System and/or BES Cyber Asset?
Yes
Yes
Yes
No
If the baseline configuration includes security-patch levels, does the CIP Senior Manager have to approve every security patch that is implemented on every applicable asset?
Yes
No
What is the intent of the term "active" vulnerability assessment? This needs to be clarified by the drafting team?
Yes
Yes
Yes
Yes

Yes
Individual
Richard Powell
JEA
Yes
BES Cyber Assets – Need to clarify that the definition applies to physical devices. BES Cyber Security Incident – “suspicious event” is subjective and the word “compromised” is ambiguous. Either define them or remove them. BES Cyber System Information – See APPA comments (define BES Cyber System Impact). CIP Senior Manager – JEA supports APPA comments (change CIP to CIP-002 – CIP-011). Reportable BES Cyber Security Incident – The word “compromised” is ambiguous. Delete or define the word.
Yes
The main issue for JEA is that a new broad-brush approach, attempting to associate reliability of the BES to arbitrary counts of lines, substation MVA, and generation MW is not effective. It will both over-identify and under-identify critical BES elements. Instead, NERC and the industry would be best served and the reliability of the BES best ensured by CIP carefully specifying a new reliability-based methodology for use by the industry. As an alternative, NERC could use the current version 4 bright line criteria modified by the version 5 classification scheme to determine High and Medium Level assets. For the currently proposed criteria: 2.1 – The value of 1500 MW should be defined as either the nameplate or the continuous “rated” capability (where the equipment has been de-rated by the Responsible Entity for age/reliability). 2.7 – 2.7 – The IROL designation (criteria 2.8) correctly identifies transmission facilities that are critical to the reliability of the BES and makes criteria 2.7 unnecessary. The voltage or MVA capacity of a transmission line does not represent the criticality of the line to BES reliability. However, if the criterion 2.7 remains, JEA believes the voltage criteria adopted in version 4, criteria 1.7 is more appropriate than the newly proposed 200kv. 2.8 – Need clarification of what “single station or substation location” is (or is not). If the intent is any facility listed on an IROL, the criteria should state such. 2.13 – Under BAL-002, NERC has established a requirement to address loss of generation. This should eliminate the need for the generator control center portion of criteria 2.13 (part 2). Should the drafting team choose to maintain the second part of criteria 2.13, the 300 MW rating identified is too low and should be revised to be 1500MW in alignment with criteria 2.1.
No
See APPA comment (90 days instead of 30).
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No

JEA supports FMPA comments (VSL to R5 time frame of “within the audit period”).
Yes
Yes
No
2. The phrase “associated with” is used as a “catchall” phrase that leaves three definitions open ended and potentially confusing. The definitions are found in the “Definitions of Terms Used in Standard” for CIP-003 through 010. The definitions are recommended to read: • Associated Electronic Access Control or Monitoring Systems – Applies to Cyber Systems that provide Electronic Access Control or Monitoring for a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems • Associated Physical Access Control Systems – Applies to Cyber Systems that provide Physical Access Control for a corresponding High or Medium Impact BES Cyber Systems. • Associated Protected Cyber Assets –Protected Cyber Assets within a High or Medium Impact BES Cyber Systems.
Yes
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (retain event logs for 90 days, like CIP-007 R4.4). See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
See “Associated…” comment in question 15.
No
JEA supports APPA comments (change “remediation” to “mitigation”). See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
JEA supports APPA comments (clarify retain event logs of R4.4) See “Associated…” comment in question 15.

No
JEA supports APPA comments (initial change of default passwords R5.4) See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (remove communication of incident R1.3.3 and coordinate with EOP-004-2)
No
JEA supports APPA comment (in R2.2, implement “by” the effective date)
Yes
Yes
No
JEA supports APPA comments (Part 1.5 preserving corrupted drive could reduce reliability). See “Associated…” comment in question 15.
No
JEA supports APPA comment (Clarify Part R2.2 – that information is useable) See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
Yes
No
JEA supports APPA comments (Part 1.3 – delete “as necessary”) See “Associated…” comment in question 15.
No
See “Associated…” comment in question 15.
No
R3.3 - Should PACS (Physical Access Control Systems) be included with EACM (Electronic Access Control and Monitoring) of CIP 007? See “Associated…” comment in question 15.
Yes
No
Access Control of information should be consolidated into CIP-004. See “Associated…” comment in question 15.
No
2. The phrase “associated with” is used as a “catchall” phrase that leaves three definitions open ended and potentially confusing. The definitions are found in the “Definitions of Terms Used in Standard” for CIP-003 through 010. The definitions are recommended to read: • Associated Electronic Access Control or Monitoring Systems – Applies to Cyber Systems that provide Electronic Access Control or Monitoring for a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems • Associated Physical Access Control Systems – Applies to Cyber Systems that provide Physical Access Control for a corresponding High or Medium Impact BES Cyber Systems. • Associated Protected Cyber Assets –Protected Cyber Assets within a High or Medium Impact BES Cyber Systems.
Yes
Yes

Group
Kansas City Power & Light
Scott Harris
Yes
Proposed definitions that include defined terms introduces additional confusion and the opportunity for misunderstandings. We recommend review of these definitions to address the identified issue. As a general comment, the proposed definitions lack clarity and are far too complex. It is difficult to comment on these definitions as there is uncertainty as to what the SDT was targeting. In general, KCP&L subscribes to the EEI comments regarding the definitions. If changing nomenclature is not specific to a directive or does not enhance security / reliability, the terms should stand as they currently exist with proposed adjustments to definitions if necessary. The BES Reliability Operating Services definition is a set of criteria and not a definition. The criteria specified are overly detailed. We recommend serious consideration is given to simplification. In addition, the criteria should be limited to the functions that support the real-time reliability of the BES. The current criteria include planning systems and tools that should not be included for consideration.
Yes
The purpose of the bright line criteria in CIP-002-4 was to establish clear and unambiguous criteria for determination and identification of critical assets applied to all facilities. That purpose was basically achieved. The proposed set of “definitions” and criteria in version 5 has completely reversed those efforts reintroducing ambiguity. Once again, it has become unclear with the current proposed “bright line” criteria what cyber equipment and systems are to be protected. Version 5 as proposed has reintroduced Registered Entity judgment in the determination. In addition, specifically for item 2.7, there is no engineering basis for the method to determine what transmission facilities should be included in CIP considerations. Utilizing the proposed “weighting” technique, despite the effort to defend such in the “Guidelines and Technical Basis” section, complicates the process further and does not provide sound rationale for application of this criteria. The phrase “adversely impact” leaves too much room for interpretation and will lead to additional confusion and misunderstandings. KCP&L strongly recommends the removal of this proposed CIP-002-5 Attachment 1 and replace with CIP-002-4 Attachment 1. This will likely need modification to include Medium and Low criteria to align with the other efforts in CIP version 5.
No
The following are general comments that permeate throughout CIP Version 5: 1. There is no need or purpose for the section “4.2 Facilities” under the applicability section. The criteria already established by Attachment 1 satisfy the direction for facilities under consideration. This section promotes confusion and is not helpful. We recommend removal. 2. Section 4.1.8 identifies the Regional Entity as an applicable entity. The Regional Entity has been defined by NERC in the Rules of Procedure as the Compliance and Enforcement Authority (CEA). The CEA has no operating obligations or operating authority. We recommend removal. This also applies to Section 4.1.7 concerning the NERC obligation for operations or operating authority. We recommend removal. In requirement 1 it says; “All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low impact and do not require discrete identification.” However, in M1 it says “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” We recommend this inconsistency is corrected with an adjustment to either the Requirement or the Measure. Requirement 1.1 says; “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation…”. This is unclear and the underlined portion doesn’t make sense. KCP&L recommends modification to, “when a change to BES Elements is completed and / or the facility is placed into operation”.
No
The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. The requirement should direct an entity to develop their Cyber Asset lists. Furthermore, the entity is directed to perform a review and approval process. The level of review and approval should be determined by the entities governance model, organizational structure, compliance culture, etc. It is inappropriate for the CIP Standards to dictate how the organization manages cyber security requirements or compliance with regulations.
No
The Violation Risk Factors (VSL’s) appear overly weighted to the HIGH and SEVERE severity levels.

The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an enity.
No
The Standards Development Process should not produce standards or requirements that dictate how an entity is to accomplish meeting a requirement. We recommend removal of this from the Standard. The level of review and approval should be determined by the entities organization and governance structure. It is inappropriate for the CIP Standards to dictate how an organization should manage security and protection of the Bulk Power System. Further, the Internal Compliance Program principles endorsed by NERC recommend that a strong compliance program is one that is supported by executive management. Registered entities implementing this type of program recognized by NERC. This action is sufficient and does not require the need for the Standard to dictate the appointment of a Senior Manager by name.
No
The SDT should not use specific examples under each topical area as it does in the Guidelines and Technical Basis section unless the list is all inclusive. Providing a general overview or definition of each topical area within the Requirements and Measures section under each sub-requirement (2.1-2.10) is preferable to listing a few examples under each topical area in a separate section of the Standard.
No
Reference to the CIP Senior Manager should be removed for the reasons stated earlier. Suggest the following content change: "Each Responsible Entity shall review each of its cyber security policies and obtain organizational approval initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals."
No
The phrase "make aware" is only a slight improvement over the phrase "readily available" used in the previous versions of this Requirement. Both leave room for interpretation. If you read the R4 Rationale and R4 Measures with the R4 Requirement, this Requirement is relatively clear. However, when the Rationale is removed upon final approval, the intent of the SDT will be lost. KCP&L recommends incorporating the clearly stated direction to communicate the intent of the SDT, stated in the Rationale, in the Requirement.
No
We recommend removal of the Senior Manager reference within the requirement for reasons stated previously.
No
We recommend removal of the Senior Manager reference within the requirement for reasons stated previously.
No
1. This language cites a High VSL when 'not all' individuals have been made aware of elements of the cyber security policy. This seems to contradict the intent described in the R4 rationale in which 'it is not the intent of the SDT for the responsible entity to have the burden of proving that each and every individual can access the document.' 2. The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
Yes
No
Comment is specific to Part 2.10 of Table R2. Language in the table seems to require training on network connectivity for anyone with access to High and Medium BESCS. For some categories of users (e.g., Operators) this will be both out of context and irrelevant. For some categories (e.g., Network administrators) this will be unnecessary for job functions that require network connectivity knowledge. Recommendation is to strike item 2.10.

No
Measure 3.1 where it calls for the date access was first granted is a point of concern for both legacy employees (where it may be impossible). Requirement 3.2 – Propose content change • Original content – Require completion of the training specified in CIP-004-5, Requirement R2 at least once every calendar year, but not to exceed 15 calendar months. • Proposed change – Require annual completion of the training specified in CIP-004-5, Requirement R2. • Rationale – The wording adopts the CAN-0010 approach for annual as defined within the registered entity.
No
KCP&L recommends removal of the second sentence in Requirement 4.2. Requiring the reason a 7 year background check was unable to be fully completed will add additional cost contributing little or no value to the personnel risk assessment program. KCP&L recommends removal of Requirement 4.4 as it is not practical or cost effective for an entity to validate contractors or service providers are following the stipulations of CIP-004-5 R4. This stipulation would require entities to audit contractors and service providers which is not practical. We recognize the risk associated with contract personnel that do not have appropriate screening and clearance for the access as discussed. We recommend additional discussion around options for closing the gap, such as a registration function applicable to vendors and service providers operating in the space granting compliance enforcement authority for the regulator to review the CIP-004-5 R4 compliance of said entity.
Yes
No
Requirements 6.1, 6.2 and 6.3: These requirements should remove the Senior Manager reference for reasons stated previously. In addition, we recommend the content be changed to: Establish criteria for job functions that require electronic access, physical access, and/or cyber information maintaining a current list of personnel granted such access.
No
Requirements 7.1 through 7.5 and industry HR processes and practices are out of synch regarding HR practices and processes in the determination of dates for resignations, terminations, and transfers. These requirements are in desperate need of additional thoughtfulness in consideration of HR processes that can include adjustment of dates for resignations, terminations, and transfers to meet HR needs. In addition, these requirements do not consider the potential need for personnel to have a transition time as they transfer from one job function into another job function within an organization.
No
The proposed VSL's do not consider sufficient thoughtfulness to give Registered Entities credit for efforts to achieve compliance with requirements. Requirements R1 through R4 do not have Low or Moderate severity levels. There is room to recognize efforts to meet compliance.
No
Requirement 1.3: Outbound is of little security value and will come at additional expense to entities. Following the stipulations of the CIP Standards helps to ensure the integrity of the cyber assets physically and electronically. Inbound is definitely necessary. KCP&L recommends removal of the "outbound" language in the requirement and the measure. Requirement 1.5: It is not possible to detect "malicious communications" for some Electronic Access Point (EAP) equipment. We recommend replacing "at" to "for" in the requirement to recognize that some EAP equipment may not have such detection capability.
No
Requirement 2.2: this requirement lacks clarity to understand the scope and boundary for which remote session encryption is required. We recommend the SDT clarify the boundary for this requirement.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No

Requirement R1.2: The measure includes additional requirements regarding egress controls. This is not included in the requirement and contributes minimal improvements to the physical security of cyber assets. The CIP Standards require control of personnel who can physically access cyber assets and stipulates escorting of non-authorized personnel. Ingress controls and monitoring are sufficient to protect cyber assets. Requirement 1.3: This requirement does not recognize defense in depth implementations nor does the requirement recognize alternative actions and measures that can be implemented in the temporary absence of a control. Failure to include these as alternative measures and limiting entities the current proposed requirement can result in substantial unwarranted costs. Recommend the SDT modify this requirement to include defense in depth implementations and alternative actions. Requirement 1.4: This requirement limits physical access alerts to only go "to personnel who are responsible for response". What is important is that alerts go to personnel regardless if the personnel can respond to the alert or to personnel who can notify other personnel to respond to the alert. Restricting this to personnel responsible for a response is shortsighted and does not recognize organizational structure. In addition, the requirement is too broad in alerts issued for "any access point in a Defined Physical Boundary." Recommend changing this to "any access at a Defined Physical Boundary."
No
Requirement R2.2: a. Applicability – Applicability wording of "Medium Impact BES Cyber Assets" should be changed to "Medium Impact BES Cyber Assets with External Connectivity." i. Rational - Medium Impact BES Cyber Assets should only require full Defined Physical Boundary physical protections and Visitor Control Programs when they have External Connectivity (i.e. routable and dial-up). Standalone Medium Impact BES Cyber Assets can not be remotely attacked so their scope of impact is basically similar to other non-cyber based devices at the location. Serial connected Medium Impact BES Cyber Assets have very limited attach vectors which are better addressed with electronic protections. We therefore feel standalone and serial connected Medium Impact BES Cyber Assets should have physical protections similar to those required for Low Impact BES Cyber Assets. To support this approach the following changes are suggested. b. Requirements – Proposed Change i. Original Text – A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the entry and exit on a per 24-hour basis, the visitor's name, and individual point of contact. ii. Proposed Change - A process requiring manual or automated logging of the entry and exit of visitors that includes date and time of the first entry and last exit, the visitor's name, and individual point of contact. iii. Rationale – The proposed change capture the intent with (hopefully) clearer language. The 24 hour basis may introduce expectations that 'round-the-clock' logging needs to be in place. Some visitations may cross the midnight time-line, which shouldn't introduce additional requirements.
No
Requirement R3: 1. R3.1 a. Overall observations – the shift from (pre-V5) maintenance on 'mechanisms' to the Draft 1 'systems' expands this requirement beyond the intent. • This should be more focused on testing to ensure alerting and control mechanisms work as intended. • Use of controls should be considered 'tested' in situations where applicable devices are used every day (i.e. card readers). b. This sub requirement cites tasks to be conducted 'prior to commissioning.' Since many controls are expected to be in place prior to V5 adoption, there should be language within the implementation plan to capture devices in use at the time the standard becomes effective.
No
The Table of Compliance Elements cites references to sub requirements that appear to be incorrect: • Lower – Part 1.7 should point to 1.6 • High – Part 1.6 should point to 1.5
No
Requirement R1.1 – Requirements – Proposed Content Change 1. Original Content – Disable or restrict access to unnecessary logical network accessible ports and document the need for any remaining logical network accessible ports. 2. Proposed Change – Enable only logical accessible ports needed, including port ranges where required. 3. Rationale – The proposed language incorporates much of the legacy (CIP-007-3 R2.1) language. The additional requirement to document the need for remaining logical ports extends beyond what FERC Order 706 requests without adding security benefits. 4. There is no direction or explanation about what an "unnecessary" port is nor does it address who the ultimate authority to make such a decision. This requirement leaves far too many components open for interpretation by the auditors and leaves entities in a precarious position of

possible non-compliance based on the opinions of the individual auditors. 5. The requirement language states that access to an “unnecessary” port can be disabled or access to the port can be restricted. It does not require any documentation detailing how access to the port is to be restricted nor does it require any documentation of these “unnecessary restricted” ports. It only requires documentation about the need for any “remaining” logical network accessible ports. This oddly worded requirement leaves too many components open for interpretation by the auditors and leaves the entities in a precarious position of possible non-compliance based on the opinions of the individual auditors. Requirement R1.2 1. Requirements – Content Change a. Original Content - Disable or restrict the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. b. Proposed Change – Protect against the use of unnecessary physical input/output ports that could be used for network connectivity, console commands, or removable media by disabling, restricting, or use of signage. 2. Measures – Content Change a. Original Content - Evidence may include, but is not limited to, documentation stating specific or types of physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. b. Proposed Change - Evidence may include, but is not limited to, documentation stating specific physical input/output ports to restrict and screen shots or pictures showing the ports restricted either logically through system configuration or physically using a port lock or signage. 3. The measure for this requirement indicates there needs to be a physical or software restriction on the physical input/output ports, but the requirement is not clear about the specific intent to physically, either through hardware or software, disable or restrict the use of physical input/output ports.

No

Requirement 2.1 1. Requirements – Content Change a. Original Content - Identify a source or sources that are monitored for the release of security related patches, or updates for all software and firmware associated with BES Cyber System or BES Cyber Assets. b. Proposed Change – Identify a source or sources that are monitored for the release of security related patches, or security updates for software and firmware associated with BES Cyber System or BES Cyber Assets. 2. Measures – Propose striking the last sentence “The list could be sorted by BES Cyber System or source.” It introduces additional requirements with no clear security benefit or alignment with FERC Order 706. 3. Need clarification on when a “remediation plan” is needed. Is it required in delay between OS patch release and vendor approval? When vendor will not approve patch? When there is a vulnerability for which no patch has been released? Requirement 2.3 – Clarification Needed KCP&L uses multiple sources to identify the release of security patches. For example, Microsoft may release an alert that a patch is available on date X but, we don’t receive a vendor alert that the patch is safe to put on until date Y. The wording does not state which date takes priority. Is it the earliest? Is it the latest? Is it up to each entity to decide? Need clarification added. Requirements 2.2 and 2.3 should be switched, as 2.3 requires the establishment of a process for remediation, and 2.2 addresses the creation or revision of the remediation plan. Requirement 2.2 a. Requirement – Propose content change i. Original content - Identify applicable security-related patches or updates and create a remediation plan, or revise an existing remediation plan, within 30 days of release from the identified source that addresses the vulnerabilities within a defined timeframe. ii. Proposed change – Identify applicable security-related patches or updates within 30 days of release from the identified source that addresses the vulnerabilities, and create or revise a remediation plan that addresses the vulnerabilities within a defined timeframe. iii. Rationale – The rewording captures the chronological order of the elements within this requirement to provide clearer guidance. Requirement 2.3 b. Requirement – As currently worded, there is no allowance for changes in the remediation plan should outage coordination, or other resource constraints require modifications to the remediation plan. This is a point of concern that should be addressed. c. Measures - Example measures for this requirement include items, such as, Exports from automated patch management tools that provide the installation date, verification screen captures that show Component software revision, registry exports that show software has been installed, etc. Using our current system for vulnerability management, a patch that isn’t relevant produces no evidence. The system only shows security patches that need to be installed. Using this system, KCP&L will not have installation dates, registry exports, etc. to provide as evidence. It is the lack of an applicable security patch being listed on reports that indicates compliance in our program. Need clarification that this is acceptable.

No

1. Requirement 3.2 a. Requirement – Content Change i. Original content – Disarm or remove

identified malicious code. ii. Proposed change – Mitigate the threat of identified malicious code. iii. Rationale – In some instances, the presence of malicious code may present a lesser risk to the reliability of the BES than disarming/removal processes, especially when the malicious code may not exploit a feature used within the Cyber System. b. Measure – Add a bullet to allow for evidence of manual removal. 2. Requirement 3.3 c. Requirement – Propose content change i. Original content – Update malicious code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). ii. Proposed change – Update malicious code protections from the identified source within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns). iii. Rationale – The addition of 'the identified source' provides a context for determination of availability. d. Include testing within both the requirements and measures as alluded to within the Application Guidelines (page 41). e. Measures – Format (i) and (ii) to a bulleted list signifying 'or' criteria f. Part 3.3 requires an update within 30 days. What "starts the clock" on this requirement? Is there an allowance for an approval step from a 3rd party vendor after the OEM has released the signature or pattern update? In some instances, a 3rd party vendor may have to approve prior to a Responsible Entity implementing a release and their delay could cause timing concerns. 3. Requirement 3.4 g. Applicability – Propose deletion of Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems as they do not appear to be Transient Cyber Asset related. h. Requirements – Content Change i. Original Content - Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to BES Cyber Assets or Protected Cyber Assets. ii. Proposed Change – Deploy method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets and removable media when connecting them to Medium or High Impact BES Cyber Assets or Protected Cyber Assets. i. Measures – Content Change i. Original Content – Evidence may include, but is not limited to, logs showing when Transient Cyber Assets and removable media were connected to BES Cyber Assets or Protected Cyber Assets, and an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. ii. Proposed Change – Evidence may include, but is not limited to, an inventory of Transient Cyber Assets and the methods used to detect, deter, or prevent malicious code. iii. Rationale – Excised content introduced prescriptive criteria that introduced additional resources without clearly addressing the requirement. 4. Requirement 3.5 j) Part 3.5 requires logging each Transient Cyber Asset connection, but this would be captured in the Configuration Change Management requirements of CIP-010-1. As it is covered elsewhere, recommend this requirement be removed from this section of the standard.

No

1. Requirement 4.1 a. Requirements – Content Change i. Original Content - Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. ii. Proposed Change – Log generated events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Any detected failed access attempts at Electronic Access Points 4.1.2. Any detected successful and failed login attempts 4.1.3. Any detected malware 4.1.4. Any detected potential malicious activity. Devices that cannot log a particular event do not require a TFE to be generated. iii. Rationale – Content from the application guidelines has been introduced to promote the guidance that TFE's are not required in instances in which devices cannot log a particular event. iv. Requirement 4.1 includes the use of "any" in the list of activities to log. Not all activities require follow up or investigation and that is the purview of CIP-008-5. Specifically, "any" failed login may not be an indication of a problem. Certainly there is a threshold that deserves attention, but the broad use of the term "any" makes this requirement too broad. v. Requirement 4.1.4 is far too broad of a statement. Even if an entity uses an intrusion detection system, each IDS vendor has their own set of signatures. Who will be the authority on what is considered "potential malicious activity"? 2. Requirement 4.2 a. Applicability – Propose deletion of Associated Physical Access Control Systems and Associated Electronic Access Control Systems as they are out of scope for this requirement. b. Requirements – Content Change i. Original Content – Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert. ii. Proposed Change – Generate alerts for events that the Responsible Entity determines necessary. c. Measures – Content Change i. Original Content – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate real-time alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity

determines necessitate a real-time alert; Screenshots showing how real-time alerts are configured. ii. Proposed Change – Evidence may include, but is not limited to paper or system generated listing of event classes and conditions which necessitate alerts; Assessment documentation or report showing analysis was performed to determine which events the Responsible Entity determines necessitate an alert; Screenshots showing how alerts are configured. iii. Rationale – Removed the usage of 'real-time' as it presents concerns demonstrating compliance. 3. Requirement 4.3 d. Requirements – Content Change i. Original Text – Detect and activate a response to event logging failures before the end of the next calendar day. ii. Proposed Change – Activate a response to failures of event logging before the end of the next calendar day after identification. iii. Rationale – Some devices generate logs so infrequently that identification of logging failure may extend beyond any calendar day. The spirit of this requirement remains intact as one day remediation is required once the log failure is identified. iv. Requirement 4.3 sets a timeframe of "before the end of the next calendar day". This is a very short timeframe. Certainly, logging failure should be addressed. Recommend a longer time frame is needed. 4. Requirement 4.4 e. Requirements – Content Change i. Measures – Content Change 1. Original Text – Evidence may include, but is not limited to, security-related event logs from the past ninety days and records of disposition of security related event logs beyond ninety days up to the evidence retention period. 2. Proposed Change – Evidence must include, but is not limited to, security-related event logs from the past ninety days. 5. Requirement 4.5 Requirement 4.5 inserts a manual review when automation and alerting, both mentioned previously in the standard are much more effective and reasonable controls. If a Responsible Entity is compliant with Requirements 4.1-4.4, then a manual review is a redundant effort which provides no additional security. Recommend requirement 4.5 be removed.
No
1. Requirement 5.1 a. Overall – In both the original content and proposed change there exists instances where access is a component of validation and/or authentication. This presents a potential compliance challenge that should be addressed. b. Requirements – Content Change i. Original Content – Validate credentials before granting electronic access to each BES Cyber System. ii. Proposed Change – Authenticate user account access before granting electronic to each Medium or High Impact BES Cyber System or Associated Protected Cyber Asset, where technically feasible. iii. Validating credentials was seen as vague specific to technical compliance so authentication is offered as an alternate approach to satisfy the root requirement (and mirrors the language in the change rationale). The addition of 'where technically feasible' was to recognize technical capabilities currently in place may not adequately demonstrate compliance with this. 2. Requirement 5.2 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 3. Requirement 5.3 – Propose deletion as it replicates the requirements identified within CIP-004-5 R6.1. 4. Requirement 5.4 a. Requirements – Content Change i. Original Text – Procedural controls for initially changing default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on BES Cyber Assets, Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. For the purposes of this requirement an inventory of Cyber Assets is not required. ii. Proposed Change – Procedural controls for initially removing, disabling, or changing default passwords, where technically feasible. For the purposes of this requirement an inventory of Cyber Assets is not required. iii. Rationale – The additional wording identifies the multiple methods which can be used to mitigate default passwords. 5. Requirement 5.5 a. Requirements i. Change Systems to Assets throughout as password limitations should be identified to the device level. ii. Add language to 5.5.3 to cover instance where accounts may not be able to support password change to permit the entity specified time frame to be equal to the life-time of the BES Cyber Asset where technically required. iii. Requirement 5.5.3 is confusing and unclear, especially the license and service agreement language. Also, the inclusion of "based on the impact level of the BES Cyber System" is not helpful. Recommend that the impact phrase be stricken.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
Yes
No

Requirement R2.1 states, "…and include recording of deviations taken from the plan during the incident or test". The measures require that we justify any deviations taken. No two incidents are ever the same and they will seldom follow a strict plan. The purpose of a sound incident response plan is to provide a framework to detect, contain, eradicate and recover allowing the freedom to assess and analyze a circumstances and conditions and take appropriate actions. Recommend this be removed from the requirement and the measure. 1. Requirement 2.2 a. Content Change ♣ Original Content • Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): o by responding to an actual incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Proposed Change • Test the incident response plan(s) annually. A test of the plan may include: o A response to an incident, or o with a paper drill or table top exercise, or o with a full operational exercise. ♣ Rationale – References to requirements needed upon the effective date should be captured within the implementation plan, allowing the standard to identify requirements (only) in place once the standard is approved. b. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence showing annual testing of the BES Cyber Security Incident response plan(s). Types of exercises may include discussion or operations based exercises. Document lessons learned within 30 days of incident or exercise. Use lessons learned to update incident response plan(s). ♣ Rationale – The Homeland Security Exercise and Evaluation Program identifies seven types of exercises within HSEEP, each of which is discussions-based or operations-based. 2. Requirement 2.3 Propose deletion as this sub requirement merely identifies retention requirements already documented within Compliance (C.1.2).
No
1. Requirement 3.2 1. Requirements – Propose content change a. Original content – Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan. b. Proposed change – Use lessons learned from incident responses or incident response exercises to update the incident response plan, within sixty days of documenting lessons. c. Rationale – It takes 30 days from the time an exercise is executed to the review and completion of an after action report. The thirty day clock should start once the after action report is completed. This is in line with the proposed 60 day timeline in R3.3. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan. ♣ Proposed Change – Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or incident response within thirty calendar days of the lessons learned associated with the response plan. 2. Requirement 3.3 1. Requirements – Content Change ♣ Original Content • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan. ♣ Proposed Change • Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that test or incident. 2. Measures – Content Change ♣ Original Content – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan. ♣ Proposed Change – Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan test or incidence response and the dated, revised plan.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
1. Requirement R1 • 1.1 – Propose alternate language (carried forward from previous versions) 1. Create and implement a recovery plan that at a minimum includes: 1. Conditions for activation of the

recovery plan 2. Roles and responsibilities of the responders • 1.2 – Propose deletion as this sub requirement has migrated to R1.1 proposed R1.1 rewrite. • 1.3 1. Requirement – Content Change 1. Original – One or more processes for the backup, storage, and protection of information required to restore BES Cyber System functionality 2. Proposed Change – One or more processes for the backup, storage, and restoration of information required to restore BES Cyber System functionality 3. Suggest additional content supporting mirroring and/or redundancy within the backup/recovery methods such as: 1. Mirroring and/or redundancy can be considered as complementary measure in support of this requirement, but a process must be in place to ensure retrieval of previous versions should current version(s) require reverting to a previous instance. 2. Measure – Content Change 1. Original – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and protection of information required to successfully restore a BES Cyber System. 2. Proposed Change – Evidence may include, but is not limited to, documentation of specific processes for the backup, storage, and restoration of information required to successfully restore a BES Cyber System. • 1.4 – Correct headers from 'part' to 'Applicability,' 'Requirements,' and 'Measures' 1. 1.4 1. The current form does not adequately address FERC Order 706, paragraphs 739 and 748, and in fact contradicts the intent that 'The Commission does not believe that every change will necessitate verification of the backup and restoration processes' from paragraph 740. 2. Propose 'new' sub requirement applicable to High Impact BES Cyber Systems to require: 1. Upon implementation of significant changes to High Impact BES Cyber Systems, verify that backups are operational before they are relied upon for recovery purposes. 3. Propose rewrite 1. Original – Information essential to BES Cyber System recovery that is stored on backup media shall be verified initially after backup to ensure that the backup process completed successfully. 2. Proposed Change – Ensure that backup processes are completed successfully for Information essential to BES Cyber System recovery. 3. Rational – This focuses on successful completion of the backup process which can be done within the routine backup. Verification would be moved to its own requirement applicable to High Impact BES Cyber Systems and limited to significant change instances. • 1.5 1. Requirement – Content Change 1. Original Content – Preserve data, where technically feasible, for analysis or diagnosis of the cause of any event that triggers activation of the recovery plan(s) as required in Requirement R1. 2. Proposed Change – Document root cause for events that trigger activation of the recovery plan(s) as required in Requirement R1. 3. Rationale – Root cause documentation should be the focus for this requirement. The current draft language requires potential impediments to restoration efforts and is too vague.

No

1. Requirement 2.1 1. Requirements – Content Change ♣ Original – Implement the recovery plan(s) referenced in R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between executions of the plan: by recovering from an actual incident, or with a paper drill or tabletop exercise, or with a full operational exercise ♣ Proposed Change – Implement the recovery plan(s) referenced in R1 annually: • by recovering from an actual incident, or • with a tabletop exercise, or • with a functional exercise ♣ Rationale – Use of the functional exercise aligns with the R2 rationale content citing NIST SP 800-84 exercise types. Requirements in advance of the effective date of the standard should be addressed within the implementation plan. 2. Measures – Content Change ♣ Original – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with a full operational exercise) of the recovery plan at least once each calendar year, not to exceed 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. ♣ Proposed Change – Evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a tabletop exercise, or with a functional exercise) of the recovery plan annually. For the table top or functional exercise, evidence may include meeting notices, minutes, or other records of exercise findings. 2. Requirement 2.2 1. Requirements – Content Change ♣ Original Text – Test any information used in the recovery of BES Cyber systems that is stored on backup media initially and at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and reflects current configurations. ♣ Proposed Change – Test information used in the recovery of BES Cyber systems that is stored on backup media annually, to ensure that the information is useable. 3. Requirement 2.3 1. Overall ♣ This requirement (to be done every 39 calendar months) appears to overlap considerably with 2.1 (to be done every year). ♣ Every 39 calendar months exceeds the 3 year retention identified within the Compliance section. ♣ How does

this differ from current EOP-008 requirements? 2. Requirements – Content Change ♣ Original – Test each of the recovery plans referenced in Requirement R1, initially upon the effective date of the standard, and at least once every 39 calendar months thereafter through an operational exercise of the recovery plans in a representative environment that reflects the production environment. An actual recovery response may substitute for an operational exercise. ♣ Proposed Change – Exercise the recovery plan(s) at least every 39 calendar months through an operational exercise in a representative environment. An actual recovery response may substitute for an operational exercise. ♣ Rationale – Actions required to take place prior to the effective date of the standard should be captured within the implementation plan.
No
Requirement 3.1 1. Requirements – Content Change ♣ Original – Review the recovery plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. ♣ Proposed Change – Review the recovery plan(s) annually and document any identified deficiencies. ♣ Rationale – Requirements addressing tasks to be done prior to the effective date should be captured within the implementation plan. Requirements 3.2 – 3.3 Recommend a 60 day timeframe for requirements 3.2-3.4, to be consistent with the recommendation for CIP-008-5. Requirement 3.4 Propose deletion as the requirement is too broad with no clear alignment with FERC Order 706 or security benefit.
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
1. Requirement R1.1 1. 1.1.4 – Propose content change ♣ Original Text – Any custom software and scripts developed for the entity; ♣ Proposed Change – Any custom software and scripts installed on the BES Cyber Asset that can affect the security posture. ♣ Rationale – The change focuses scope to eliminate software and scripts not in use. 2. 1.1.5 – Propose content change ♣ Original Text – Any logical network accessible ports; and ♣ Proposed Change – Any network accessible ports or services; and ♣ Rationale – This clarifies the requirement to focus on 'active ports and services' rather than Ethernet jacks. 2. Requirement R1.2 1. Requirement – Propose content change ♣ Original Text – Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Proposed Change – Document approved changes to the BES Cyber System that deviate from the existing baseline configuration. ♣ Rationale – As documented earlier in this comment form, requiring Senior Manager (or delegate) authorization introduces resource constraints that impede the effective documentation of changes without adding security benefits or alignment with FERC Order 706. 2. Measure ♣ First paragraph – Add 'or,' at the end of the first bulleted paragraph. ♣ Second paragraph – Propose content change • Original Text – A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) were an individual with the authority to authorize the change was in attendance. • Proposed Change – A record of the change with authorization of the change. • Rationale – Citing a "change advisory board" within the measure overly represents adequate evidence in support of the requirement. 3. Requirement R1.3 1. Requirements – Propose content change ♣ Original Text – Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change. ♣ Proposed Change – Update the documented baseline configuration as necessary within 30 calendar days of completing the change. ♣ Rationale – The proposed rewording provides more focus on the root requirements. 4. Requirement 1.5 Requirement 1.5 is duplicative of Requirement 1.4. Are Control Centers expected to perform dual testing procedures? This does not add to the security of a Control Center and simply adds additional work. Recommend removal of Requirement 1.5.
Yes
No
Requirement 3.2: An active vulnerability assessment of test environments as required in Requirement

3.2 will be burdensome and expensive for smaller entities. Additionally, requiring smaller entities to purchase a vulnerability assessment tool or contract for this service for every install is also burdensome and expensive.
Yes
Yes
Yes
No
The Violation Risk Factors (VSL's) appear overly weighted to the HIGH and SEVERE severity levels. The VSL's should reflect a qualitative approach that recognizes the risk and/or impact non-compliance with a requirement may have on the reliability of the BES and the compliance efforts made by an entity.
No
References to requirements to be conducted in advance of the implementation date should be migrated over into the implementation plan. This ensures any pre-requisites are captured within the implementation plan, freeing this content from the standards to provide clearer guidance. This occurs in the following sections: 1. CIP-002 a. R2 b. M2 2. CIP-003 a. R3 3. CIP-008 a. R2.2 b. M2.2 c. R3.1 4. CIP-009 a. R2.1 b. R2.3 c. M2.3 d. R3.1 e. M3.1 f. VSL (High-R2) g. VSL (Severe-R2) h. VSL (Severe-R3) 5. CIP-010 a. R3.1 b. R3.2 6. CIP-011 a. R1.3 b. VSL (High-R1)
Individual
Rebecca Moore Darrah
MISO
In its comments on Version 4 of the CIP standards in Docket No. RM11-11, MISO raised a number of concerns arising out of the identification of Critical Cyber Assets through the application of the bright line criteria in Attachment I of CIP-002-4. In its comments, MISO stated: MISO is concerned that application of the "bright line" criteria proposed in the NOPR, some of which require identification of Critical Assets based on determinations made by Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners, will create significant new burdens on Reliability Coordinators, Planning Authorities/Coordinators, and Transmission Planners – without the benefit of promoting the additional consistency and clarity that the Commission and NERC are seeking in approval of the NOPR. This concern is furthered by certain ambiguities in the "bright line" criteria that MISO has identified, particularly with regard to the treatment of data centers that support control centers. Finally, MISO is concerned that the requirement that Reliability Coordinators identify must-run units as Critical Assets may cause certain Generator Owners to preemptively take their units offline prior to identification of them as must-run. Although Attachment I of Version 4 is used to identify Critical Assets while Attachment I of Version 5 is used to identify BES Cyber Assets and Systems, MISO remains concerned about these issues in the Version 5 Standards, arising out of items 2.3, 2.8 and 2.9 of Attachment I of CIP-002-5. Because MISO has fully expressed these concerns in its comments on Version 4, MISO will not repeat the concerns here; rather, MISO hereby incorporates its comments on Version 4 of the CIP standards, which were filed on Nov. 21, 2011, Docket No. RM11-11
In the "Background" section of CIP-002-5, the SDT writes that one "of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems." The "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" defines the term BES Cyber System as "[o]ne or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services." The SDT goes on to state that the use of the term BES Cyber System is intended "to provide a higher level for referencing the object of a requirement." MISO requests clarification from the SDT on two issues associated with this language. First, the "Background" section provides the example of a BES Cyber System that is subject to a malware protection requirement and states that by using the concept of a BES Cyber System, "it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual

device to comply." However, neither the definition of BES Cyber System nor the malware requirements in CIP-007-5 indicate, on their own, that compliance with the requirement does not require every BES Cyber Asset that comprises a BES Cyber System to have malware protection. MISO is therefore concerned that the Regional Entities will continue to enforce the CIP standards on an individual BES Cyber Asset basis, per a literal interpretation of the text of the Version 5 Standards. As such, MISO requests more explicit confirmation of the holistic approach of the Version 5 Standards as indicated by the "Background" section of CIP-002-5. In addition, MISO requests additional examples similar to the malware example already provided. Second, MISO requests clarification regarding a Responsible Entity's ability to "determine the level of granularity at which to identify a BES Cyber System[,]" as stated in the "Background" section of CIP-002-5. In the same paragraph, the SDT states that the level of granularity is "left up to the Responsible Entity," but also that "defining the boundary too broadly could make the secure operation of the BES difficult to monitor and assess." While this language implies that Responsible Entities will be able to define the borders of BES Cyber Systems without oversight, MISO questions whether the Regional Entities would defer to the judgment of Responsible Entities with regard to the "proper" level of granularity of BES Cyber Systems, particularly since the SDT states that overly broad boundaries could make the secure operation of the BES "difficult to monitor and assess." As a result, MISO requests clarification that the Regional Entities would not play a role in the definition of boundaries of BES Cyber Systems, and suggests that the SDT provide a series of examples of the definition of the boundaries of BES Cyber Systems of varying types and sizes.

CIP-003-5, Requirement R2: Requirement R2 requires Responsible Entities to implement one or more cyber security policies that address each of ten listed topics listed. The "Guidelines and Technical Basis" section of this Standard state that the "cyber security policy must cover in sufficient detail the ten topical areas required by CIP-003-5 R2" and proceeds to list a number of sub-topics associated with each of the ten required topics that the "Responsible Entity should consider for each of the required topics." MISO requests confirmation that a cyber security policy that addresses each of the sub-topics identified in the "Guidelines and Technical Basis" section of CIP-003-5 will be considered to cover the ten topical areas identified in Requirement R2 "in sufficient detail."

CIP-004-5, Requirement R3: Requirement R2 requires Responsible Entities to have a role-based cyber security training program for personnel who need authorized electronic or unescorted physical access to BES Cyber Systems. The applicability for Requirement R2 is "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems." Requirement R3 requires the implementation of this cyber security training program for each individual needing authorized electronic or unescorted physical access, however the applicability of Requirement R3 is "High Impact BES Cyber Systems," "Medium Impact BES Cyber Systems," "Associated Physical Access Control Systems," "Associated Electronic Access Control or Monitoring Systems," and "Associated Protected Cyber Assets." The difference in applicability between Requirements R2 and R3 is ambiguous and is likely to create confusion among Responsible Entities. If documentation of a training program is required only for Responsible Entities with "High Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems," implementation of that training program should have the same applicability. MISO requests clarification of this issue.

CIP-004-5, Requirement R7: Requirement R7, Part 7.1 states that for "resignations or terminations, revoke the individual's unescorted physical access and Interactive Remote Access to BES Cyber

Systems at the time of the resignation or termination." The "Change Rationale" section states that this modification was made due to statements by the Federal Energy Regulatory Commission in Order No. 706 that access should be revoked immediately for any person no longer needing access. However, a footnote in Part 7.1 states that "[s]ince termination is often recorded without consideration to the time of day, 'at the time' does not require a to-the-minute or to-the-hour time-stamped comparison of access logs and the termination action." This footnote is ambiguous and will create confusion among Responsible Entities regarding the maximum allowable amount of time for revoking unescorted physical access and Interactive Remote Access to BES Cyber Systems. For instance, if a Responsible Entity were to revoke access on the same date that an employee with such access was terminated, would the Responsible Entity be in compliance? MISO therefore recommends that the SDT clarify or provide a safe harbor provision in Part 7.1.
CIP-005-5, Requirement R1, Part 1.3 requires Responsible Entities to "[r]equire explicit inbound and outbound access permissions at each identified [EAP] using routable protocols, including granting or denying access permissions." Requiring both inbound and outbound access permissions is redundant, and the added expense and effort required to implement such a framework would not be commensurate with the security benefit created by doing so. Electronic communication between devices requires both devices to acknowledge such communication in order for the communication to succeed. Such acknowledgment requires a signal to be sent from the initiating device to the other, and a response is then sent back to the initiating device. Until this initiation of communication is complete, no other communication can occur. If communication is disabled in one direction, the initialization of communication, i.e., the handshake, cannot occur, and further communication is not possible. Requiring only inbound access permissions should therefore suffice. Moreover, implementation of outbound access requirements in addition to inbound ones would be costly and resource intensive. As such, MISO recommends that outbound access permissions not be required in addition to inbound ones.
CIP-009-5, Requirement 1, Part 1.4 requires information "essential to BES Cyber System recovery that is stored on backup media" to be "verified initially after backup to ensure that the backup process completed successfully." This requirement places a significant burden on Responsible Entities with a large number of BES Cyber Systems or BES Cyber Assets comprising BES Cyber Systems. Such Responsible Entities may perform thousands of backups on a daily basis; as such, initial verification after each backup would require an extraordinary amount of resources while providing only a minimal benefit to the security of BES Cyber Systems over that attained by performing random sample verifications or sample verifications based on the type of Cyber Asset backed-up. MISO therefore requests that the SDT modify this requirement to provide for sample verifications, or to clarify that the current language of Part 1.4 is not intended to require initial verification following every backup.

Individual
Michelle D'Antuono
Ingleside Cogeneration LP
Yes
Overall, Ingleside Cogeneration LP agrees that expanding the number of cyber security definitions in the NERC glossary helps us gain a common understanding of a complex topic. There are a couple of terms that could be improved: First, the definition of “BES Cyber System” includes a statement that a “Maintenance Cyber Asset is not considered part of a BES Cyber System.” We believe this should be a “Transient Cyber Asset”, which will then be consistent with the definition of “BES Cyber Asset.” Second, the definition of “BES Reliability Operating Services” is close, but not exactly identical with the write-up in the “Guidelines and Technical Basis” section of CIP-002-5. Since this is essentially replacing the concept of a “Critical Asset” under the Version 4 standards, it is important to have a consistent description in both places. Furthermore the Functional Entity mapping to each operating service (Page 18 of CIP-002-5) is very helpful. The SDT should consider including it in the definition as well.
Yes
The most major change made to the CIP categorization criteria from Ingleside Cogeneration LP’s perspective is the addition of a Low Impact rating for every generation facility that does not meet the High or Medium Impact thresholds. This will force every registered GO and GOP to adhere to about 40 requirements in the remaining CIP standards. We are not convinced that the cost to “NERC-adapt” our existing cyber security policies, encourage cyber security awareness, and that cyber asset access management will lead to a corresponding reliability benefit. In addition, Regional audit resources would be better utilized to focus on truly critical locations – each hour spent on validating Low Impact facilities is one better spent on high or medium impact facilities. We recommend this category be eliminated. Secondly, Criterion 2.13 calls for “control centers that control 300 MW or more of generation” that are not already rated as High Impact, must be considered Medium Impact. The term “control center” is not capitalized – and it must be for consistency. Otherwise, it is possible that an auditor will declare all 300+ MW generation facilities to be at least Medium Impact, not just those that support two or more geographically separate locations. Lastly, Criterion 2.7 seems to have been modified to include some transmission substations operating at 200 kV to 300 kV. The present Version 4 bright-line criterion only includes those operating above 300 kV. Since this includes substations that are interconnected to generators, it seems likely that 200 kV substations newly identified as Medium Impact will require cyber hardening of the generation facilities as well. Again, there is no evidence provided by the SDT that a weighted assessment of the transmission facilities better identifies critical substations than the Version 4 criterion. This criterion should be changed back to the one approved by the industry in CIP-002-4.
No
There should not be a Low Impact rating for every facility that does not meet the High or Medium Impact thresholds. Our resources and Regional audit resources would be better served if allowed to focus on truly critical locations – each hour spent on validating Low Impact facilities is one better spent elsewhere.
Yes
Yes

Yes
No
We are not convinced that the cost to adapt our existing cyber security policies to specifically include the content proposed under CIP-003-5 R2 will lead to a corresponding reliability benefit. Similar to the manner in which they handle other NERC requirements, Compliance Enforcement Authorities will look for language that matches that in each of the ten listed items – whether clearly applicable to Ingleside Cogeneration LP or not. This usually means that if key words are not identical, a violation is assessed. The alignment of cyber security policies to the NERC format seems to be a paperwork exercise only, and makes little sense in the case of Low Impact facilities. Our resources, and our Regional Entity audit resources, would be better spent elsewhere. We recommend this requirement be made applicable to High and Medium Impact facilities only. In addition, it is likely that many of the low impact facilities, such as cogeneration facilities located within an industrial complex, currently have procedures in place. These are corporate wide procedures, and have been put in place for various agencies, i.e Department of Homeland Security, and this requirement would result in multiple procedures for a facility, causing confusion and would add no reliability value.
Yes
No
The rationale statement for CIP-003-5 R4 correctly captures the SDT's intent that the cyber security policy is available and accessible to personnel – not to prove that each and every individual can access the document. However the language of the requirement does not read that way. In fact, it seems to require that the Responsible Entity must track each individual's awareness of the appropriate elements of its cyber security policy. Ingleside Cogeneration LP believes that the requirement should include language that it is sufficient to post the policy on the corporate Intranet site or posted on bulletin boards that are accessible to all employees. These statements are presently captured in measure M4 and can be used as is. This provides accessibility to our personnel and on-site contractors. The education of cyber vendors is a much larger problem. Typically, their maintenance pools diagnose our systems remotely – and are not willing to distribute customer-specific cyber policies to their staff. We believe that an industry-specific policy needs to be developed and made publically available that will serve this need. It would seem likely to us that a NERC-driven initiative would catch the attention of such vendors – and could be written in a way that would be universally applicable to all industry stakeholders.
Yes
Yes
Yes
No
The "Guidance and Technical Basis" section addressing CIP-004-5 R1 correctly captures the SDT's intent that the cyber security awareness program is informational only – not to prove that each and every individual was made aware (i.e.; formal training.) However the language of the requirement does not read that way. In fact, it seems to require that the Responsible Entity must track each individual's awareness of the cyber security on a quarterly basis. Ingleside Cogeneration LP believes that the requirement should include language that it is sufficient to distribute quarterly reminders through email, on posters, or at meetings. These statements are presently captured in the "Guidance and Technical Basis" section and can be used as is. This will cover our personnel and on-site contractors. Maintaining the awareness of cyber vendors is a much larger problem. Typically, their maintenance pools diagnose our systems remotely – and are not willing to distribute customer-specific awareness materials to their staff. We believe that an industry-specific awareness program needs to be developed and made publically available that will serve this need. It would seem likely to us that a NERC-driven initiative would catch the attention of such vendors – and could be written in a way that would be universally applicable to all industry stakeholders.

No
Ingleside Cogeneration LP believes that CIP-005-5 R1.1 is unnecessary. The requirement applies to Low Impact facilities only and calls for technical or procedural controls to be defined that restrict electronic access. Its intent, as stated in the “Change Rationale” box, is to demonstrate that sufficient protections exist that prevent inappropriate access from public and other non-trusted networks. The SDT further infers that if enough Low Impact facilities are compromised by a cyber attacker, it may lead to higher level impacts to the BES. We are not convinced that such a risk exists – nor does the SDT provide any evidence that it does. This means that the cost to adapt our existing cyber security policies to specifically include the content proposed under CIP-005-5 R1.1 will not lead to a corresponding reliability benefit. The alignment of electronic access controls to the NERC format seems to be a documentation exercise only, and makes little sense in the case of Low Impact facilities.
No
Ingleside Cogeneration LP believes that the physical security requirements for Low Impact facilities (CIP-006-5 R1.1) are unnecessary. The requirement calls for operational or procedural controls to be defined that restrict physical access. Its intent, as stated in the “Change Rationale” box, is to “allow for programmatic protection controls as a baseline.” This appears to us to be a confirmation that no true reliability benefit is served by R1.1. From our viewpoint, the alignment of physical security controls to the NERC format seems to be a documentation exercise only, and makes little sense in the case of Low Impact facilities.
No
While Ingleside Cogeneration LP agrees with the intent and need for procedural controls which eliminate default passwords from BES Cyber Assets, we believe that CIP-007-5 R5.4 should not apply to Low Impact facilities. We are not convinced that the cost to adapt our existing password procedural controls to specifically include the content proposed under CIP-007-5 R5.4 will lead to a corresponding reliability benefit. From our perspective, the alignment of cyber security policies to the NERC format seems to be a paperwork exercise only, and makes little sense in the case of Low Impact facilities. Our resources, and our Regional Entity audit resources, would be better spent elsewhere.
No
The requirements for a cyber security incident response plan are similar, if not redundant with, those being developed under EOP-004-2 (Project 2009-02). If there are key items missing in EOP-004-2 that do not satisfactorily address a cyber attack, they should be corrected there. Otherwise Ingleside Cogeneration LP believes that we would be placed in a double-jeopardy situation for any gaps in the cyber security incident response plan.
No
The requirements for the execution of the cyber security incident response plan during an actual

intrusion attempt and the regular testing of the procedure are similar, if not redundant with, those being developed under EOP-004-2 (Project 2009-02). If there are key items missing in EOP-004-2 that do not satisfactorily address a cyber attack, they should be corrected there. Otherwise Ingleside Cogeneration LP believes that we would be place in a double-jeopardy situation for any failures to execute in accordance with CIP-008-5 R2.1 and R2.2. In the case of R2.3, the SDT calls for Responsible Entities to retain documents related to reportable cyber incidents for three years. However, item 1.2 under the "Compliance" section of CIP-008-5 states that the Compliance Enforcement Authority can request evidence dating back to the previous audit – which could be up to six years. In theory, the language in the requirement should predominate, but it is not clear to Ingleside Cogeneration that it would. Therefore, we recommend that a statement be included in the requirement which clearly shows its supremacy.
Yes
Individual
Scott Berry
Indiana Municipal Power Agency
Yes
BES Cyber System – Maintenance Cyber Asset is not a defined term. IMPA suggests using the term Transient Cyber Asset or defining Maintenance Cyber Asset. BES Cyber System Information – BES Cyber System Impact is not a defined term. CIP Manager – The definition should exclude CIP-001. Cyber Asset – definition is way too broad and could include devices such as a thermostat. Needs to be more tightly defined and be more applicable to the operation of the BES and should also relate somehow to how the device is accessed or connected – e.g utilizes/is connected via routable protocol and/or dial-up modem. There are numerous assets that are programmable that utilities use that have very minimal impact on the reliable operation of the BES (such as a programmable thermostat). BES Cyber Asset – need better definition on "if rendered unavailable, degraded, or misused…". This could be as simple as someone removing the trip output wiring – which could just as easily happen on a electro-mechanical relay with the same results. A BES Cyber Asset should be narrowed down to include if it is connected via routable protocol or dial-up modem and by use of this connection it is rendered unavailable, degraded, or misused would …… BES Cyber Security Incident – the last statement could be interpreted to include someone cutting a substation chain link fence. This needs to be more narrowly defined or removed from the definition. BES Reliability Operating Services – again very broad in scope. In addition these Services, as defined, are confusing and vague and could lead to numerous interpretations by auditors.
Yes
IMPA would like to see the addition of another category called "Low Impact without Connectivity". This category would be made up of Low Impact BES Cyber Assets that do not have routable protocol or dial-up access. It would be impractical to attempt a coordinated cyber attack on BES Cyber Assets without connectivity. Since it would be impractical or very difficult to coordinate a cyber attack and in taking into account that we are talking about Low Impact Cyber Assets, IMPA believes these assets

would not need to comply with the CIP standards because the costs would be unjustified. In addition there should be additional bright line criteria used to delineate a Control Center that meets the requirements for Medium Impact. For example use a weighted value as is done in 2.7 but for transmission facilities operating at 100 kV and above.
Yes
IMPA agrees with the requirement and not requiring discrete identification of Low Impact BES Cyber Assets or Systems. However, IMPA does not understand how entities are going to prove to auditors that the identification and categorization was done without having to produce an inventory or listing of assets to the auditors. The VSLs seem to imply that Low Impact BES cyber Assets or Systems need to be discretely identified. M1 states in part that "Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls." The only way to completely satisfy M1 would be to inventory and identify each and every Low Impact BES Cyber Asset and BES Cyber System. R1.1 provides a timetable to note a change to BES elements and Facilities that requires an entity to change the classification from a lower to a higher impact category but doesn't provide a timetable for the phase-in for the entity to meet the potential additional Standard(s) Requirements caused by this change.
Yes
Yes
Yes
No
The bullets are incorrectly numbered. R2 should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. R2 would be overwhelming and costly for a small entity to comply with if that entity has a single facility that may have only 1 Low Impact BES Cyber System. This should align with the Applicability for CIP-004-5 R1 through R7.
No
This should apply only to High Impact and Medium Impact BES Cyber Systems (see R2). In addition, it is not clear if each individual cyber security policy needs to be improved or if the approval of the CIP Senior Manager (one signature) covers all of the cyber security policies.
No
This Requirement should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. See Applicability for CIP-004-5 R1 through R7.
Yes
Cyber Security Policy should not be capitalized (it is not capitalized in R2 and R3).
Yes
no comment
No
This Requirement should apply only to those entities that have High Impact or Medium Impact BES Cyber Systems. See Applicability for CIP-004-5 R1 through R7. In addition there may only be a single person that this would apply to at a smaller entity that has a single Low Impact BES Cyber System. Quarterly reinforcement would carry little value. IMPA recommends a semi-annual or annual reinforcement frequency.
No
IMPA does not agree with the use of "must" in M2. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of "must" in M3. Measures are not requirements but are examples of evidence.
No

IMPA does not agree with the use of “must” in M4. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M5. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M6. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M7. Measures are not requirements but are examples of evidence. Part 7.1. IMPA finds it very difficult and maybe impossible to revoke access at the same time that a resignation is received. Footnote 2 does not address resignations, only termination. In addition, IMPA understands what the SDT is stating in the application guidelines for a voluntary termination under R7, but the requirement 7.1 does not make the same statement as in the guidelines. Auditors follow the requirements during an audit and not the SDT application guidelines.
No
The Severe VSL for R3 is either a yes or no answer which eliminates the high VSL.
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence. IMPA also believes that R1 will force entities with Low Impact systems to inventory them in order to provide evidence that it has performed or satisfied this requirement.
Yes
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence.
No
The way the VSLs are written just one missed EAP is a severe violation. The VSLs should be written in a manner to not make just one missed EAP a severe violation.
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence. Part 1.1 is very ambiguous and is very open to interpretation by entities and auditors which can lead to many violations of this requirement. For example, an entity may see that a fence and a gate with a padlock are sufficient. An auditor may deem this to be insufficient and cite a possible violation. Do both horizontal and vertical dimensions need to be enclosed? IMPA recommends the use of bright line criteria to ensure entities and auditors are on the same page for what constitutes a sufficient physical boundary. In the Requirements column “Define operational or procedural controls to restrict physical access” whereas in the Measures column “documented operational AND procedural controls exist”. This needs to be consistent.
No
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence. Part 2.2 The use of “on a per 24 hour basis” needs to be clarified. Do visitors need to be logged out at the end of 24 hours and then logged back? Does it mean use military time?
No
IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence. It is not clear if Part 3.1 applies to High, Medium, and/or Low Impacts.
no comment
No
IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence.
No

IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence.
No
IMPA does not agree with the use of “must” in M4. Measures are not requirements but are examples of evidence. Part 4.3 In order for this requirement to be met, an entity must use a redundant system to recognize an event logging failure. Therefore, this requirement seems to imply the use of redundancy. Part 4.4 This requirement covers data retention and should be moved to the data retention section.
No
IMPA does not agree with the use of “must” in M5. Measures are not requirements but are examples of evidence.
no comment
No
IMPA does not understand how entities are to “identify, classify, and respond to BES Cyber Security Incidents” on Low Impact systems. In order to “identify” BES Cyber Security Incidents on Low Impact systems, it seem like these entities will need to use a system to monitor potential cyber incidents. Entities with High and Medium Impact systems are required to use systems to “identify” BES Cyber Security Incidents, however, IMPA does not believe that entities with Low Impact systems should be forced through an “unwritten” requirement to use a system to monitor potential cyber incidents. This requirement should only apply to Medium and High Impact systems, especially since EOP-004 requires entities to respond and report to cyber security incidents that they are aware of, even for Low Impact systems. CIP-008-5 R1 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. IMPA does not agree with the use of “must” in M1. Measures are not requirements but are examples of evidence.
No
CIP-008-5 R2 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. See answer to question 34. IMPA does not agree with the use of “must” in M2. Measures are not requirements but are examples of evidence. Part 2.3 This requirement covers data retention and should be moved to the data retention section.
No
The question does not match the requirement. CIP-008-5 R3 – Applicability should be restricted to High Impact and Medium Impact BES Cyber Systems. This would better dovetail with Applicability Requirements of CIP-004-5, 005-5, 006-5, and 007-5. See answer to question 34. IMPA does not agree with the use of “must” in M3. Measures are not requirements but are examples of evidence.
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
no comment
No
For unplanned scenerios, IMPA recommends 18 months and not 12 months. If an entity experiences an unplanned scenerio in Jan of a year and needs to budget for the equipment or software, then the entity needs time to purchase and then perform the work.
Group

Paul Skare, et al
Paul M. Skare
Yes
With NERC CIP v5, we believe a graded security approach with low, medium and high impact on the BES is a sound approach, but have found it mostly focused on medium and high impact systems, and mostly the medium and high impact systems are bundled as a pair. For example, some password requirements are given for medium and high impact systems, but the draft is completely silent about what should be done for low impact systems. There is no reason not to mandate a no default password policy for *all* systems within the BES. Yes, there might be a few cases where legacy systems do not support anything but hard-coded defaults, but these could be documented en masse as exceptions (with associated compensating controls) rather than let these exceptions be used as an excuse to allow a poor password policy. In an effort to reduce the burden to industry we recommend including a grandfather clause that provides certain exceptions for legacy low-impact systems (such as those that do not have external computing interfaces or capabilities). As noted, the systems are graded into low, medium, and high, but the requirements/controls are not applied in a graded three-tier approach. Most requirements lump high and medium into one category and ignore low. Ideally we should have requirements that get successively stronger as we migrate from low to medium to high. There are a number of concerns that either exist in multiple places throughout the CIP standards or are applicable to the standard as a whole they include: * Consistency of the capitalization of terms * Consistency in the use of the terms Cyber Asset and Cyber System * Consistency in the use of the terms Cyber access and electronic access * Section 4.2.4.2 of many of the requirements use the term Electronic Security Perimeters. Has this been deprecated? * We disagree with Section 4.2.4.2 as an exemption - Communication links should be protected between ESPs * As defined, CIP Exception circumstances are not that exceptional. Scaling back requirements within an exceptional circumstance is acceptable, but completely suspending requirements is not. * Include a definition of terms section to the standards. The applicability section of each standard defines how the term applies to that standard but does not fully define the meaning of the term. Note: This and other comments submitted by our team represent our collective judgment as subject matter experts—they are not the official position of the Department of Energy nor of the Pacific Northwest National Laboratory.
No
Section 4.1.2 How are smart grid devices being operated by Distribution Providers? * Battery Storage is another question that is not addressed * Other smart grid assets (100KV+) Section 4.2.4.x Cyber Assets should be prefaced by BES Should the last paragraph on page 7 say “cyber security plan”?
No
Section 4.2.4.4 What is the definition of Cyber System vs. Cyber Asset? There is a need for consistency in use – especially in the tables. Section 5. Background – It seems this entire section is predicated upon a table which is missing. There is no table [Table Reference] pg 7 and under Applicability there is no table to aid in understanding of all the different “Applicability Columns” R2 Should include a Procurement Policy requirement R2 Should include a Resiliency Policy requirement R2 1.5 System Security: Should include third-party, outsourcing, and availability or be considered as separate topics. Guidelines R2 2.1 Personnel Security: Should explicitly include subcontractors and outsourced services R2 2.3 Remote Access should be moved into System Security Include language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity’s policies and controls. R2 2.7 Recovery Plans should include a prioritized recovery strategy
No

CIP-004-5 should also include the case where one organization has equipment in another organizations facility (i.e. substations)
No
The wording of the requirement is confusing. The measure for 3.1 does a better job defining the requirement than the requirement.
No
1.2 The requirements column should state “Control and secure all connectivity through the use of identified Electronic Access Points (EAPs). “ 1.4 Eliminate the “where technically feasible” loophole. The statement should simply be “Perform authentication when establishing dial-up connectivity with the BES Cyber System.” 1.4 Dial-up access for either non-interactive or interactive sessions should be authenticated. As written, 1.4 only protects non-interactive sessions.
No
Eliminate the “where technically feasible” loophole. The statement should simply be “Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items.” NEW: As written, low impact systems do not have to be protected with passwords, nor are the users required to be authenticated. Requirements for low impact systems should be added.
No
M1. Typo: - As stated “Evidence must includes…” should be “Evidence must include…” 1.5 Clarification needed with respect to the applicability column as to what impact level the associated physical access control systems apply. Explicitly state that this applies to all systems.
No
3.1 High and medium impact systems should have their associated physical access control systems monitored (and tested) more frequently that once every 24 calendar months. Testing frequency should be dependent upon the impact level (i.e. annual testing of a control center is not too frequent).
No
The requirement for all of CIP-007-05 should follow a graded approach to match the impact level of the various systems where the lower the impact level the more time or leniency is afforded to meet the requirement.
No
Patch management is optional for low impact systems. Even these systems should have patches applied, but perhaps in a less timely manner than is required for medium and high impact assets.
No
Malicious code protection is not required for low impact systems. Even these systems should be monitored/protected.
No
Once again, low impact systems are not included. Security event monitoring should also apply to low impact systems. R4 4.5 Two week lag before logs from high impact systems have to be reviewed. The reviews should be more timely, especially if only one calendar day is given to rectify issues discovered. We saw in GridEx how timeliness is important in this area.
No
Password management is not specified for low impact systems. No guidance is given regarding

sharing/reusing passwords between systems. R5 5.4 Eliminate the “where technically feasible” loophole. The statement should read “Procedural controls for initially changing default passwords unless the default password is unique to the device or instance of the application…” R5 5.6 Eliminate the “where technically feasible” loophole.
No
Seems OK. However, the definition of a reportable incident seems a bit vague.
No
1.2 Worded poorly. (Currently: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.) Should more clearly state that (pre) approval is needed for configuration management changes.
No
2.1 Caveat of “where technically feasible” applies to both medium and high impact systems. Compensating controls should be applied to high impact systems when built-in monitoring of baseline changes is not technically feasible.
No
3.3 Change in phrase order makes the requirement easier to understand “Perform an active vulnerability assessment prior to adding a new Cyber Asset to a Cyber System or Electronic Access Control or Monitoring System, except for CIP Exceptional Circumstances.
No
No uniform requirements for how BES Cyber System Information is to be handled. Is it business sensitive, official use only, etc? Furthermore, does the level of protection vary based upon whether the information is about high impact or medium impact systems? Missing a statement about how one is authorized to view BES Cyber System Information. How does one get added to the list of those with a “need to know” the information? The aspects of trust and the needed controls for trusted parties would be useful, especially regarding external entities such as vendors, contractors, DOE, NERC, etc.
Individual
Christine Hasha
Electric Reliability Council of Texas, Inc.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes

Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Regarding 7.1, request definition of when the clock starts for revoking access upon termination or resignation. This is of particular concern with relying on notification from external parties such as Regional Entities, vendors, contractors, etc. Regarding 7.2, request definition of when the clock starts for revoking access upon reassignment or transfer. Is there an allowance for training or support of the prior position? Regarding 7.3, request definition of when the clock starts for revoking access upon termination or resignation. This is of particular concern with relying on notification from external parties such as Regional Entities, vendors, contractors, etc.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes

No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also submits these additional comments. Regarding 2.1, remove the comma from the requirement. The comma changes the requirement to address all updates and firmware regardless of security impact.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Request allowances in 3.3 for signatures/pattern updates that cause trouble. Suggest adding “Create a plan to mitigate the vulnerability where it is determined that the signature or pattern update cannot be safely applied.” Also, request similar language to R2 in identifying the source for updates. Regarding 3.5, request reasoning for this requirement. How does this requirement address the rationale listed? This will be of particular difficulty when dealing with CDs as well as assets that have no capability of logging event.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT also offers these additional comments. Regarding 1.5, request clarification of retention of the preserved data. Also, needs to be noted that these activities must be secondary to recovery and not impede recovery.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 2.2, request clarification of what information is necessary. Does this include the operating system information from vendors? Does this mean testing every backup or every tape ever made? Does it have to be restored or just perform verification at the end of the backup? Regarding 2.3, is testing of each scenario in the plans required?
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 3.1, it is not practical to perform a review of all documents on the specific date of the effective date of the Standard.
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Request flexibility to have appropriate management structures utilized in automated change management processes.
Yes

No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
No
ERCOT has joined the SRC comments filed. Please see SRC comments. ERCOT offers these additional comments. Regarding 2.2, request clarification of the requirement. Does this mean destruction of data on the identified BES Cyber Assets only?
Yes
No
ERCOT has joined the SRC comments filed. Please see SRC comments.
Individual
Gregory Campoli
New York Independent System Operator
Yes
The Definition for External Routable Connection states that “The BES Cyber System is accessible from any Cyber Asset…” This should say “a” Cyber Asset rather than “any” Cyber Asset. The word “associated” (Associated Electronic Access Control or Monitoring Systems, Associated Physical Access Control Systems, Associated Protected Cyber Assets) is used throughout the Standards, but Associated is never defined. The terms Electronic Access Control or Monitoring System, Physical Access Control System, and Protected Cyber Asset are defined, but how is a Protected Cyber Asset different from an Associated Protected Cyber Asset? Description of an Associated Protected (or Physical Access or Electronic Access Control Systems) in the Applicability Section of the Standards states they are …”System associated with a corresponding High or Medium Impact BES Cyber System”. The Definitions document lists Protected Systems, but not Associated Protected Systems. What is a System associated with a corresponding System? Do not understand what these words mean. The Definition of a BES Cyber Asset refers to assets that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. The definition also states: “This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Service”. The key information appears to be that a problem with an asset can adversely impact a BES Reliability Operating Service within 15 minutes. However, it also appears that the occurrence of the initial event has no bearing on this evaluation. Definition would be clearer if it emphasized the impact to one of the BES Reliability Operating Services rather than being rendered unavailable, degraded, etc. “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. Under “BES Reliability Operating Services”: • “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Request clarification of the scope of this “Operational Directives”. Does it include a company’s messaging system? Two-way radios? What is the relationship with the new COM-002? • Request clarification that these Coordination and Communications are limited to Reliability, not Market Systems. • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.

Yes
The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways. Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly-complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced through-out the Standards. One of the BES Reliability Services identified in Att. 1 is Balancing Load and Generation and one of the bullets under it is Demand Response. However the description of Demand Response includes the Ability to identify load change need and the Ability to implement load changes. These criteria are the same as the Manually Initiated Load Shedding bullet and are not criteria we would typically associated with Demand Response. Need a clarification on what Demand Response means in Att. 1 One of the BES Reliability Services identified in Att. 1 is Situational Awareness. Att. 1 seems to define Situational Awareness as what is going on in one's own system whereas Situational Awareness is typically used to describe system-wide awareness. Need clarification on what Situational Awareness means in Att. 1. Need clarification on the role/responsibility of PC, TP, GO, GOP, RC, PA in CIP-002-5, Att. 1, 2.3, 2.8, and 2.9 Comments: Recommend that 2.8, 2.9 and 2.11 start with "Applies to all Regions except…" For 2.8, 2.9 and 2.11 request that the SDT clarify whether the exception is all, or not WECC. In 2.12, "system" and "Facility" are not the proper terms to use. An operator is responsible for automatic load shedding or the other forms of load relief mentioned. For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
CIP-002 requires update to Cyber Asset listing within 30 days of a change "…intended to be in service for more than 6 calendar months…". This is not auditable and we should delete the phrase regarding intentions. Transient Cyber Assets (assets directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset) are a poor security practice. Cyber Assets should not be connected to the protected systems without proper security and controls, whether it be temporary or permanent. For clarity and consistency with the previous change, request changing M1 from "as required in R1 and list of changes to the BES (" to "as required in R1 and list of changes to the BES Elements and Facilities)". Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term "Facilities" in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be "compliant" with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation "requirements" in a guidance document rather than in the requirements in the standard. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are

introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
Yes
No
Regarding CIP-003-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
Yes
Yes
No
The last bullet for M4 on page 12 is inconsistent with R4 since M4 requires periodic training instead of R4’s making staff aware of cyber security policies. Request that M4 be updated to be consistent with R4.
Yes
No
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
No
Comments: Regarding CIP-004-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Recommend removal of

R2.3 and R2.4 since they are redundant to R2.2, or explain the difference between R2.2 and R2.3, R2.4. Request removing “potential” from R2.7 since training should include how to determine whether a BES System Event occurred or not.
Yes
No
For all R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”.
No
For R6.1 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber Systems. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 1. The Responsible Entity should be able to determine the approval process for authorization of access to BES Cyber System Information. 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.6 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I” in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend removing the "following the resignation or termination" since it is redundant and inconsistent with the sibling Requirements. Recommend changing 7.4 from "For resignations or terminations," to "For terminations, resignations, reassignments, or transfers,".
No
The Standards allow systems used for access control or monitoring to be located outside an ESP. It is a poor security practice to locate Associated Cyber Assets/Systems outside an ESP and these assets, if they are protecting BES Cyber Assets and are important enough to protect, should also be located in an ESP Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 Electronic Access Points is the 1.2 identified Electronic Access Points or not? Request clarification that the 1.5 EAP is the 1.2 identified Electronic Access Point or not? Request clarification on 1.5's "at each EAP". Is that inside or outside or both? Regarding CIP-005-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with

requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request Requirement 1.2 be updated to allow "escorted physical access." Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.4 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary. " to "issue real time alerts for detection of breach through an access point". For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6. Regarding CIP-006-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification on what the "Associated" "Applicability" (High/Medium/Low BES Impact) for 3.1 and 3.2 Request capitalization of "locally mounted hardware or devices" in Requirement 3.1 so that it refers back to the defined term "Locally Mounted Hardware or Devices" .
No
Request clarification on 1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on 1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Regarding CIP-007-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have

some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request clarification of "remediation" in 2.2 since it reads that the patch must be applied, which does not allow to have an exception when applying the patch is the worst scenario such as creating a denial of service. For 2.2, suggest wording like "create a remediation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to the patch or the overall process?
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media". The Measure for 3.4 does not match the Requirement.
No
CIP-007, R4.5 requires summarization/sampling of logged events for Associated Systems (access control, monitoring, physical access, protected asset associated with a corresponding High or Medium Impact System), but does not require such protection for a Medium Impact BES Cyber System. How can more stringent controls be required for a system associated with another system than required for the system itself? Or is it just a type that excluded it from R4.5? Request changing 4.1.4 from "Any detected potential malicious activity" to "Any detected malicious activity" since the scope of potential includes all activities. Request clarification on 4.3, does the failure need to be detected within a calendar day? Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. In 4.5 clarification is needed for the associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems?
No
For 5.2, does the CIP Senior Manager or delegate approval policy or procedure for each authorization of access? In 5.2, should the Requirement be interpreted as "each use" as in "The CIP Senior Manager or delegate must authorize the use of each administrator, shared, default, or other generic account types." Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
No
Regarding CIP-008-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
: 2.1 is a new Requirement. Request the rationale for this new Requirement. Recommend changing

from "When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test." to "When a BES Cyber Security Incident is classified or identified, the Responsible Entity must follow its incident response plan." Recommend removing “initially upon the effective date of the standard” from 2.2 of Table R2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered.
No
Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend that 3.2 wording be consistent with the 2.2 wording. For 3.3, recommend changing 1) "Update" to "Update as necessary" and 2) "the completion of the review of that plan" to "the completion of the review performed in 3.2" .
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommend removing Requirement 1.5. Reliability's top priority is restoration of service. Forensics in a recovery mode may not support BES reliability and requiring such actions may negatively impact the BES Cyber System restoration process. Regarding CIP-009-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Recommend that 2.1 be implemented 180 days from the effective date of the Standard. For 2.1, request clarification, is “full operational exercise” the same as “functional exercise” as described in the rationale? For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1 recommend 1) removing “or when BES Cyber Systems are replaced” as it is addressed in CIP-009 R3.4 and 2) removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two

Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Recommend that 3.4 be referenced by CIP-009 R3.1. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.

No

Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." For 1.1, 1.2, 1.3 and 1.4, recommend changing the Requirements to be consistent with their Applicability --- from "For a change to the BES Cyber System" to "For a change to the BES Cyber System or Associated Systems or Associated Assets". Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold. Regarding CIP-010-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.

No

Recommend removing "where technically feasible" from 2.1 since the remaining words should not need an exception.

No

For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Recommend changing 3.2 from "in a production environment" to "in a production environment, or a test environment" to allow Entities more flexibility in meeting this Requirement.

No

Request clarification on 1.1. Some interpret this Requirement as what is the Entity's process for identifying BES Cyber Systems Information. If correct, the Measure should be "show me the methodology (document)." Others interpret these Measures as labeling BES Cyber System Information. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. Regarding CIP-011-1, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. There are potential issues with implementation of CIP Version 4 versus CIP Version 5. As written, CIP Version 5 appears to have some requirements that would be enforceable on the effective date and there may be a need for an implementation and/or conversion timeframe. The words in the Standards

Requirements appear to be at odds with the Implementation Plan and clarity is needed. Additionally, there is concern with the need to be “compliant” with requirements that simply rely on documentation. Documentation is not a mechanism to ensure reliability and/or security of the bulk power system. An approach that should be considered is to have documentation “requirements” in a guidance document rather than in the requirements in the standard.
No
Request that footnote 2 in 2.1 be moved into that Requirement.
No
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Otherwise, this Scenario table is confusing because it repeatedly uses 12 months while the earlier text uses 18 months. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.
Group
Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)
Marianne Swanson
No
Yes
The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has developed a mapping between NERC CIP v5 requirements and the high-level security requirements in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber Security. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf This mapping identifies any gaps between CIP v5 and the NISTIR 7628 high-level security requirements and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were identified. The CIP-002-5 criteria provide a sound approach for identifying low, medium, and high impact systems within the BES. This three level approach aligns well with the three level approach (i.e., low, moderate, and high) used within the NISTIR. Most requirements in the current CIP drafts are applicable to both medium and high impact systems as a bundled pair and they are silent on their applicability to low impact systems. In contrast, the NISTIR uses a graded requirement approach that specifies baseline controls that apply at low impact levels and then specifies strengthened controls for moderate impact and even stronger controls for high impact levels. The CIP version 5 standards will be significantly strengthened if they were to incorporate a similar graded approach when applying requirements.
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.1, to include the concept of “continuous improvement” and best practices (to align to NISTIR 7628, SG.CA-

3, Continuous Improvement).
Yes
Yes
Yes
No
To align with the NISTIR 7628 high-level requirements, CIP should elaborate requirement: R2, 1.3, to include following - 1) Responsible Entity should document document allowed methods of access to the BES Cyber Systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 2) Responsible Entity should incorporate in their policies the usage restrictions and criteria for allowing each remote access (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 3) Responsible Entity should setup authorization procedures prior to granting remote access; 4) Responsible Entity should enforce requirement criteria for providing remote access to the BES Cyber systems (to align with NISTIR 7628, SG.AC-2, Remote Access Policy and Procedures); 5) Responsible Entities shall implement policies and procedures for managing remote sessions in their BES Cyber Systems access control policies and procedures (to align with NISTIR 7628, SG.AC-13, Remote Session Termination); 6) Responsible Entities shall include in procedures and criteria of granting Remote access encryption, authentication of all communication media through limited number of manageable access control points (to align with NISTIR 7628, SG.AC-15, Remote Access). R2, 1.5 to include following - Responsible Entities shall include in their policies and procedures to grant access privileges to their BES information Systems based on minimum privilege justified by the business requirement for access requests (to align with NISTIR 7628, SG.AC-19, Control System Access Restrictions). R2, 1.6 to include details on what the policy should address including objectives, roles and responsibilities, and the the scope of the incident response program, and require the identification and classification of potential interruptions (to align with NISTIR 7628, SG.IR-1, Incident Response Policy and Procedures). R2, 1.7 to specify required elements of the recovery plan (to align with NISTIR 7628, SG.CP-1, Continuity of Operations Policy and Procedures and SG.CP-2, Continuity of Operations Plan). R2, 1.9 to include following - 1) Responsible entities shall restrict access to external information systems or restrict processing, storing or transmitting controlled information through External Information systems over which the Responsible Entities have no control (to align with NISTIR 7628, SG.AC-18, Use of External Information Control Systems); 2) Responsible entities shall have a documented media protection security policy that addresses the objectives, roles, and responsibilities fo r the media protection security program as it relates to protecting the organization's personnel and assets; the scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and procedures to address the implementation of the media protection security policy and associated media protection requirements (to align with NISTIR 7628, SG.MP-1, Media Protection Policy and Procedures); and 3) Requirement that data communications be addressed in the information protection policy (to align with NISTIR 7628, SG.SC-1, System and Communication Protection Policy and Procedures).
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R4, 4.1, to include detailed personnel screening requirement detailed in NISTIR 7628, SG.PS-3, Personnel Screening, as follows: Basic screening requirements should include - a. Employment history; b. Verification of the highest education degree received; c. Residency; d. References; and e. Law enforcement records.
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R6, 6.1, 6.2, 6.3, and 6.4 to include security authorization for granting escorted/ unescorted access permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security). R6, 6.5 and 6.6, to include security authorization for periodic review of permission for performing assigned work functions for contractors and third party providers, including service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management (to align with NISTIR 7628, SG.PS-7, Contractor and Third-Party Personnel Security).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R7, 7.1, to include requirement of exit interview to convey the constraints imposed on the individuals/ contractors/ Third Party Service Providers, due to revocation of privileges caused by change in assignments or termination of job (to align with NISTIR 7628, SG.PS-4, Personnel Termination).
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.2, to identify - 1) specific authentication credential management requirements (initial authentication credential content; administrative procedures for initial authentication credential distribution/lost credentials/lost, compromised, or damaged authentication credentials/revoking authentication credentials; changing/refreshing authentication credentials on an organization-defined frequency; and specifying measures to safeguard authentication credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management); and 2) devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication). R1, 1.3 to identify devices to be identified and authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, to include - 1) The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications; 2) The organization changes the diversity of operating systems and applications on an organization-defined frequency; and 3) The organization employs randomness in the implementation of the virtualization (to align with NISTIR 7628, SG.SC-28, Virtualization Technique). R2, 2.2, to include - 1) cryptographic key establishment and management (to align with NISTIR 7628, SG.SC-11, Cryptographic Key Establishment and Management); and 2) use of FIPS-140-2 approved or allowed cryptography and other security functions (to align with NISTIR 7628, SG.SC-12, Use of Validated Cryptography).
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R4, 4.2, to specify - 1) the use of an automated mechanism to necessitate a real-time alert (to align with NISTIR 7628, SG.IR-6, Incident Monitoring); and 2) receiving security alerts, advisories, and directives from external organizations (to align with NISTIR 7628, SG.SI-5, Security Alerts and Advisories). R4, 4.3, to specify some events that alerts should be generated (to align with NISTIR 7628, SG.AU-5, Response to Audit Processing Failures).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R5, 5.1 to specify devices to be identified/authenticated prior to establishing a connection (to align with NISTIR 7628, SG.IA-5, Device Identification and Authentication). R5, 5.3 to specify requirements for managing authentication credentials for users/devices, including supplemental guidance to safeguard credentials by not loaning/sharing credentials (each individual must be identified for any shared account as opposed to sharing credentials) (to align with NISTIR 7628, SG.IA-3, Authenticator Management).
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.3, to specify - 1) data is reported in compliance with applicable laws and regulations (to align with NISTIR 7628, SG.IR-7, Incident Reporting); 2) external entities that should be considered for not only communication but coordinated effort related to cyber security incidents (to align with NISTIR 7628, SG.IR-11, Coordination of Emergency Response).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, to specify the use of an automated mechanism in response to an incident (to align with NISTIR 7628, SG.IR-6, Incident Monitoring).
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.3, to specify information to be backed up (to align with NISTIR 7628, SG.IR-10, Smart Grid Information System Backup). Information to be backed up includes user-level information, system-level information and system documentation including security related documentation. The confidentiality and integrity of the backup information shall be maintained. R1, 1.3, 1.4, and 1.5 to specify alternate storage sites (to align with NISTIR 7628, SG.CP-7, Alternate Storage Sites) and requirements to recover/reconstitute Smart Grid systems to a secure state (to align with NISTIR 7628, SG.CP-10,

Smart Grid Information System Recovery and Reconstitution).
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R2, 2.1, 2.2, and 2.3, to specify requirements to recover/reconstitute systems to a secure state (to align with NISTIR 7628, SG.CP-10, Smart Grid Information System Recovery and Reconstitution).
Yes
Yes
Yes
Yes
Yes
Yes
No
To align with the NISTIR 7628 High-level requirements, CIP should elaborate requirement: R1, 1.1 to specify - 1) requirements to partition the communications for telemetry/data acquisition services and management functionality. The information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path (to align with NISTIR 7628, SG.SC-2, Communications Partitioning); and 2) requirements to employ underlying hardware separation mechanisms to facilitate security function isolation; and isolate security functions (e.g., functions enforcing access and information flow control) from both non-security functions and from other security functions (to align with NISTIR 7628, SG.SC-3, Security Function Isolation). R1, 1.2 to specify more granular retention requirements as applicable to law/regulations (to align with NISTIR 7628, SG.IA-2, Identifier Management).
Yes
Yes
Yes
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
“BES Cyber Asset” could be improved by reinstating the phrase “and causes a Disturbance to the BES” that was in earlier drafts approved by the SDT. This would also help clarify what the phrase “adversely impacts” means by giving the industry a more concrete basis on which to determine what does/does not fall into this definition. “Situational Awareness” is a major concern because as currently defined its scope is so ambiguous and overly broad that it will inhibit meaningful implementation. Southern suggests adding clarifying phrases such as “wide area” and “for operational purposes.” The bullet point for “Change Management” should be deleted or further refined because this is a very generic term that means many different things to many different people and disciplines. “Control Center’’ has a major flaw in that it includes any facility that houses any BES Cyber Asset that is doing anything for more than one location. As such, the term “Control Center” is ambiguous and overly broad. For example, a master radio located on a pole-top that is aggregating data from more than one substation could be interpreted to be a control center according to this definition. Southern suggests including a more explicit definition that specifically references facilities where system operators are performing the BA/RC/TOP functions and any associated data centers. Southern also

suggests explicitly excluding field locations that aggregate data for use by the control center. “BES Cyber System Information” should add the words “BES Cyber System” in front of the phrase “network topology diagrams” for consistency purposes and to better clarify what types of diagrams are included. Southern also suggests deleting the phrase “or similar” in this definition and throughout the standard to avoid unnecessary ambiguity and confusion. “BES Cyber System” should have the word “Maintenance” changed to “Transient” to match the other definitions in the standard. “CIP Exceptional Circumstance” should have the word “BES” in front of “Cyber Security Incident” to match the proposed glossary term. “External Routable Connectivity” – spell out “ESP” (i.e., Electronic Security Perimeter) in the definition or be consistent with the External Connectivity definition. “Intermediate Device” – spell out “DMZ” (i.e., Demilitarized Zone).

Yes

As an overall comment in CIP-002-5, Southern has three primary concerns centered on (i) the inclusion of distribution assets in the applicability of the standards, (ii) the inclusion of low impact assets, and (iii) the extensive shift in methodology from previous versions of the standards. In addition, Southern suggests the following changes to the bright line criteria and guidance that help clarify the language. Inclusion of distribution assets Southern strongly suggests that the CIP standards remain focused directly on BES reliability. The inclusion of distribution assets in the applicability sections 4.2.1 and 4.2.2 of each of the reliability standards needs to be struck. Low impact assets Low impact assets are problematic in that they are high in volume creating extensive resource needs to comply with the CIP-002-5 requirements and creating a potential distraction from the primary focus of adequately protecting the High and Medium Impact assets. In order to move forward with expedient progress on Version 5, and to not let Low Impact assets distract the industry from adequately protecting High and Medium Impact assets, Southern proposes that Low Impact assets and their requirements be moved to another standard separate from High and Medium Impact assets and requirements. Southern also suggests that inventory and auditability issues with Low Impact systems could be better addressed by removing the Low Impact category and modifying the corresponding programmatic requirements to apply to the Responsible Entities themselves rather than to particular assets. Extensive shift in methodology CIP-002-5 as drafted contains an extensive shift in methodology when compared to previous versions of the CIP-002 standards. The new methodology is generating a significant amount of confusion in the industry. While the proposed approach is different, it is not clear that this change produces a significant difference from what would be protected using the industry approved methodology found in previous versions of the standards. The terms introduced as reliability services are often ambiguous and do not help focus application of the standards. For example, situational awareness is a broadly applicable term and if interpreted broadly has few limits. Therefore, Southern suggests that the SDT build from the Version 4 methodology with appropriate categorization and refinements to address remaining FERC directives and removing the reliability operating services approach. Enhancements to bright line criteria In criteria 1.4, the reference to 2.12 should be 2.13 to correctly include control centers. In criteria 1.3 and 1.4, the “that includes” should be changed to “is limited to” in order to not leave these criteria completely unbounded. Criteria 2.1 with its historical nature needs to account for decommissioned generating units. A unit that would have historically met this criteria but has been decommissioned should not be subject to this standard. Southern suggests adding “commissioned” or “active” to the beginning of the criteria. Criteria 2.5, first bullet should read “Up to and including the first interconnection point of the starting station service of the generation unit(s) to be started”. For criteria 2.7, Southern suggests returning to the industry balloted and approved language that is in CIP-002-4 regarding 345kV with 3 or more lines. Criteria 2.10 needs to be limited to the plant switchyard, otherwise the entire grid could be included. Southern suggests using the phrase “on site facilities”. Additionally, criteria 2.10 needs to include logic similar to R2.5 to determine if there are equivalent independent transmission alternative paths. Suggested changes to the guidance On pg. 25, the Medium Impact Generation bullet that begins Part 2.5 – As worded, this could be interpreted to cover both Generation and Transmission. The Transmission part picks up with the sentence that begins with “The drafting team further …”. Consider moving some of this material to the Transmission section that starts on pg. 27 and refer to it from pg. 25. Also consider moving the cranking path diagrams to the Transmission section that starts on pg. 27 into Part 2.5. On pg. 28, Part 2.7 paragraph – It is not clear how autotransformers in a station should be factored into this calculation. Do autotransformers count as a connection to another station? Does it matter if the autotransformer (including generator step-up transformers) is connecting to a higher voltage level such as 500kV versus a lower level such as 115kV? Please provide guidance on how to treat autotransformers and

GSUs in the calculation. On pg. 29, third bullet, in the 1st sentence in the guidance section for criteria 2.12, Southern suggests changing “are capable of performing” to “perform” which makes it match the actual criteria without adding ambiguity. Additionally, the reference to 2.13 in the second sentence should be 2.12. On pg. 29, the word “Systems” in UFLS and UVLS should be consistently capitalized.
No
Southern is very concerned with R1.1 as it centers on every “change to BES Elements and Facilities”. Southern believes that as currently drafted this requirement will be subject to varying interpretations and will be essentially impossible to implement and audit. For example, it will require some form of master list of every BES change, some determination of whether each change affected any cyber asset and to what degree, and the expected duration of every change to the BES. Southern believes this is an onerous burden and an incorrect approach to place on the industry. Some BES Elements and Facilities are integrated into critical cyber systems. Southern suggests making this impact change determination dependent upon BES Cyber Asset changes which is a much more manageable burden. Otherwise, Southern suggests returning to an annual review or alternatively the addition of a very specific list of BES changes for which the analysis must occur. Southern believes more clarity is needed in R1 on the concept of “its” and “owns”. Cyber Assets could be leased from entities outside the industry who are the “owners” and are not subject to the CIP standards. This may be as simple as changing it to “owns or leases”. R1.1 describes what to do when Facilities are placed “into” service but provides no guidance on what to do when Facilities are “out-of-service”. The SDT should consider a companion R1.2 for when Facilities are “out-of-service” which minimizes administrative overhead and compliance risks and maximizes potential for restoration of service with sound security.
Yes
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement. For instance, the VRF should be used to differentiate between violating the Disturbance Control Standard (BAL-002), and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRF’s should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF’s are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRF’s can be applied.
Yes
No
Southern suggests that all measures should have bullet points rather than sequential numbers. As the measures are examples that “may include”, then the format of the individual items should not suggest that they must all be present. R2 and Measure #2 includes the verb “shall implement” and “and records that indicate the required ten topics were implemented.” This is quite open-ended as anything the entity decides to include in their policy that is above and beyond the CIP requirements could be the source of a violation of this requirement. Proving the implementation of all these policies on all BES cyber assets is overly burdensome on the industry.
Yes
No
The measure suggests the intent of the requirement is to make the policies widely accessible to those who have access to BES Cyber Systems. The requirement as worded, with the phrase “make individuals who have access to BES Cyber Systems aware”, would require tracking to the individual level for every BES Cyber System. With this wording, the provided measures do not meet the requirement. Southern suggests not using the word “individuals” and focusing the requirement on making the policies available rather than making individuals aware.
No

Southern strongly suggests refocusing R5 and R6 requirements on naming the CIP Senior Manager and the activities he's responsible for without the administrative overhead of tracking delegates and delegate authorities in paperwork. Updating the CIP Senior Manager within 30 calendar days of a change is reasonable. R5 and R6 as worded create unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. No other reliability standard requires explicit documentation and tracking of delegation. Delegation is an ordinary business activity. How a company organizes and delegates internally should not be a matter of reliability standards. Alternatively, sufficient language would be any industry approved version of the CIP-003 R2 language.
No
See response to question 10.
No
Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. Lower degrees of severity are often needed within the VSLs. For example, in R3, as written, the VSL is High for a policy that covers all CIP requirements and is also High for a policy that covers one CIP requirement. Therefore, R3 potentially unfairly penalizes entities who have implemented multiple policy documents. Southern suggests (i) basing the R3 VSL on R2 and the number of parts not approved within the required timeframe and (ii) adding additional granularity, rather than the current wording of "not all". Consistent with Southern's response to question 9 above, in R4 Southern suggests not using the word "individuals" and focusing on making the policies available rather than making individuals aware. Consistent with Southern's response to question 10 above, R5 and R6 needs to be re-focused on the CIP Senior Manager and their responsibilities and away from creating and maintaining delegation paperwork. In general, regarding VRFs in each of the CIP standards, it is Southern's understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRF's can be applied.
Yes
No
CIP-004-5 Table R2 is highly repetitive, seems to provide an incomplete start to a role-based training program, and appears to misinterpret FERC Order 706 – paragraph 434. The FERC order does not mandate role-based training, but that "any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security." This can be accomplished in numerous ways. Southern suggests a return to approved language in CIP-004-3 or CIP-004-4 with the directed FERC clarification that "training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity," not just CCAs. This can be accomplished with adding one or more bulleted items to R2.2 in CIP-004-3.
No
In previous versions of the standard, 'Protected Cyber Assets' were only subject to CIP-007 requirements. Version 5 expands on that with requirements such as the CIP-004 R3 training requirement, which also implies that access is tracked to the individual level on these types of Cyber Assets. Southern suggests that the requirements to which Protected Cyber Assets are subject be matched with current practice in current standards.
Yes
No

See reply to CIP-004 R3 (Question #15). In addition, applying this to EACMS without further qualification is problematic. The phrase “authorized electronic access” to an EACM would mean anyone with an ID on that system; essentially anyone who just has a record in the database. There is negligible risk from a person who is just authenticated out of a common ID store if they have no access to the actual BES Cyber Systems and entities should not be required to do PRA’s on every individual in a common ID store. Southern suggests separating this requirement such that administrators of the EACMs require PRAs, but not every person represented by a record in the EACM. If an entity has a directory service or a token authentication service that has CIP and non-CIP user IDs in it, the standard would not apply to people with no BES Cyber System access.
No
In Parts 6.1 and 6.3 the requirement for the CIP Senior Manager or delegates of the CIP Senior Manager to authorize access should be eliminated. Consistent with answers on questions 10 and 11, Southern strongly suggests focusing requirements on security requirements and results without the administrative overhead of the CIP Senior Manager or his delegates approving all access in paperwork. R6, Parts 6.1 and 6.3 as worded creates unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. Alternative language would be any industry approved version of the CIP approval language. It is strongly suggested that access review requirements use the model of R1.3 in CIP-011-1 rather than the ‘zero defect’ model they currently employ. Southern believes the desired behavior is to “find, fix, repeat” rather than having compliance violations levied for finding and fixing errors. The requirements should require entities to “self-audit” on a periodic basis, complete with remediation plans and deadlines for mitigation of issues found. If the above approach is not taken, then an issue arises in 6.4 – 6.6 where any access that was provisioned in error but never used is a violation. There is a paragraph in the included guidance that says this should not be considered a violation, but guidance does not override what the requirement plainly states. Southern suggests changing the language to be based on “users who used their access” to more closely match the intent. Throughout this requirement, it uses the phrase “Access permissions shall be the minimum necessary for performing assigned work functions.” Southern believes this to be overly onerous to audit (if not essentially unauditable to prove every access right on every cyber asset for every individual is necessary for some work function). Southern believes this phrase is unnecessary as the point of the authorization is to insure that there is a need for the requested permissions. Auditing to the authorization we feel is sufficient and the phrase should be deleted. More explanation is needed on the difference between R6.4 and R6.5. R6.5 appears to be a superset of R6.4 and both are performed on the same timetable. Measure (iv) in R6.5 appears to cover R6.4. Southern suggests deleting R6.4.
No
The standard addresses numerous forms of employee status changes, but does not address employee retirements. The included guidance suggests that access revocation for retirement should occur “day of”, but the requirement itself does not seem to allow this. R7.2 is problematic in that most in-company job transfers in some large organizations occur on the weekend (Saturday). If the person is remaining a trusted employee and is just transferring jobs, is there sufficient risk to require that all the access be revoked on Sunday? Southern suggests changing the timeframe to allow for weekend transfers. R7.3 is problematic for audits. How does an entity prove that access to every piece of BES Cyber System information, including paper prints, has been revoked? Southern suggests changing the language to “revoking access to areas designated for BES Cyber System Information”. This is still problematic, but much less so, and is language already contained within the change rationale in the requirement.
No
Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe and as worded may work against desired behavior. For example, R3 needs to be written to promote the desired behavior of “find, fix, repeat” rather than having compliance violations levied for finding and fixing errors. The R3 VSL should be reworded to account for evidence of periodic review and promptness in fixing errors, if any, once detected. In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take

into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRF's are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.

No

R1.1 needs to be made explicit that the Low Impact systems can have their electronic access controls documented as a group or at a site level. Southern suggests changing the Applicability to "Responsible Entities" rather than Low Impact systems as that requires an audit at a system or device level. R1.3 should make it explicit that the responsible entity determines the "explicit criteria". Leaving this unaddressed leaves the requirement open to audit interpretation.

Yes

No

Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. For example, as currently drafted CIP-005-5 has only Severe violations meaning any violation of a requirement is a Severe VSL. Additional thought needs go into what would really constitute a Severe violation and what should be lower severity levels or no violation. For example, in R2, configuration errors or necessary temporary conditions should be a lower severity level or no violation than not implementing an Intermediate Device at all.

No

In previous versions of the standard, "Protected Cyber Assets" were only subject to CIP-007 requirements. Version 5 expands on that with several requirements in CIP-006. The requirements assume that all PCAs are within the same Defined Physical Boundary with their associated BES Cyber Systems. Southern suggests that the requirements to which Protected Cyber Assets are subject be matched with current practice in current standards.

No

In Table R2, Part 2.2, Southern suggests deleting "a per 24-hour basis" which may be confused with continuous logging of an individual within a perimeter. Additionally, consider modifying the language to logging date and time of "initial" entry and "work completed or final" exit to reduce administrative burden if someone has to repeatedly move into and out of a perimeter to get the work done. Continuous escort of visitors within the perimeter is already required. Examples include pulling cabling, working on an access point itself, or moving volumes of equipment into a perimeter.

No

In Table R3 Part 3.2, due to the redundancy and/or robust design present in physical access control and monitoring systems the term "failure" and "systems" creates ambiguity and confusion. One component of an access control system can fail, but access control at the access point continues to operate as designed. Southern suggests striking "failure" as outage reflected in the current approved standards is sufficient. Additionally, logging date and time of an outage implies duration is a calculated and redundant (stop time - start time). Southern suggests the following wording: "Log dates and times of outages of Physical Access Control or Monitoring Systems." The term "outage" should specifically exclude routine maintenance activities such as replacing a battery or a badge reader.

No

Southern has a general concern that Violation Severity Levels are routinely biased towards High and Severe. A review of the violations of CIP standards could shed additional light on those types of activities that companies are being sighted for at audits, and that the VSLs can and appropriately account for those violations. In general, regarding VRF's in each of the CIP standards, it is Southern's understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form "Do X" to all of "these systems" and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be

accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
Yes
Yes
The Change Rationale needs to be updated to more closely reflect the requirement.
Yes
No
The “at a minimum” is problematic and Southern suggests deleting it. The requirement has a defined list of what must be included so the “at a minimum” phrase adds nothing to the requirement. R4.1.1 needs clarification on the issue of dropped packets at an EAP. Is a dropped packet that did not meet an explicit access rule a “‘failed access attempt”? This and R4.1.4 are problematic for Internet-facing systems as maintaining such logs (of “noise”) is overly onerous. The requirement does not allow for differentiation in environments where mostly noise is expected vs. environments where no noise is expected.
No
In R5.1, change the word “granting” to “permitting” to more closely match the intent. In the remainder of the standard, authorizers grant authorized access. R5.4 is very problematic from an audit perspective for Low Impact BES Cyber Systems. Southern strongly suggests that this be required only on High and Medium Impact systems. R5.5.3 is problematic from an implementation and an audit standpoint. Version 5 requires strong physical security and greatly enhances the electronic remote access security. Southern believes with these enhancements in perimeter security on remote devices (some of which may be pole mounted or have an easily accessible password bypass jumper) that the password change interval requirement should be removed until technology allows for more central management of such devices. As more and more field devices are pulled into scope, this requirement becomes onerous quickly with little reduction in risk.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
Yes
Yes
No
Southern believes R3.4 goes well beyond the changes required from paragraph 686 of Order 706 and would be overly onerous to prove in an audit. This would require a list of all organizational or technological changes with an analysis of which impacted any cyber security incident response plan and then prove those plans were updated in response to those changes.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and

violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
R1.4 needs clarification as to whether the backup media must be verified (what the requirement states) or if it requires verification that the backup process completed successfully (what the measure says). If it is the former, then verifying multi-terabyte backups is prohibitive. Also, as a “system” level requirement, backup and verification of every individual component (a network hub for instance) is not feasible.
No
R2.2 is problematic in that it requires the entity to verify current configuration against a year old backup. Testing all backup media (multiple tera- if not petabytes) is onerous. It is also overly onerous to test every backup from every system annually. Is the standard actually requiring testing 365 backups per system if it has daily backups? The entities will spend an order of magnitude more time verifying backups than it takes to perform the back ups.
No
R3.4 would be onerous to prove in an audit. This would require a list of all organizational or technological changes with an analysis of which impacted any recovery plan from any cyber system and then prove those plans were updated in response to those changes.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
In general, CIP-010 should be re-focused towards defining, approving, maintaining, and verifying cyber security controls for the various BES Cyber Systems. The CIP standards themselves suggest that items included as a part of the security controls baseline (R1.1) would include an assessment of the OS and security related patch levels, of application software and security related patch levels, of logging enabled, of anti-virus enabled and definitions updated, of default accounts and passwords appropriately configured, and ports and services reflecting the baseline for the BES Cyber System as appropriate. Without re-working the entire proposed CIP-010 standard, which the SDT may need to consider, Southern recommends certain enhancements to the requirements below. Southern believes that the SDT has over-interpreted FERC directives and overly constrained needed flexibility in implementing the standards, particularly in Table R3. Southern suggests that the SDT review FERC directives again before making any significant changes from the industry approved CIP version 4 language. The Rationale – R1 should be re-worded to exclusively prevent unauthorized “security controls related” modifications to BES Cyber Systems. Changes not impacting security controls should be beyond the scope of the CIP standards. In Table R1, Requirements column, the requirement should be re-worded to focus on a baseline “security controls” configuration. In Table R1, R1.1.1. Physical location is not a configuration item for most if not all cyber devices. Few cyber devices know or contain a parameter to configure location. Additionally, we are already required to secure devices within a Defined Boundary according to CIP-006-5 R1 which creates double jeopardy by including this item here. Physical location should be removed from the listing. In Table R1. R1.1.3. Southern

suggests the removal of the term “commercially available” and then R1.1.4 could be deleted as R1.1.3 will cover both. R1.2 needs to clarify the SDT’s intent as to temporary changes. For example, temporary scripts may be used on a cyber asset to help troubleshoot issues. Southern would strongly suggest deleting R1.1.4. If 1.1.4 must be included then it should be scoped to those scripts which impact the security controls, not all scripts. R1.2 generates a lot of confusion in that in R1.1, we define a security controls baseline on paper, then in R1.2 we jump to changes to devices without a clear linkage between the two. Southern suggests bridging the issue by rewording R1.2 to approve changes to the documented security controls baseline in R1.1 within 30 days of a change to the BES Cyber System or to the baseline and staying away from device level change management at this point in the standard. As previously noted, authorization by the CIP Senior Manager or delegate is unnecessary, burdensome, and should be removed. Southern strongly suggests refocusing CIP-004 Version 5 R5 on naming the CIP Senior Manager and the activities he’s responsible for without the administrative overhead of tracking delegates and delegate authorities in paperwork. CIP-004 version 5 R5 and CIP-010 R1.2 creates unnecessary paperwork and administratively burdensome tasks that provide no enhancement to BES security. No other reliability standard requires explicit documentation and tracking of delegation. Delegation is an ordinary business activity. How a company organizes and delegates internally should not be a matter of reliability standards. Alternatively, sufficient language would be any industry approved version of the CIP-003 R2 and R6 language. R1.4 is acceptable as written assuming suggestions in 1.1-1.3 above are adopted. This is where changes impacting security controls come into play. Since changes impacting security controls must also be approved, Southern suggests adding a requirement 1.4.4 “changes to BES Cyber Systems which cause a deviation from the existing baseline security controls configuration must be approved.” R1.5 change rationale is misguided in that FERC directives do not mandate security controls testing in a test environment but allow for it. This requirement should and can be deleted. Security controls testing can be effectively and safely performed in a production or test environment and the utility is best able to determine which environment is suitable best on their own tools, capabilities, and knowledge of their systems. Requirement 2.1 should be re-written as to not create technical feasibility exceptions. Consider, “Indicate in your baseline security controls configuration which items are actively (through alarming or active automated monitoring) or periodically (through a manual check) monitored. Security controls BES Cyber Systems must be monitored prior to or in conjunction with implementation, and at least once within a calendar year, unless retired.” Consider adding a requirement 2.2, “Identify deviations from the authorized security controls baseline (through requirement 2.1) and document how the deviation was resolved.” The rationale for this change is that the requirements are clear and measurable, meet the intent of FERC directives, and model the correct behavior for fixing security control related issues.
No
Southern suggests that R2.1 would be more appropriately limited to High Impact BES Cyber Systems only. Applying this requirement to Medium Impact, which incorporates an order of magnitude more field assets, will generate numerous TFEs. Requirement 2.1 should be re-written as to not create technical feasibility exceptions. Consider, “Indicate in your baseline security controls configuration which items are actively (through alarming or active automated monitoring) or periodically (through a manual check) monitored. Security controls BES Cyber Systems must be monitored prior to or in conjunction with implementation, and at least once within a calendar year, unless retired.” Consider adding a requirement 2.2, “Identify deviations from the authorized security controls baseline (though requirement 2.1) and document how the deviation was resolved.” The rationale for this change is that the requirements are clear and measurable, meet the intent of the FERC order, and model the correct behavior for fixing security control related issues.
No
R3.2 should allow for the active vulnerability assessment to occur in production environments where the entity has determined it is safe to do so. It should not be limited to test environments only. Is the intent of R3.3 that a new cyber asset would have a vulnerability scan run against it or that somehow the cyber security controls would be tested? With the proposed changes above in questions 43 and 44, Table R3 is no longer needed and can be deleted. As written, it is confusing, wordy, and appears to misinterpret the FERC directives. However, the intent of 3.4 can be preserved as a part of the proposed 2.2 above in question 43.
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF

is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
Overall, Southern suggests that the BES Cyber System Information related access requirements in CIP-004 be placed in CIP-011 so that the entire Information Protection program requirements are in one standard.
Yes
No
In general, regarding VRFs in each of the CIP standards, it is Southern’s understanding that the VRF is supposed to measure the impact to the BES from the violation of a particular requirement and is used to differentiate between violating the Disturbance Control Standard (BAL-002) for instance, and violating a requirement to have a signature on a document. However, CIP standards have requirements that are of the form “Do X” to all of “these systems” and the VRF is very dependent on the system involved. VRFs should be able to take into account the predetermined impact level of the system on which the violation occurred. For example, an entity should not be accessed a High VRF on a violation of a requirement against a known Low Impact cyber system. However, currently the VRFs are assigned per requirement, regardless of what that requirement applies to. NERC should either take the impact of the cyber system into account on VRF determination, or the SDT should split the requirements so that appropriate VRFs can be applied.
No
It’s not clear what an 18-month implementation timeframe is based on. And, depending on the final language of Version 5, it may not be possible to fully implement Version 5 in the allotted timeframe. Parallel implementation paths or overlapping implementation timeframes with CIP Version 4 or the just the significant change in methodology from CIP-002-3 to the drafted CIP-002-5, will probably create a situation where some or most but not all can reach full compliance with this aggressive implementation plan. Therefore, Southern suggests that the SDT consider creating an exception process, as reviewed and agreed to by the regional entity, to establish the compliance deadline for some assets for good business reasons. As stated in question 2 and reiterated here, Southern suggests that the SDT re-consider making significant changes to the CIP-002-4 asset identification methodology which will also help speed implementation of Version 5 by building on previous versions of the standards and our existing experiences. The notion of planned and unplanned change needs to be better explored. In addition, unplanned change needs to be better defined. It is difficult to envision an unplanned change to the BES except during exceptional circumstances. At the same time, it is easy to envision unplanned changes to cyber systems to address real-time issues. The implementation plan is not fully clear on how to determine if a change is planned or unplanned and creates incentive for change to be categorized as “unplanned.” Southern suggests that the correct position is for cyber assets to be treated as if they are in-scope during commissioning and be fully compliant in parallel with commissioning whenever possible. However, Southern also suggests that the SDT consider creating an exception process, as reviewed and agreed to by the regional entity, to establish effective compliance deadlines for some assets for good business reasons. Alternatively, consider a defined at least 24 month period to reach full compliance for existing and new assets. Additionally, consider 12 months for all changes.
Individual
David Grubbs
City of Garland
Yes

Under the definition of BES Reliability Operating Services under the section titled "Balancing Load and Generation" in the first sentence the words "in the operating planning horizon" should be deleted. This time horizon is well beyond the 15 minute effect as described in the Standards.
Yes
Under Section 4.1.2 Applicability on page 5, and again in section 4.2.2 on page 6, for DPs it states "Transmission Operator's restoration plans" that is very broad. Should be limited to paths used in the TOP Black Start Cranking Paths and facilities identified under Attachment 1, item 2.5 except for the voltage such as substations operated at 69 kV.. Under Section 4.2.4 Exemptions, page 6, should specifically exclude telephone systems and other voice communications systems that are not located within an ESP On the Figure on Page 7 The word Protected needs to be included (ie "Version 4 Protected Cyber Assets") in the title above both halves of the of the figure. Under Attachment 1, Item 1.3 and 1.4, the criteria for determining which control centers should be under the high category the 2.4 Black Start Resources should be under Transmission Operator Control Centers not under Generator Operators since under the EOP standards during Restoration such units are under the control of the TOP not the GOP/BA. Any cyber control by the GOP is minimal. On page 8, under Real Time Operations, do not agree with the last sentence that- says that "redundancy does not mitigate cyber security vulnerabilities." There is some level of redundancy with multiple technologies that could mitigate any vulnerability.
No
Under R1.1 believe that the 30 days should be extended to 60 days and that the 6 calendar months should be extended to 12 calendar months due to delivery times of replacement equipment. Temporary connections frequently last 9 to 11 months during construction activities.
No
Should state "not later than the effective date" not specify "upon the effective date". Approval should not be on a specific single date. This applies throughout all of the standards where this phrasing is used.
Yes
Yes
Yes
No
Should state "not later than the effective date" not specify "upon the effective date". Approval should not be on a specific single date. This applies throughout all of the standards where it is used.
No
This should not apply to visitors – should read “shall make individuals who have authorized unescorted access…”. Visitors, although potentially have physical access to BES Protected Systems, should not need to be trained prior to entry, only their escorts need to be trained.
Yes
Yes
Note the typo. There is an extra "2" at the end of the sentence.
No
A general comment for many of the CIP Standards. It appears that most of the VSL are of the High and Severe Category. Many of these violations should be in the LOwer or Moderate VSL, particularly those dealing with paperwork.
Yes
Yes
No

Under R3.1 should require training only for "unescorted" access.
Yes
Yes
Yes
No
Table Part 7.1 It is impossible to always revoke access upon the termination date or resignations in the cases where multiple companies are involved. We cannot enforce this in 3rd party companies. Additionally, it is impossible to immediately change locking mechanisms in remote substations that are spread across large geographical regions. Many substations have multiple utilities utilizing the same control house. Keeping track of every employee in every support company is not practical and will reduce reliability. For High Impact Facilities terminations the next business day is practical. For resignations seven or days is reasonable. For Medium Impact facilities which may require driving to the remote site several days may be needed to get to all facilities. Table Part 7.2 While this may work in a control center, it is not practical or reasonable in transmission substation settings, particularly for devices that are not remotely connected. Please Note: Promoting someone or transferring someone does not make that person a security risk and should not be treated as such. Believe Medium Impact systems should have 30 days or more to complete since may require onsite trips to reprogram every device at the remote locations. Reprogramming and testing may take several days at each location. The better solution would be to use the same wording as in part 7.1 and only require "removing unescorted physical and Interactive Remote Access to BES Cyber Systems." This is possible by the following day. If this is adequate for terminated employees why shouldn't this be adequate for transferred employees.
No
Not all violations are High or Severe
No
Comments: Table Part 1.5 IDS should not be required - a firewall should be sufficient.
Yes
No
No
Table 1 – Strike “egress” from measures – egress is not stated in the requirement Clarify if this means that a substion employee working all day in a control house can just swipe a card once and then go in and out without reswiping the card as a visitor is allowed or does this require swiping a card every time he crosses the Defined Physical Boundary
Yes
Yes
No
No
Table 1 Part 1.1 – Need provision for TFE Table 1 Part 1.2 – Need provision for TFE A general comment that many of these requirements throughoout all of the proposed CIP standards, while practical in a PC or Control Center environments are not practical in substation and generation environments. Need to have the ability to request a TFE for many requirements.
No
Table 2 Part 2.1 – remove comma after the word “patches,” - the comma in the sentence requires that all software patches be included whether they are security related or not. Additionally, it is not

practical to include firmware as very few vendors post when firmware updates become available
No
Table 3 Part 3.3 – needs to define when the 30 days start – when the EMS vendor says it can be applied or when the virus definition manufacturer says it is available. Additionally, needs provision for TFE in case the virus definition kills the application. Table 3 Part 3.5 – should not apply to USB memory devices, CDs, test equipment in the substation, etc – if it does, requirement should be struck as this would be extremely burdensome. Logging connections does not prevent any introduction of malware.
No
Table 4 Part 4.1 – Although this may be practical for PCs, many substation devices do not have any logging capability at all – need ability to file TFE Table 4 Part 4.1.1 – Electronic Access Points should be addressed under CIP-005 Table 4 Part 4.1.4 – use of the word “potential” is vague and is not auditable The Application Guidelines indicate this is not required for devices that do not support logging. This is not what the requirement states. If this is what is meant then the requirement needs to state it. Table 4 Part 4.3 – strike “before the end of the next calendar day” – end sentence with “failures” Table 4 Part 4.5 – strike 4.5 completely – it is a duplication of 4.2 and 4..3
No
Requirement 5.6 would make a denial if service attack on an asset much more successful if someone could go down the list of accounts and access the account until locked out on all accounts. Would be better to alert for event rather than lock out.
No
should have lower and moderate VSLs
Yes
No
A Cyber Security Event may be totally different than anticipated in the plan. Flexibility needs to be allowed to respond to the event regardless of what is in the plan.
No
Table 3 Part 3.1 – Consider rewording so that the initial incident response plan implementation is no later than the effective date and the review and update is conducted during the initial calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
No
Table 1 Part 1.5 – should be struck completely – preservation of forensic evidence should never take priority over the restoration of the BES. At most should state that "to preserve evidence if it does not adversely affect the restoration of the system"
No
Comments: Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 2 Part 2.2 – remove the word “any” from the requirement. That could require reloading EVERY piece of information stored. Every daily backup tape, etc. Table 2 Part 2.3 – should be struck as it is a duplication of 2.1 – problems with 2.3 as written are what constitutes a full operational test of the plan – is it sufficient to reload one server or one workstation or replace a card in a computer? Additionally, if there are 4 scenarios written in the plan, do you have to do an operational test of each scenario?
No
Consider rewording so that the recovery plan implementation is no later than the effective date and updated once each calendar year. Table 3 Part 3.4 – change from 30 days to 60 days
No
No
Do not believe physical location is required. Table 1 Part 1.4.2 – strike “availability” – “availability” is a business function, not a security function – question – if you make 40 changes in a year and

“availability” goes down 1% (if you can determine that), how do you verify
No
Table 2 Part 2.1 – Should not be applicable to Medium Impact BES Cyber Systems unless they are remotely connected. For non-networked equipment this is an unreasonable requirement. Although it is Technically Feasible to have someone continually log on to the device every hour or every day to see if a change has been made this is impractical.
No
Consider rewording so that the implementation is no later than the effective date. Table 3 Part 3.2 – strike completely – 3.1 should be sufficient
No
No
COnsider rewording to no later than the effective date.
No
The requirement needs to be further clarified.
No
Many of the application guidelines interpret the requirement significantly different than I read the requirement. I request that the application guidelines be made a part of the standard and allowed to be used as a defence. I am afraid that auditors will use the requirement without the explanation or exemptions that are included in the Guidelines and audit to the language of the requirement. Where they can be interpreted differently the language in the Application Guideline needs to be included in the requirement or at least made equal in enforcement with the requirement.
Yes
I do not have any problem with the implementation plan but believe that those without entities that do not have a regulatory body would. Regulatory approval generally takes 6 to 15 month or longer. I believe that the effective date for non-regulated entities should be at least 6 to 12 months longer after BOT approval than after regulatory approval for regulated entities.
Group
ISO/RTO Council Standards Review Committee
Christine Hasha
Yes
Refer to additional comments submitted for Question 49. CIP Exceptional Circumstance: Request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” The definition needs some flexibility for entities to take appropriate measures without risking reliability of the BES that may not fit neatly into the conditions listed. Reportable BES Cyber Security Incident: Request that the drafting team keep this definition consistent with the efforts of the 2009-01 project team. The current definition does not align to the requirements listed in the new version of EOP-004. Intermediate Device: Recommended changes: “A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the Interactive Remote Access; 2) may be a termination point for required encrypted communication; and 3) may restrict the Interactive Remote Access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside an Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.” Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access may be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants. BES Cyber Security Incident: “Suspicious” is not an auditable term, and should be removed. What is an “attempt”? What attempts are serious enough to justify having to be reported? The definition should be made to read: BES Cyber Security Incident A malicious act that: • Compromises the Electronic Security Perimeter or

Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System, or • Results in unauthorized physical access into a Defined Physical Boundary. BES Reliability Operating Services: “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet • Recommend clarification that “Facility” is the NERC Glossary term--in “facility operational data and status” under “Inter-Entity Real-Time Coordination and “Communication”: • Recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" • For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret.
Yes
• For 2.12, request that “system” be capitalized as it appears to align properly with the NERC definition. Also, recommend removing “as required by is regional load shedding program”. • For 2.3, 2.8, and 2.9, need to clarify the role and responsibility of PC, TP, GO, GOp, RC and the PA on impact ratings. Who is responsible for assets being improperly categorized? What avenues are there for appeal?
No
Regarding CIP-002-5, the Applicability sections of CIP-002-5 through CIP-011-5 should be consistent. Note that CIP-005-5 and CIP-006-5 sections 4.2.2 are different from the other Standards. The capitalized term “Facilities” in Section 4 needs to be clarified. Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1. This question applies to the Applicability sections of CIP-002-5 – CIP-011-5. Regarding 1.1, suggest a grammatical fix: “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation…” The word “intended” should not be used in the requirement because it is not auditable. Request it be replaced with “planned”. M1: This sentence needs to be clarified. It appears to require documentation of the low impact assets though this is not required. “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” Request changing M1 from “as required in R1 and list of changes to the BES” to “as required in R1 and list of changes to the BES Elements and Facilities”. The process to classify and categorize cyber assets (CIP-002) and then identify other assets which must be protected (CIP-005 and CIP-007) is excessively complicated. In addition to the BES Cyber Assets that are classified as high, medium, and low in CIP-002, the other standards introduce 10 additional categories of assets to protect in various ways: • Associated Physical Access Control Systems • Associated Protected Cyber Assets • Associated Electronic Access Control or Monitoring Systems • Electronic Access Points (with External Routable Connectivity) • Electronic Access Points (with dial-up connectivity) • Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries • Transient Cyber Assets • Medium Impact BES Cyber Systems with External Routable Connectivity • Medium Impact BES Cyber Systems at Control Centers • Low Impact BES Cyber Systems with External Routable Connectivity Some of these assets are defined in the Applicability Section of the standard (which will not be included in the final standard) while some are introduced in the standards themselves and these categories may or may not be included in the definitions document. This approach is overly complicated and does not allow the CIP Standards to stand alone without dependence on other documents. This also leads to the need for future questions, interpretations, CANs, etc. The Standards should be revised so that all assets which need to be protected are defined in CIP-002 rather than introduced throughout the Standards.
Yes
Recommend adding the following: “…has had its CIP Senior Manager or delegate review and update…”. Request that “initially upon the effective date…” be revised to not require all approvals on the effective date of the standards. It is not practical to expect all documentation to be approved precisely on the effective date.
Yes
Yes
Yes
Request clarification of the meaning of “implement” M2.2.

No
Suggested change: “Each Responsible Entity shall review each of its cyber security policies and obtain approval of the policies by its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” As written, the requirement appears to require approval of the CIP Senior Manager rather than of the policies.
Yes
No
Suggested change: “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved by the CIP Senior Manager and shall specify the authority that is being delegated.”
Yes
The requirement has a typographical error. Footnote 2 is not in superscript. Request clarification that R6 does not require re-delegation when the CIP Senior Manager changes. Request change from “Changes to the CIP Senior Manager and” to “Changes to the CIP Senior Manager or”.
Yes
Yes
No
Request clarification of whether personnel with access to only protected information need training/awareness. SDT should include this as an additional requirement. Request that the differences between R2.2, R2.3, and R2.4 be detailed.
Yes
No
For all measures related to R4 table entries, recommend changing “documented risk assessment program” to “documented personnel risk assessment program” to avoid confusion with a corporate risk assessment program. For R4.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For clarity, recommend changing 5.1 from “authorized electronic or unescorted physical” to “authorized electronic or authorized unescorted physical”. For R5.2 recommend adding language to “grandfather” previous seven-year criminal checks executed for the previous version of CIP Standards. The additional language should spell out when this “grandfathering” expires, which is also when a new check will be required.
No
For R6.1 2. Change “authorize electronic access, except” to “authorize electronic access to BES Cyber Systems, except” 3. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.2 similar comments to R6.1, except that this requirement already refers to “BES Cyber Systems.” 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For R6.3 2. Change “minimum necessary” to “minimum that the responsible entity considers necessary”. For 6.4, request clarification of whether variances noted in the verification would be required to be a self report. For R6.5, Change “minimum necessary” to “minimum that the responsible entity considers necessary”. Request clarification of whether variances noted in the verification would be required to be a self report. For R6.6 Request clarification of whether variances noted in the verification would be required to be a self report. 1. Change “minimum necessary” to “minimum that the responsible entity considers necessary” in the Requirement. 2. In the measure for 6.6, change “BES Cyber System information” to “BES Cyber System Information” – capitalize the “I”

in Information.
No
Request that the footnote for 7.1 be moved into the requirement. Recommend changing 7.2 to "For an individual, no longer acting in a role requiring unescorted physical access or electronic access to BES Cyber Systems, unescorted physical access and Interactive Remote Access will be removed within the next calendar day." Recommend changing 7.3 to “For resignations or terminations, revoke the individual’s access to BES Cyber System Information by the end of the next calendar day following the date of termination.”
Yes
No
Request clarification on the scenario where Low Impact BES Cyber Systems are mixed in the ESP with High/Medium BES Cyber Systems. Is this Low Impact BES Cyber System subject to 1.1 or 1.2? Request clarification that the 1.3 and 1.5 Electronic Access Points are the Electronic Access Points identified in R1.2.
No
Recommend changing 2.1 from "Require an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset." to "Do not allow the Cyber Asset initiating Interactive Remote Access direct access to a BES Cyber System or a Protected Cyber Asset." since the existing Requirement is too prescriptive and does not allow new technology. Recommend changing M2.3 from "Note that a UserID is not considered an authentication factor" to "Note that a UserID and password are not considered two authenticating factors" since the existing words are incomplete.
Yes
No
Request clarification of 1.1 Applicability since it does not identify which of High/Medium/Low BES Impact these are "Associated" with. Request Requirement 1.2 be updated to allow "escorted physical access." Request that Measure 1.2 be consistent (not add a Requirement) with Requirement 1.2, specific to "ingress and egress". Request clarification of Requirement 1.3 "Utilize two or more different and complementary physical access controls" is this multi-factor authentication such as key, badge, keypad or bio-metric? Request that Measure 1.3 be consistent (not add a Requirement) with Requirement 1.3, specific to "ingress and egress" Request changing Requirement 1.4 from "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access through any access point in a Defined Physical Boundary " to "Issue real time alerts (to individuals responsible for response) upon detection of a breach through an access point". Request similar changes to R1.5. For consistency, recommend removing "applicable" from "protecting applicable BES Cyber Systems" in Requirement 1.6.
No
Recommend removing "continuous" from "Require continuous escorted access of visitors" so that the Requirement is auditable from Requirement 2.1. Recommend changing 2.2 from "the entry and exit on a per 24-hour basis," to "the entry and exit to the Defined Physical Boundary on a per 24-hour basis, ".
No
Request clarification of 3.1 and 3.2on what the "Associated" under "Applicability" pertains to (i.e.: High, Medium, or Low BES Impact).
Yes
No
Request clarification on R1.1, is this at the BES Cyber System level or at the Asset level or can the Entity choose? Request clarification on M1.1, why does the Measure refer to BES Cyber Asset while the Applicability refers to Systems? Recommend that “of BES Cyber Assets” be removed.
No

Request clarification of "remediation plan" in 2.2. Suggest wording like "create an implementation plan or a plan to mitigate the vulnerability where it is determined that the patch cannot be safely applied". What is the intent of CIP Exceptional Circumstances in 2.3? Is it intended to mean deviating from the remediation plan in 2.2? Is the "process for remediation" specific to each patch or the overall process? Recommend removing “CIP Exception Circumstances” since the conditions in the definition do not align with the circumstances that may prevent the implementation of the patch. Suggest wording like "process for completion of the defined implementation plan or a plan to mitigate the vulnerability if it is determined that the patch cannot be safely applied".
No
Request allowances in 3.3 for signatures/pattern updates that cause trouble. Suggest adding “Create a plan to mitigate the vulnerability where it is determined that the signature or pattern update cannot be safely applied.” Recommend changing 3.4 from "Transient Cyber Assets and removable media" to "Transient Cyber Assets or removable media".
No
Suggested wording: “Upon detection, activate a response to event logging failures before the end of the next calendar day. Request the rationale of 4.5's "two weeks". Recommend one month as a compromise between the prior version's 90 days and the suggested one week. Request clarification for inclusion of associated protected cyber assets. Are these protected cyber assets associated with only high impact BES cyber systems, or could they be associated with medium impact BES cyber systems? Request clarification of whether variances noted in the review would be required to be a self report.
No
For 5.2, does the CIP Senior Manager or delegate approve policy/procedure for each authorization of access or each actual use/login of the account? Request clarification of 5.5.3, specifically "the significance of passwords in the set of controls used to prevent unauthorized access to the BES Cyber System and existing service agreements, warranties or licenses."
Yes
Yes
No
For 2.1, recommended wording changes; "When a BES Cyber Security Incident is identified or tested, the incident response plans must be used and include recording of deviations taken from the plan." Recommend removing “initially upon the effective date of the standard” from R2.2 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Please ensure that R2.3 aligns with the Evidence Retention section of the standard. Due to audit schedules, the entity may be required to retain the information for more than 3 years.
No
Recommend removing “initially upon the effective date of the standard” from 3.1 of Table R3 because it unrealistically forces an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering is not considered. For 3.3, recommend changing "Update" to "Where necessary, update”. Recommend changing "the completion of the review of that plan" to "the completion of the review performed in 3.2".
No
The VSLs need to align with the requested changes in questions 34-36.
No
For 1.3, request clarification of the “protection of information”. Is this integrity, availability or other information protection such as access controls, encryption? For 1.4, request clarification, is this a backup media verification process? If not what is the intent? Recommended change: “When backing

up Information essential to BES Cyber System recovery, verify the media to ensure that the backup process was successful.”
No
For 2.1 and 2.3 of Table R2 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 2.1, request change to “functional exercise” rather than “full operational exercise”. This is consistent with the information provided in the rationale. Recommend that 2.1 and be implemented 180 days from the effective date of the Standard. For 2.2, request clarification that “any information” may be a sample and not all or each type of information. Does backup media include all media used in the recovery process such as vendor media? What does current configuration mean, as this may never be current? In 2.3, request 1) a definition of “operational exercise” and 2) clarification of “representative environments”. What is the scope, all network devices, systems and items that make up the BES Cyber System? This appears to be a new requirement as paper drill does not appear to be supported. Recommend this shall be implemented 180 days from the effective date of the Standard.
No
For 3.1, recommend removing “or when BES Cyber Systems are replaced” as it addressed in CIP-009 R3.4. Recommend removing “and document any identified deficiencies or lessons learned” as they are addressed in CIP-009 R3.2 and R3.3. Recommend that 3.4 be referenced by CIP-009 R3.1. For 3.1 of Table R3, recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. Request that 3.3 be updated to be consistent with CIP-008 R3.3 for sixty days. Request CIP-008 R3.5 language be consistent with CIP-009 R3.5.
No
The VSLs need to align with the requested changes in questions 38-40.
No
Recommend changing 1.3 to avoid double jeopardy. Change "Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change." to "Update the baseline configuration as necessary within 30 calendar days of completing the change approved in 1.2." Recommend removing "High Impact BES Cyber Systems" from 1.4's Applicability since these are covered by 1.5 which is a higher threshold.
Yes
No
For 3.1 and 3.2 of Table R3 recommend removing “initially upon the effective date of the standard” because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. Grandfathering should be considered. For 3.1, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend change for 3.2 “…perform an active vulnerability assessment in a test environment which models the baseline configuration of the BES Cyber System in the production environment.”
Yes
No
For 1.3, request clarification of whether variances noted in the assessment would be required to be a self report. Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames

specified. Grandfathering should be considered.
Yes
Yes
The table label Scenario of Unplanned Changes is for unplanned changes after the effective date. If true, the surrounding words should explicitly state so. Due to the CIP version 4 and version 5 implementation cycles, there is a lack of understanding as to what needs to be implemented, leading to uncertainty as to how long an implementation period would be needed. It is unrealistic to expect entities to begin implementing Version 4 requirements and then have to implement Version 5 requirements within a very “narrow” window. Since Version 4 is not FERC approved, there is the possibility of Version 4 being effective while version 5 is in implementation. Version 4 may only be effective for a few months. A summary of comments applicable to more than one standard: . • Recommend removing “initially upon the effective date of the standard” from 1.3 of Table R1 because it will lead to forcing an Entity to be compliant with two Versions of the Standard at the same time. The increased demands placed upon Entities to be compliant with Version 5 will make it very difficult to become compliant when going from Version 4 to Version 5 within the time frames specified. • Request that Applicability sections of CIP-002-5 – CIP-011-5 be consistent. Note CIP-005-5 and CIP-006-5 sections 4.2.2 are different from other Standards. • Request clarification of the capitalized term “Facilities.” Does this refer to the NERC Glossary of Terms or section 4.2? For example, see CIP-002-5 sections 4.1.2 and 4.2.1, and note this question applies to the Applicability sections of CIP-002-5 – CIP-011-5. The SRC appreciates the efforts of the drafting team in producing the published standards. We look forward to responses to the comments and subsequent revisions to the standards. A fiftieth question should have been included in this comment form asking for general comments or concerns. A question asking general comments should be included as part of every comment form posted to the industry.
Individual
Darryl Curtis
Oncor Electric Delivery Company LLC
Yes
CIP Exceptional Circumstance: Request revision to “A situation that may involve one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, a Cyber Security Incident requiring emergency assistance (internal or external to an entity), a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.” Reportable BES Cyber Security Incident: Request that the drafting team consider the efforts of the 2009-01 project team and assure consistency between the definition as proposed under the new version of EOP-004 (Version 2).
Yes
Every two years within the ERCOT interconnect, the ERCOT ISO facilitates the bidding and selection of Black Start generation resources. Oncor Electric Delivery Company, as a Distribution Provider, Transmission Owner, Transmission Operator, and Load Serving Entity (and as further defined within the constraints of the Texas retail market) is not part of this selection process. Likewise, Oncor may not be able to sufficiently implement CIP Compliance on impacted facilities (substations) in a timely manner as there is typically a two month time span between selection and implementation of newly selected generation units as Black Start resources . Oncor will be significantly time-constrained on achieving strict compliance on any of its own, newly identified BES Cyber Systems and/or BES Cyber Assets once any applicable generation units are selected. Consideration should be given to provide a doable CIP implementation schedule for Distribution Providers, Transmission Owners, Transmission Operators and Load Serving Entities within the standard to accommodate newly acquired applicable Black Start resources.
Yes
Grammatical Correction: “Update the identification and categorization within 30 calendar days of when a change to BES Elements and Facilities is placed into operation…” M1 States: “Evidence of categorization of Low Impact BES Cyber Assets and BES Cyber Systems may be demonstrated by the application of the required controls.” – According to R1, Entities that own BES Cyber Assets and BES

Cyber Systems shall identify and categorize only its High and Medium Impact BES Cyber Assets and BES Cyber Systems. All remaining are deemed “Low Impact”. Oncor Electric Delivery suggest that some clarification in the language is needed for M1:
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Jose H Escamilla

CPS Energy
Yes
BES Cyber Asset definition should take into consideration redundant system in determining availability. A system with high availability typically involves multiple levels of redundancy. A high availability multi-site system will not likely experience an interruption that would impact the BES Reliability Operating Services. It is recommended that the SDT adopt a definition that takes into account the availability BES Cyber Assets to the end-user (i.e. system operators).

Individual
Adam Menendez
Portland General Electric
Yes
General Comments: Portland General Electric Company (PGE) takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because PGE believes that the definitions require additional clarity and that certain terms, including “dial up accessible” must be defined. PGE is opposed to any instances of changes where there is no clear need as each modification requires extensive resources to modify existing compliance processes, documentation, and evidence. Requirements and/or Measures that use all-encompassing or absolute words like “any” and “all” introduce compliance challenges, as satisfying these definitions potentially introduce extensive additional elements that would be out of scope and increase risk of non-compliance. PGE requests the standards drafting team (SDT) to clarify, ‘locations’ as it relates to facilities. The term is vague and does not provide a clear understanding for how entities’ can identify and categorize its BES Cyber Assets and BES Cyber Systems according to the criteria contained in CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems. If the SDT did enhance the term ‘location’ with geographical parameters (IE: How is a wind facility considered? What is an acceptable distance between generating units?) this would enhance entities’ classification processes. • BES Cyber Asset – PGE agrees with EEIs proposed change • BES Cyber Security Incident – PGE agrees with EEIs proposed change • BES Cyber System – PGE agrees with EEIs proposed change • BES Cyber System Information - PGE agrees with EEIs proposed change • Defined Physical Boundary – PGE agrees with EEIs proposed change • Inter-Entity Real-Time Coordination and Communication – PGE agrees with EEIs proposed change • Add the following definitions (from CAN-0007) - PGE agrees with EEIs proposed change • Other terms which would benefit from definitions o Adverse o Annual – Propose use of definition within CAN-0010 o Impact o Security Plan o Associated o Dial up-Accessible • Existing definitions that would benefit from alternative wording - PGE agrees with EEIs proposed change
Yes
PGE agrees with EEIs proposed suggestions
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. PGE believes that applying the BES Reliability Operating Services approach as set out in CIP-002-5 is confusing and therefore will be exceptionally difficult to implement. Additionally, the BES Reliability Operating Services approach expands the scope of the standards beyond what is necessary for security or reliability of the BES. This expanded scope will significantly increase demands on labor and capital and will not deliver a markedly more secure system. Further, it will make auditing the standards difficult which may slow the industry’s ability to correct misconceptions in application of the standards. 2. CIP-002-4, on the other hand, establishes a bright-line approach which is well understood by the industry and has already been approved by stakeholders. Retaining the structure set out in CIP-002-4 will encourage compliance and make auditing of the standards and corrections to application much simpler, thereby protecting the security and reliability of the BES. In addition, PGE believes that CIP-002-4 could be compatible with a tiered high-medium-low approach as is contemplated by the

Standards Drafting Team in Version 5. 3. Applicability – PGE agrees with EEIs concerns in reference to UFLS and UVLS is a point of concern and agrees with the proposed. 4. CIP-002-5 R1 – PGE agrees with EEIs proposed changes 5. CIP-002-5 R1.1 - PGE agrees with EEIs proposed changes 6. Because PGE believes that a compliance structure that is easy to understand, apply and enforce increases security and reliability, PGE votes “no” on CIP-002-5 and encourages the Standards Drafting Team to retain CIP-002-4.
No
PGE agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following reasons: PGE also agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes
No
PGE agrees with EEIs comments and proposed changes. This goes beyond the scope of FERC Order 706.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reason because the standard is worded in a way that PGE believes could create confusion regarding the timing of the requirements.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE agrees with EEIs comments and proposed changes. Additionally, PGE proposes clarity for how these requirements are applied with regard to shared administrative accounts? The shared administrative accounts standard (CIP-007 R5.2) has been removed, in favor of this requirement, but it is not explicit here that this applies to shared administrative accounts. The conflict between these requirements in previous versions has caused some confusion.

No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard creates confusion around what evidence is required to prove compliance. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. The standard as written is vague when applied to the Electronic Security Perimeter and does not account for the technical capabilities of virtual environments. 2. Additionally, as server virtualization is more fully deployed in CIP-compliant environments, there will be a need to think differently about where security products are deployed. In the below statement from page 39 of the CIP-007-5 document, please take note of this section: "This control is another layer in the defense against network-based attacks, therefore it is the intent that the control be on the device itself; blocking ports at a perimeter does not satisfy this requirement. "The issue with this type of thinking is that applications are starting to move off of the virtual servers to virtual appliances running on the hypervisor. It could be very important that the wording of requirements related to servers not assume that products like firewalls, anti-virus, intrusion detection, etc actually resides on the server itself. 3. When server virtualization is being used, does every virtual server residing on a physical host, have to be treated at the same “impact” level? For example, can a physical host have a “high impact” virtual server used by the Control Center, and also contain other virtual servers with a “low impact” rating. 4. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.

No
PGE agrees with EEIs comments and proposed changes. R4.2 Consideration- The real time alerting required by R4.2 may not be technically feasible in all situations and the requirement does not provide adequate guidance on what to do in such situations. Additionally, it is not clear how to treat shared administrative accounts for purposes of compliance with R5. R4.3 Consideration- This sub-requirement seems to conflict with 4.5. If the purpose of 4.5 is to “identify… potential event logging failures” and occurs every two weeks, what about the 4.3 requirement to “detect and respond to event logging failures before the end of the next calendar day”? Please clarify.
No
PGE agrees with EEIs comments and proposed changes. R5 Consideration - How shall this requirement be applied with regard to shared administrative accounts? The shared administrative accounts standard (CIP-007 R5.2) has been removed, in favor of this requirement, but it is not explicit here that this applies to shared administrative accounts. R5.1 Consideration - If PLCs are included in the definition of BES Cyber System they may not be technically capable of meeting this requirement.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion regarding applicability and evidence measures. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO for the following specific reasons: 1. As written, the standard is overly broad and vague. It is not clear what exactly “information used in the recovery of BES Cyber Systems that is stored on back up media” relates to and because of this confusion, the standard could apply to hundreds of thousands of files. The lack of clarity in what the standard requires owners to test means that PGE cannot determine if compliance with this standard is technically feasible or, if it is possible, what the resulting burden would be. 2. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have

assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard does not effectively capture the intent of FERC Order No. 706. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
Yes
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes overly broad and confusing regarding applicability. PGE also agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE agrees with EEIs comments and proposed changes.
No
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because PGE believes the implementation plan is incomplete because it does not capture all of the milestones laid out in the standards themselves necessary to achieve compliance. PGE also agrees with EEIs comments and proposed changes.
Group
EPUC, CAC and NCA
Donald Brookhyser
No
No
Yes
Yes
No
The following comments address the approach of Version 5 generally. They are provided here as the first available opportunity in this comment form: These comments are submitted by the Energy Producers and Users Coalition, the Cogeneration Association of California, and Nevada Cogeneration Associates #1 and #2 (collectively “the Cogeneration Parties”). As drafted, the Version 5 CIP standards impose significant new requirements on Responsible Entities, arguably without any material change in real protections related to access to, or vulnerability of, cyber systems. These additional administrative burdens are being imposed on entities that are already registered and compliant with the existing version of the standards, although their susceptibility to threat has not increased. The new standards will not impose any new limitations on access to cyber assets, and only create

additional, burdensome administrative support for the existing limitations. The Cogeneration Parties recommend that Responsible Entities that identify only Low Impact Cyber Systems in complying with CIP-002 be excused from compliance with any other CIP standard. Discussion All of the facilities operated by the Cogeneration Parties are generating facilities that are small enough that their assets qualify under the Version 5 definition as Low Impact BES Cyber Systems. This exclusion due to size probably applies to most of the generators in the Western Interconnection. As such, all of the substantive requirements that actually limit access or address vulnerabilities do not apply. This includes Standards CIP-004, Requirements 2-7; CIP-005, R2; CIP-007, R1-4; and CIP-009 through CIP-011. What will apply to these generators are the requirements for more detailed plans (Standard CIP-003 and CIP-006, R1), more training and awareness (CIP-004, Requirement 1), and a Cyber Security Incident response plan (Standard CIP-008). The CIP standards have up until this point been limited in their applicability based on access. The standards only required compliance from generators with cyber equipment that had either a routable protocol or dial-up access. That limitation excused from compliance with the CIP standards many of the generators that had registered. The early descriptions of Version 5 of the standards suggested that this same limitation on compliance based on access would be continued. But to the contrary, the draft has added many new requirements that are not so limited. The only requirement so limited by access is CIP-005, R1. To provide some rational limitation on the administrative burdens imposed by these proposed standards, the Cogeneration Parties suggest that where a Responsible Entity has only Low Impact Cyber Systems, it must perform the identification of cyber systems required by CIP-002 and then be excused from compliance with any of the other CIP standards.
No
See answer to Question 7

Group
Tacoma Power
Travis Metcalfe
Yes
Under the “BES Cyber Asset” definition there should be a different category for assets that can be misused versus those can only be rendered inoperable. For example, the loss of a RS232/RS484 to fiber optic converter on a 500 kV transformer temperature gauge would result in a minor loss of situational awareness, thus becoming a medium impact cyber asset. The focus should be on assets that could potentially be misused. BES Cyber Asset-“Adversely Impact” should also be a defined term. It should be defined as: An effect that results in a violation of any BAL, INT, IRO, or TOP standard or makes unavailable or significantly reduces operational ability.” BES Cyber System Information—The current definition uses the phrase “security procedures”. “Security procedures” covers a wide variety of possible procedures rendering the definition vague and overbroad. Provide clarification as to what security procedures need to be protected. BES Reliability Operating Services- This definition is overly broad because impacts to some of the specific bulleted items do not directly impact BES reliability. Furthermore, some of these functions are typically performed or stored outside of a control center with no electronic link to real time control systems. Recommend removing the following sections: 1. “Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc).” Some of this data is calculated, stored or communicated outside of a real-time control system. 2. “Know generation status, capability, ramp rate, start time “Some of this data is calculated, stored or communicated outside of a real-time control system. 3.”Monitoring and alerting (such as EMS alarms)” Not all EMS alarms are critical to BES reliability. 4. “Change management - Current Day & Next Day planning - Contingency Analysis” These functions are typically performed by engineers in an office environment instead of a real-time control center. These functions are not needed with a 15 minute time frame, but the current definitions could lead to categorizing the computers to do these functions as cyber assets. Control Center-This definition is overly broad because it includes many locations not traditionally thought of as control centers. The definition should include that the site is regularly staffed by System Operators and a separate definition should be created for data centers and other facilities that perform some of the same functions. Examples of unmanned locations that would become control centers per the current definition include: Substations that present the status of remote breakers or equipment, each communication facility that has more than one utility present, and the terminals of a transmission line that use tele-protection. Cyber Assets devices that are not programmable via communications should be excluded from a list of BES Cyber devices. There are many substation devices programmed via DIP switches or just an HMI such as temperature monitors and serial communications media converters that represent a very low possibility of misuse, but could currently be classified as medium impact assets. Tacoma Power also supports the comments submitted by APPA. Tacoma also supports the comments submitted by the Edison Electric Institute with the exception of the changes proposed for BES Cyber Security Incident.
Yes
Attachment 1 criteria for a High Impact rating should be more specific than “any” for a Control Center or Backup Control Center performing the functional obligations of a Balancing Authority Tacoma Power supports APPA’s comments regarding BA’s designated as High Impact for the following reason.

• There are 107 Balancing Authorities subject to NERC regulation but not all have the same level of impact to the BES. For example the States of New York and Texas have one Balancing Authority each, while Arkansas and Arizona each have eight and Florida has eleven. Some BA's in States with multiple BAs are operated by relatively small municipal utilities and control less than 1,000 MW. CIP-002-5 needs to set a threshold limit to determine which BA's should be categorized as High Impact and which should be categorized at a lesser impact level. CIP-002-5 states that BES Cyber Assets are those cyber assets that, if rendered unavailable, degraded, or misused, would impact the BES Reliability Operating Services within 15 minutes of the activation or exercise of the compromise. Both High Impact and Medium Impact categories contain the time element in their definition but Low Impact does not. The standard needs to be clear on whether the time quantifier applies to Low Impact assets. CIP-002-5, R1 states that "All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification". Subsequently some of the CIP-003-5 through CIP-011-5 standards identify specific requirements and measures that apply to "Low Impact" systems. Therefore, the standards are unclear as to how an entity may demonstrate compliance with requirements that apply to "Low Impact" systems without providing "discrete identification" of these systems. For example, CIP-005-5, R1.1 requires entities to "define technical or procedural controls to restrict unauthorized electronic access" with a measurable to include "documented technical and procedural controls that exist and have been implemented". The standards appear to be self-contradictory in that they require documentation for implementation of controls on "Low Impact" systems but state that "Low Impact" systems do not require discrete identification. This will become problematic both for auditing compliance and ensuring all Low Impact systems have been identified and properly protected. Recommend requiring a list of Low Impact Assets. CIP-002-5, Attachment I, criteria 2.13 sets a threshold of 300 MW or more of generation for generation control centers to become "Medium Impact". Unlike the "1500 MW in a single interconnection" value in criteria 2.1 for "Medium Impact" systems, which is derived from the most significant Contingency Reserves operated in BAs in all regions, the 300 MW threshold is not clearly justified in the application guidelines. There is a statement in the Transmission section of the CIP-002 Application Guidelines stating "the drafting team understands that the real-time impact to the Bulk Electric System of a loss of load, or the equivalent amount of generation, will be similar, with….loss of generation resulting in a frequency low condition." This statement appears to directly contradict the 1500 MW limit in 2.1 in regards to generation. The standard and application guidelines fail to justify or articulate how the UFLS and UVLS 300 MW "bright line" for transmission load shedding is applicable to Generation. Recommend that the SDT provide justification for this requirement Regarding the NERC definition of "Control Center" and the use of the definition in CIP-002-5 Attachment I, the definition is not clear on whether two or more process control systems at two or more generation plants, whose combined outputs exceed the 300 MW threshold, that are interconnected to provide maintenance staff with real-time data but are not directly used by the System or Generator Operator for supervisory control of the generator would be considered "Control Centers". As an example, consider two hydroelectric generation facilities separated by a mile of river each with a process control system for the generators. These two local control systems are interconnected for use by roving local maintenance staff but data from these systems is independently sent from each generation facility via telemetry to the System and Generator Operator's SCADA system for use in controlling and monitoring the generators. It is not clear from the definition whether the process control systems at the facilities would be considered "Control Centers" due to the interconnection or whether, because these systems are not the same as the System Operator's SCADA system, they would be excluded. Recommend that the SDT provide clarification. Please refer to comments on the definitions for BES Reliability operating services and Adversely Impact. As currently written, this would categorize almost every cyber asset in EHV substations as medium impact. In context with the PSP access and logging requirements, this effectively eliminates having any electronic devices mounted directly on Substation equipment as it would be impractical to meet those requirements. Recommend further refining the definition. The description of redundancy in the background information should be expanded to clarify whether different systems without common mode failure points are allowed. For example, if load and generation forecasts can be manually entered by a System Operator but are usually entered using an automated forecasting tool, is the automated tool considered redundant or superfluous cyber asset? Tacoma Power recommends expanding/clarifying the definition.

No

Tacoma Power supports the comments of the Edison Electric Institute.

No
Tacoma Power supports the comments of the Edison Electric Institute.
No
Updating documentation required by R1.1 should not go from lower to severe just by doubling the time. Periods of 60, 90, 120 and 120+ days would be more appropriate based on the time requirements than the proposed 40, 50, 60 and 60+ days.
Yes
No
Recommend that for clarity under R2 1.5 the policy currently named System Security be renamed to Cyber System Security. Recommend making a distinction of how 1.10 - Provisions for declaring and responding to CIP Exceptional Circumstances differs from 1..6 – Incident Response and 1.7 – Recovery Plans.
Yes
Yes
Yes
Yes
Yes
Yes
No
Tacoma Power supports the comments of the Edison Electric Institute.
No
The application of the standard is inconsistent. If the requirements of CIP-004-5 R2 are not applicable to Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Assets, why are they included in CIP-004-5 R3? We suggest including the Associated PACS system in CIP-004-5 R2 or deleting it from CIP-004 R3.
No
Tacoma Power supports the comments made by NPCC and the Edison Electric Institute.
No
The application of the standard is inconsistent. If the requirements of CIP-004-5 R4 are not applicable to Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Assets, why are they included in CIP-004-5 R5? We suggest including the Associated PACS system in CIP-004-5 R4 or deleting it from CIP-004 R5.
No
Tacoma supports the comments made by Edison Electric Institute with the exception of changing the quarterly review to an annual review.
Yes
Yes
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.

Yes
No
R1.1 According to CIP-006-5 R1.1, Associated Physical Access Control Systems must have controlled access on par with a Low Impact BES Cyber System. According to Part 1.1 of the table, this does not require the protection of a Defined Physical Boundary that restricts access to only authorized individuals, nor does it require logging of access events. Furthermore, it specifically states that it does not require a detailed list of individuals with access. This appears to be inconsistent with the requirements of CIP-004-5 R3, R5, R6, and R7 which include completion of role-based training, a personnel risk assessment, and approval of access rights prior to granting access, review of access rights, and timely revocation of access rights. These requirements would seem to require listing individuals with authorized access and tracking access events. R1.2 and 1.3 Measures of evidence for CIP-006-5 R1.2 and R1.3 include the statement: "…ingress and egress is controlled by one or more of the following methods…" Controlled egress is currently not required. Recommend changing "ingress and egress" to "access." R1.5 It appears inconsistent that unauthorized access alerts and response are required on par with the monitoring and response requirements for the Defined Physical Boundaries that protect High and Medium Impact BES Cyber Systems if a Defined Physical Boundary that restricts physical access to only those that are authorized is not required per CIP-006 R1.1. Recommend rewriting the requirement to clarify this issue. Tacoma Power also supports the comments submitted by APPA. Tacoma Power also supports the Edison Electric Institute comments with the exception of the change to requirement. 1.4.
Yes
Yes
Yes
Yes
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by the Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and the Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by Edison Electric Institute.
No
Tacoma Power supports the comments submitted by Edison Electric Institute.

No
Tacoma Power supports the comments submitted by Edison Electric Institute.
Yes
No
Tacoma Power supports the comments submitted by APPA and Edison Electric Institute.
No
Tacoma Power supports the comments submitted by Edison electric Institute.
No
Tacoma Power supports the comments submitted by Edison Electric Institute as modified below. 1. 3.1 1. Requirements – Proposed content change ♣ Original Text – Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed. ♣ Proposed Change – On an annual basis, conduct a paper or active assessment of the cyber security controls to determine the extent to which the controls are implemented correctly and operating as designed. • Propose the addition (3.1.1) of minimum cyber security controls to be assessed that; o Are referenced within these standards; and o Are not already required to be assessed in other standards (removing double jeopardy implications) ♣ Rational • Annual (as defined within CIP-0010) should be the consistent approach to allow entities to standardize annual requirements on a consistent basis. • Active assessment is cited within Part 3.2 (to be done every 39 months) so we've removed it from this part to avoid overlap. 2. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the output of the tools used to perform the assessment. ♣ Proposed Change – Evidence may include, but is not limited to: • A document listing the date of the assessment, the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; • A document listing the date of the assessment and the assessment results. ♣ Rational – Annual should align with CAN-0010 definition. Documentation of assessment results focus on the root information in support of vulnerability rather than potentially extensive data (from tools) that may require extensive resources to retain. 2. 3.2 1. General observations ♣ While the application guidelines recognize production devices which may not be capable of modeling within a test environment (ICCP, etc.), this requirement does not provide clear guidance to follow where these instances occur. ♣ The 39 month cycle exceeds the 3 year retention requirements. 2. Requirements – Propose content change ♣ Original Text – Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. ♣ Proposed Change – At least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. Document the differences between the test environment and the production. 3. Measures – Propose content change ♣ Original Text – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment. ♣ Proposed Change – Evidence may include, but is not limited to, a document listing the date of the assessment (performed within 39 calendar months of the previous assessment), the output of the tools used to perform the assessment, and a list of differences between the production and test environments. 3. 3.4 1. Requirements – Propose content change ♣ Original Text – Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan.

♣ Proposed Change – Document the results of the assessments (conducted within 3.1-3.3) and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of that action plan. ♣ Rationale – referencing parts 3.1 – 3.3 provides alignment with the previous parts of the standards.
Yes
No
Tacoma Power supports the comments submitted by Edison Electric Institute.
Yes
Yes
Yes
Individual
Scott Miller
MEAG Power
Yes
MEAG Power supports the comments submitted by APPA.
Yes
MEAG Power supports the comments submitted by AECI.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
Yes

Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.

Yes
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
No
MEAG Power supports the comments submitted by APPA.
Yes
Yes
Yes
Yes
No
MEAG Power supports the comments submitted by APPA.
Individual
Maggy Powell
Constellation Energy on behalf of Baltimore Gas and Electric, Constellation Power Generation, Constellation Commodities Group and Constellation Energy Control and Dispatch
Yes
Because the definitions underpin the suite of CIP standards, it is key that they are clear and understood by all stakeholders. Constellation offers the following comments and suggestions on the proposed definitions: BES Cyber Asset – The definition needs to better focus on the cyber asset rather than the 15 minute time qualification. The 15 minute description should be removed whenever "BES Cyber Asset" is used in a standard as it will be duplicative to the definition. Also, "when required" does not seem necessary in the definition. Proposed Revision: BES Cyber Asset – A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation adversely impact one or more BES Reliability Operating Services. This is regardless of any delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. Redundancy shall not be considered when determining adverse impact. A Transient Cyber Asset is not considered a BES Cyber Asset. BES Cyber Security Incident – The definition should clarify that the terms "malicious" and "suspicious" are to be determined at the discretion of the Registered Entity and not by an auditor. In addition, in accordance with a request to return to using the term Physical Security Perimeter instead of Defined Physical Boundary (below), replace DPB with PSP. Proposed Revisions: BES Cyber Security Incident – A malicious act or suspicious event (as determined by the Registered Entity) that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or • Results in unauthorized physical access into a Physical Security Perimeter. BES Cyber System – The word "typically" in the definition is too vague and lessens the clarity of the definition or its use in other standard language. “Typically” should be removed from the definition and the body of proposed standards. “Maintenance Cyber Asset” should be replaced with “Transient Cyber Asset.” Proposed Revision: BES Cyber System – A BES Cyber Asset or group of BES Cyber Assets (logically or physically) that operate one or more BES Reliability Operating Services. A Transient Cyber Asset is not considered part of a BES Cyber System. BES Cyber System Information – The term: "BES Cyber System Impact" is stated in all capitals, but “impact” should be in lower case since it is not defined. BES Reliability Operating Services – In general, further consolidation of the operating services is needed. Assets such as governors, automatic voltage regulators, and power system stabilizers fall into a number of the different BES Operating Services; therefore, a reordered definition will be more cohesive. For example, combining "controlling frequency," "controlling voltage," and "monitoring and control" are all related to ensuring

the BES is operating within its bounds. In addition, further clarity on who/what provides these services needs to be added (e.g. "Aspects of BES Dynamic Response, Spinning reserve - Providing actual reserves" it is not clear who provides the reserves). The Application Guidelines language in CIP-002 offers a good example for revision (see pages 19-22). The Operating Services definitions should include the parenthetical reference to describe who/what provides the service. Specifically under the section on Dynamic Response, Special Protection Systems or Remedial Action Schemes, the word “possibly” is too vague and should be removed. As well, further clarification is needed on what “software” is intended for inclusion. Unless “software” is specifically clarified, it should be removed. Proposed Revision: BES Real-Time Reliability Operating Services – BES Real-Time Reliability Operating Services are those real-time services or functions contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services: Dynamic Response to BES conditions - Operation, monitoring or control of BES Elements, Facilities or systems that automatically respond to a BES condition. The operation, monitoring or control of BES Elements, Facilities or systems designed to perform an action or respond to a condition precedent. Aspects of BES Dynamic Response include, but are not limited to: • Spinning reserve (contingency reserves) – Deploying reserves (GOP) – Monitoring reserve levels (BA) • Governor Response – Control system used to actuate governor response (GO) •Protection Systems (transmission and generation) – Line, bus, transformer, generator (TO, GO) – Zone protection (TO, GO) – Breaker protection (TO, GO) – Current, frequency, speed, phase (TO, GO) - Under and Over Frequency relay protection (includes automatic load shedding) and their sensors, relays and breakers (DP) - Under and Over Voltage relay protection (includes automatic load shedding) and their sensors, relays & breakers (DP) • Power System Stabilizers (GO) • Controlling Frequency (Real Power) Generation Control (such as AGC (Automatic Generation Control)) – ACE (Area Control Error), current generator output, ramp rate, unit characteristics (BA, GOP) – Software to calculate unit adjustments (BA) – Data Transmittal to individual units (BA) – Unit controls responding to data transmittals (GOP) • Regulation Deployment (regulating reserves) – Frequency data (BA) – Governor control system (GOP) • Controlling Voltage (Reactive Power) - AVR (Automatic Voltage Regulation) – Sensors, stator control system, feedback (GOP) -Capacitive resources – Status, control (auto), feedback (TOP, TO, DP) -Inductive resources (transformer tap changer, or inductors) – Status, control (auto), feedback (TOP, TO, DP) -SVC (Static VAR Compensators) – Status, computations, control (auto), feedback (TOP, TO, DP) Balancing Load and Generation - Operation, monitoring or control of BES Elements, Facilities or systems necessary for provide awareness of or respond to load and generation balancing conditions in real-time. Aspects of the Balancing Load and Generation Operating Service include, but are not limited to: • Calculation of ACE – Field data (real time tie flows, frequency sources, time error, etc) (TO, TOP) – Software used to perform calculation (BA, RC) • Unit commitment information and communication – Know generation status, capability and load schedules (TOP, BA) • Controllable Load management/Demand Response – Ability to identify load change need (BA) – Ability to implement load changes (TOP, DP) • Remote Manual Initiated Load shedding – Ability to identify load change need (BA) – Ability to implement load changes (TOP, DP) • Remote Operation of Non-spinning reserve (contingency reserve) (GOP) Managing Constraints - Operation, monitoring or control of BES Elements, Facilities or systems that are necessary to ensure that the BES is operated in real-time within design limits. Aspects of the Managing Constraints include, but are not limited to: • Available Transfer Capability (ATC) Calculation (TOP) • Interchange schedules [Impact Analysis or Curtailment] (TOP, RC) • Identify and monitor SOL’s & IROL’s (TOP, RC) • Identify and monitor Flowgates (TOP, RC) SCADA and Substation Automation - Real-Time remote operation or control of breakers and switches and situational awareness. (TOP, GOP, RC, BA) Restoration of BES - Operation, monitoring or control of BES Elements, Facilities or systems that are necessary to reinstate reliable operation of the BES from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES Operating Service include, but are not limited to: • Blackstart unit and planned cranking paths (TOP, GOP) • Off-site power for nuclear facilities. (TOP) Situational Awareness - Operation, monitoring or control of BES Elements, Facilities or systems necessary to (i) assess the real-time condition of the BES or (ii) anticipate effects of planned and unplanned changes to BES conditions. Aspects of the Situation Awareness Operating Service include, but are not limited to: • Monitoring and alerting systems (such as EMS (Energy Management System) alarms) (TOP, GOP, RC, BA) • Change management [Change Management seems to vague compared to the other services listed. We request that the drafting team provide, more information to clarify. (TOP, GOP, RC, BA) • Current Day planning (TOP) • Contingency Analysis (RC) • Frequency monitoring (BA, RC) Inter-Entity Real-Time Coordination and Communication - Operation, monitoring or control of BES

Elements, Facilities or systems necessary for the coordination and communication of BES condition data between Registered Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to: • Scheduled interchange (BA, TOP, RC) • BES Element, Facility or system operational data and status (TO, TOP, GO, GOP, RC, BA) • Operational directives (TOP, RC) [We request that the Drafting Team provide an example of the type of directive that is covered in relation to cyber assets/systems. Perhaps one example is the operation of a breaker/relay using a BES Cyber System (Asset)] CIP Senior Manager – Greater clarity needed on what is meant by "official" and does it mean that the CIP Senior Manager must be a company "officer"? Control Center – Control Center should not be defined in CIP Version 5. The term attempts to concisely define a complex and varied setting and risks creating more complications to applying the CIP measures. The team should remove the Control Center definition and allow the boundaries established in Attachment 1 to define the various control centers intended to deploy controls. If “Control Center” must be defined, it should be done by a separate, focused drafting team to tackle the complexities inherent in such a definition. This definition could be the stumbling block to achieving stakeholder support for the suite of Version 5 standards if not properly composed. Defined Physical Boundary (“DPB”) – The term “Physical Security Perimeter (PSP)” is more widely understood as a security term than is Defined Physical Boundary (“DPB”). However, the inclusion of the 6-wall perimeter requirement in the previous PSP definition was problematic. Now that the 6-wall requirement is removed, PSP is a better term than defining DPB. In addition, we propose two other refinements. Replacement of the DPB with PSP, if approved, will require replacement of the terms throughout the standard language. Proposed Revision: Physical Security Perimeter (PSP) - The physical boundary securing locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside and for which access is controlled. Electronic Access Point (“EAP”) – The cyber asset serving as an EAP both "restricts" and allows communication. Further evaluation of this term may be warranted as it may be understood differently as a definition versus in the context of the standard language. We continue to evaluate the proposed definition and may have additional comments. Proposed Revision: Electronic Access Point (“EAP”) - An interface on a Cyber Asset controls routable or dial-up data communications between Cyber Assets. External Connectivity and External Routable Connectivity – “External Connectivity” does not appear to be used in Version 5, though the definition makes more sense as a definition of “External Routable Connectivity.” We propose removing the term “External Connectivity”, but retain the definition language for “External Routable Connectivity.” Proposed Revision: External Routable Connectivity – Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter. Physical Access Control Systems – Revise in accordance with a request to return to using the term Physical Security Perimeter instead of Defined Physical Boundary. Proposed Revision: Physical Access Control Systems - Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s) exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. Reportable Cyber Security Incident – This definition must be consistent with the language in EOP-004 and the Events Analysis Process. (Please see additional comments to Question 36 regarding the relationship between CIP-008 and EOP-004). Transient Cyber Asset – Greater clarity is needed to confirm that “connected for 30 days” means a continuous connection for 30 days. As well, the criteria should require condition 1 along with condition 2 or condition 3, but not necessarily both. Proposed Revision: Transient Cyber Asset – A Cyber Asset that is directly and continuously connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset and 1) used for data transfer, maintenance, or troubleshooting purposes, or 2) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

Yes

Repeating the definition language in Attachment 1 (for both the High and Medium Impact language) is redundant and, at present, the language does not match the proposed definition. Proposed Revision: “High Impact Rating: Each BES Cyber Asset or BES Cyber System used by and located at:” “Medium Impact Rating: Each BES Cyber Asset or BES Cyber System for:” In addition, per our proposal regarding the definition of Control Center, the term should be made lower case in Attachment 1. CIP-002-5 1.3: It's not clear what functional obligations are targeted by including TO. TO should be deleted. CIP-002-5 2.13: Generation control centers of 300 MW or more is too low of a threshold. Considering that drafting team states that a loss of generation of 1500 MW or more would have a medium impact to the BES, it is only logical that a control center capable of losing that much generation should then be medium as well.

No
It seems odd that CIP-002-5 R1.1 would require updates only when the impact category increased. As well, it is not clear whether “within 30 days” means before, after or either and it is not clear what defines the “change.” Proposed Revision: CIP-002-5 R1.1. Update the identification and categorization when a change is made to the BES Cyber Systems or BES Cyber Assets that is intended to be in service for more than 6 calendar months. The update shall be made within 30 days following when the changed BES Cyber System or BES Cyber Asset performs a Reliability Operating Service. It is also important that changes track with the language of the implementation plan. Constellation proposes changes to the Implementation Plan to address coordination with CIP-002-5 R1.1 and other concerns with the Implementation Plan. (Please see our response to Question 49). CIP-002-5 M1: Guidance to auditors should clarify the "includes, but not limited to" means that other forms of evidence other than those listed are acceptable to demonstrate compliance and it does not mean that other evidence is to be collected in additions to the types listed.
No
CIP-002-5 R.2: More clarity is needed on whether the team intends for the CIP Senior Manager or delegate approve required changes in identification and categorization. CIP-002-5 M2: For consistency with the requirement, the measure should read: "CIP Senior Manager or delegate". Proposed Revision: CIP-002-5 M2. Acceptable evidence includes but is not limited to electronic or physical dated and signed records to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate to review and update, where applicable, the identification and categorization of BES Cyber Assets and BES Cyber Systems initially upon the effective date of the standard and at least once each subsequent calendar year, not to exceed 15 calendar months between occurrences, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
CIP-003-5 R1. To accommodate the fact that a parent or affiliated company, not the Responsible Entity, may be the entity that identifies the CIP Senior Manager, this requirement should allow sufficient flexibility to accommodate varying corporate structures. Proposed Revision: CIP-003-5 R1. Each Responsible Entity shall have an identified CIP Senior Manager by name. CIP-003-5 M1. Further consideration should be given to how the qualification as a “high level official” can be audited. Does this mean that an officer of the company shall designate the CIP Senior Manager?
No
CIP-003-5 Requirement R2 does not require implementation of the ten topics, it requires implementation of the policies. Either remove the second bullet point or revise to clarify. Proposed Revision: Evidence may include, but is not limited to: 1. One or more documented cyber security policies, and 2. Records that indicate the policies address the ten topics enumerated in R2.
No
Constellation requests that “or delegate” be added to follow “CIP Senior Manager.” Given that the Senior Manager can delegate certain responsibilities, there may be instances in which the delegate is the more appropriate approver for a certain topic area that is to be covered by the policy documents.
No
CIP-003-5 M4: Further clarification is needed on the expectations of what is required to demonstrate awareness. We recognize that the measure correctly states that “Evidence may include” the listed items. Yet, we paused to consider what an effective demonstration of awareness is. Does the team feel that more than one of these listed items is required to demonstrate awareness? Further complicating the consideration is that training is not required as part of the requirement; however, dated training records are listed as an acceptable form of evidence. Listing things in measures that are not in the requirement is touchy for the audit context and auditors must be advised that training is not required. That said, it is understandable that an entity could deploy a robust awareness training program that would sufficiently demonstrate compliance on its own. Further guidance is requested.
No

CIP-003-5 R5: Constellation recommends removal of “with the exception of the approval of the Cyber Security Policy.” Note that the reference to the Cyber Security Policy as a single document in R5 is inconsistent with R2 and R3, where one or more cyber security policies are discussed. What does the SDT envision? A series of policy documents that address the 10 cyber security topics required under R2 or a single all encompassing cyber security policy document that addresses all 10 topics therein? Care should be given to avoid creating an overly cumbersome approval requirement and requirements need sufficient flexibility to accommodate varying corporate structures. CIP-003-5 M5: Change first sample bullet to RC control center instead of substation. The example may imply that all substations will be subject to this control and that may not be the case.

Yes

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-004-5 R1: The removal of the need to ensure that “everyone” received awareness is a positive improvement. CIP-004-5 Table R1, 1.1 adds a new term: “concepts.” The use of terms becomes problematic if accompanied by an assumed definition. Even though many terms – practice, program, procedures, are at times used interchangeably, entities now have experience in which auditors expected the title of the document to match exactly what is stated in the requirement even though functionally the terms were the same. Are entities to define what is meant by “concepts.” In addition, it is unclear what is meant by "reinforcement" in the R1.1 requirement. CIP-004-5 M1: Greater clarity is needed regarding the CIP-004-5 Table R1, 1.1 measures to understand what "material" qualifies as "reinforcement of such concepts." CIP-004-5 M1: Why did the command change from “may” to “must”? CIP-004-5 M2 states “must,” but only the measures in CIP-004-5 Table R2.1 state “must,” the rest state “may.”

No

CIP-004-5 R2: The term “role-based” is correctly lower case to allow the entity to define the roles and the associated training; however it should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-004-5 R2.3: Unlike the other requirements in R2, R2.3 discussed “proper use” of physical access controls. It is more consistent to remove the “proper use” reference or perhaps “implementation” is a more accurate and consistent word. CIP-004-5 Table R2 applies to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets.

No

CIP-004-5 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M3 states “must,” but the measures in Table R3 state “may.” M3 should be revised to say “may.”

No

CIP-004-5 R4: Further clarification is required on expectations regarding personnel who have a valid personnel risk assessment (PRA) in place under Version 3 or 4. Those PRAs should remain valid and entities should not be required to conduct new PRAs for the sake of the standard revision to Version 5. CIP-004-5 M4.2 in Table R4 needs additional clarity on treatment if a seven year record is "not possible" keeping in mind that background checks go back to age 18 and not before. Background checks will be needed for individuals under the age of 25. In addition, the measures do not consider whether an FBI background check qualifies as acceptable. FBI checks are considered thorough and

reliable; however, the FBI is not obligated to follow the NERC requirements. Confirmation of an FBI background check should be acceptable evidence. CIP-004-5 Tables in R4 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. CIP-004-5 M4 states “must,” but the measures in Table R4 state “may.” M4 should be revised to say “may.”

No

CIP-004-5 Tables in R5 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M5 states “must,” but the measures in Table R5 state “may.” M5 should be revised to say “may.”

No

On the CIP-004-5 R6.1, 6.2 and 6.3 requirements, further clarification needed on how "minimum necessary" is to be judged. As well, “delegate" should be plural, "delegate(s)" as authorization of access for a corporation may be made by more than one delegate. CIP-004-5 M6.1: The discussion of sampling is inappropriate for the measure because it is an auditing method rather than a form of evidence. In addition, “workflow” is too general a term here. In addition, the format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revisions: CIP-004-5 M6.1 Acceptable forms of evidence include, but are not limited to: • a system-generated list of people with electronic access • a signed document, authorization workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.2 Acceptable forms of evidence include, but are not limited to: • a system generated list of people with unescorted physical access through the Defined Security Boundary and a sampling of accounts (for automated physical access control) to verify unauthorized users do not have access • a signed document, workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.3 Acceptable forms of evidence include, but are not limited to: • a list of people with access to BES Cyber System Information and a sampling of accounts (on electronic document systems) to verify unauthorized users do not have access • a signed document, workflow or email showing such persons have authorization • similar or the same records showing the consideration of appropriate privileges on the basis of need in performing a work function were considered as part of the authorization. CIP-004-5 M6.5 Acceptable forms of evidence include, but are not limited to, documentation of the review including • a listing of all accounts/account groups or roles within the system • a summary description of privileges associated with each group or role • accounts assigned to the group or role and (iv) evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account. CIP-004-5 M6.6 Acceptable forms of evidence include, but are not limited to documentation of the review including: • a listing of authorizations for BES Cyber System information • any privileges associated with the authorizations • evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. CIP-004-5 Tables in R6 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M6 states “must,” but the measures in Table R6 state “may.” M6 should be revised to say “may.”

No

CIP-004-5 R7: Generally speaking, please provide greater information and justification on the newly proposed “at the time of” and “by the end of the next calendar day” timing requirements. Also note that workflow should be deleted from the evidence options as the term is not widely or consistently understood. CIP-004-5 R7.2 The “end of next calendar day” is problematic. The time frame should be at least 7 days and preferably 30 days. CIP-004 R7.1: Under current CIP-004 R4.2, the Responsible Entity is required to revoke authorized cyber or authorized unescorted physical access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for all other personnel who no longer require such access. As it currently exists, this requirement has proven to be a compliance challenge for many in the industry, and has required significant time and resources to implement automated and procedural controls in order to meet the proscribed 24-hour and 7 calendar day thresholds. Nonetheless, proposed CIP-004 R7 further constricts the time period in which revocations must take place. For terminations and resignations, the act of revocation has been unreasonably accelerated from 24-hours and 7-days (respectively) to “at the time” of the termination or resignation. Not only is this a drastic change, but “at the time” is an incredibly vague measure to be held to and to audit as well. Accordingly, Constellation supports keeping the existing, concrete 24-hour and 7 calendar day requirements for CCA access revocation. With regard to the proposed “at the time” requirements, Constellation requests the following additional clarifications: • The justification behind changing the existing revocation time requirements. • Definition of and/or expectations around what “at the time” means. • What is meant by “workflow” as a form of evidence? • Is evidence of “at the time” revocation expected to be time stamped? If so, how is one to show a time stamp when a badge is revoked at the time of termination or resignation? CIP-004 R7.2: With regard to reassignments and transfers, clarification is also needed as to what revocation “by the end of the next calendar day” means. Under the current standard, reassignments and transfers fall under the 7 calendar day revocation requirement. As stated above, further constricting the time in which such revocations are required to take place and replacing a firm time requirement with a vague measure is contrary to what is in the industry’s best interest and what is clearly and objectively auditable. CIP-004 R7.3: The above comments similarly applies to proposed CIP-004 R7.3, which requires the individual access to BES Cyber System information by the end of the next calendar day for resignations and terminations. CIP-004-5 Table R7: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revisions: M7.1 Acceptable forms of evidence include, but are not limited to: • a sampling of terminations • workflow or sign-off form verifying access removal associated with the terminations and dated concurrent or prior to the date of the termination action • a system-generated listing of user accounts or other demonstration showing such persons no longer have access. CIP-004-5 M7.2 Acceptable forms of evidence include, but are not limited to: ♣ a sampling of individuals transferred or reassigned ♣ workflow or sign-off form showing the review of logical and physical authorizations dated on the same calendar day as the transfer or reassignment ♣ a system-generated listing of user accounts or other demonstration showing such persons no longer have access where the review determined it was no longer needed. CIP-004-5 Tables in R7 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-004-5 M7 states “must,” but the measures in Table R7 state “may.” M7 should be revised to say “may.”

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-005-5 R1: While the rationale of CIP-005 is to focus on Electronic Access Points rather than the logical perimeter, the current approach in R1 makes it a requirement that physical and electronic monitoring systems be within an ESP because there must be defined access points. Requirement 1.3, in particular, may present an issue since explicit traffic access is to be specified along with why access

is needed. Some software makes this requirement difficult to define. CIP-005-5 R1.1: Please offer justification for the requirement to restrict unauthorized electronic access to Low Impact BES Cyber Systems when the CIP-004 program does not require declaring Low Impact BES Cyber Systems. Low Impact systems by virtue of their classification present a low impact risk; however the requirement poses a significant compliance burden. Additional consideration is needed to include this requirement and if retained, guidance needed on how to comply. Further, the applicability of CIP-005-5 R1.1 is Low Impact BES Cyber Systems with External Routable Connectivity. The definition of External Routable Connectivity is "The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol". While Constellation proposed a revision to the definition, additional insight from the drafting team will be helpful in assessing the language. Is your intent for Low Impact BES Cyber Systems to reside in an ESP? If so, does this imply implementation of additional controls or is it merely asking for documentation of how the Low Impact System is protected from access from a public network, i.e. existing controls to protect the corporate data network? In CIP-005-5 R1.2, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-005-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may." Measures in Table R1: Network diagrams, architecture diagrams, lists of access control rules and other documents are high risk security documents. Perhaps the standard language should include commitments to proper handling by NERC, Regions, auditors and any other potential external reviewers to ensure protection.

No

CIP-005-5 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may." CIP-005-5 Measures in Table R2: Network diagrams, architecture diagrams, and other documents are high risk security documents. Perhaps the standard language should include commitments to proper handling by NERC, Regions, auditors and any other potential external reviewers to ensure protection.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-006-5 R1.3: Greater consideration is needed when imposing the requirement to "utilize two or more different and complementary physical access controls …" in order to balance security with practical operations. CIP-006-5 R1.3 stands to impose significant cost without clear commensurate improvements to security. This requirement needs further vetting and a more full justification of net gains associated with such measures. CIP-006-5 M1.2 and 1.3: The Table R1 Measures for 1.2 and 1.3 include evidence on egress, while the requirements say "access." The requirements should be clear and the measures should be consistent. The requirement language should perhaps state ingress and egress if that is the expectation of the requirement. CIP-006-5 R1.4 and 1.5 – These requirements state: "Issue real-time alerts (to individuals responsible for response) in response to unauthorized physical access …" Please confirm that the entity is to define the "individual responsible for response" or clarify an alternate intent. If entity determined, it should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-006-5 R1.6 should be revised to as follows: Log (through automated means or by personnel who control entry) of physical entry into each Defined Physical Boundary protecting applicable BES Cyber Systems or Electronic Access Control or Monitoring Systems, which records sufficient information to uniquely identify the individual visitor and the date of their entry. CIP-006-5 Table R1, 1.1 Applicability: It's unclear to what the "associated" systems are intended to align. Should the order of listing be reversed to read: Low Impact BES Cyber Systems - Associated Physical Access Control Systems Please reorder within CIP-006-5 Table R1 as follows: CIP-006-5 Table R1, 1.2: Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.3: High Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.4: High Impact BES Cyber Systems -

Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 Table R1, 1.5 Applicability: It's unclear to what the "associated" systems are intended to align. CIP-006-5, M1 states "must," but the measures in CIP-006-5 Table R1 state "may." M1 should be revised to say "may."
No
CIP-006-5 R2: As written, this requirement limits entities to only having one visitor control program. The latitude to have more than one visitor control program is important to accommodate varying location configurations and potential technical limitations. Proposed Revision: "Each Responsible Entity shall implement one or more documented visitor control programs..." CIP-006-5 R2: The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Defined Physical Boundary to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit. It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort but there is no need to document everyone that acted as an escort for the visitor. The sentence, "It is also felt a Point of Contact should be documented who can provide additional details about the visit if questions arise in the future" is problematic. This sentence is ambiguous. Use of the words "should" and "if" may be interpreted several ways, potentially requiring management and documentation showing that each escort can speak to the details of every visit that occurs. Further clarification is needed to focus on a reasonable intent and to reduce uncertainty within the audit setting. The CIP-006-5 R2 Tables apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In addition, the order of the "associated" systems is confusing. Please reorder CIP-006-5 Table R2 for R2.1 and R2.2 as follows: High Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-006-5 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."
No
CIP-006-5 R3.1: Further clarification is needed on the intent/understanding behind the "prior to commissioning" for systems already in place. Prior to commissioning should be pointed at new Physical Access Control Systems commissioned after FERC approval of the CIP Version 5 standards. Proposed Revision: Prior to commissioning a new Physical Access Control System1, and at least once every 24 months after commissioning of a new Physical Access Control System, maintenance …" (Footnote 1 = A new Physical Access Control System is one that is commissioned by the Entity on a date following Version 5 CIP Cyber Security Standards approval by the applicable regulatory authority) CIP-006-5 R3.2 – Provide more insight on expectations around providing log records when the logging fails. CIP-006-5 Table R3, 3.1 and 3.2 Applicability: It's unclear to what the "associated" systems are intended to align. CIP-006-5 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may."
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
In CIP-007-5 R1.1, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."
No
CIP-007-5 R2.2: For clarity, R2.2 should replace "of" with "after" to read "…within 30 days after release." CIP-007-5 Tables in R2 apply to only High and Medium impact assets. If possible to clarify

this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-007-5 R2.1, R2.2 and R2.3, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”

No

CIP-007-5 Tables R3, M3.3: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revision: M3.3 Evidence may include, but is not limited to: • current signature or pattern updates • either screen shots showing the configuration of signature, or pattern updates for automated controls, or work logs showing the signature, or pattern updates for manual controls. CIP-007-5 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-007-5 R3.1, R3.2, R3.3, R3.4 and R3.5: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M3 states “must,” but the measures in Table R3 state “may.” M3 should be revised to say “may.”

No

CIP-007-5 R4 appears to go beyond a focused effort to account for events of concern to encompass logging of all events whether or not it is a Cyber Security Incident. Further R4.5 creates a new obligation to the CIP standards (and added paperwork burden) to summarize logged events (not incidents) to identify "unanticipated BES Cyber Security Incidents". The potentially onerous and administrative nature of this requirement could overwhelm the desired benefit of on-going assessment and improvement to practices. Please reassess whether the requirements and the compliance tasks achieve the desired goals and are commensurate with improvements to reliability and security. CIP-007-5 M4.1 identifies "event classes" which is not part of the requirement and may not be clearly understood in practice. Please clarify the intent of the term “event classes.” CIP-007-5 R4.3: It is unclear how R4.3 will be enforced. It may be difficult to detect logging failures of a specific event. If gross logging stops then you may be able to see it due to lack of events. CIP-007-5 Tables R4, M4.3: The format of the evidence options should be bulleted to be consistent with other table formats and to make the items options for evidence, not a required package of evidence. Proposed Revision: CIP-007-5 M4.3 Evidence may include, but is not limited to: • dated event logging failures and screen-shots showing how real-time alerts were configured • dated records showing that personnel were dispatched or a work ticket was opened to review and repair logging failures. CIP-007-5, Table R4: The order of the “associated” systems is confusing. Please reorder as follows: R4.1 - High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.2 and R4.3 High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems with External Routable Connectivity - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.4- High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 R4.5- High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M4 states “must,” but the measures in Table R4 state “may.” M4 should be revised to say “may.” As a minor note, in CIP-007-5 R4.1, “includes” should be singular. In rationale for CIP-007-5 R4 - remove 'of' after comprises.

No
CIP-007-5 R5.1 – may be clearer to replace “validate” with “authenticate” to match the measures. CIP-007-5 R5.2 is not practical. IT departments use administrative, shared, and other passwords in day to day operations. Requiring the Senior Manager or even a delegate to be involved in an approval process at that level could present operational barriers. This requirement should be removed. In CIP-007-5 R5.1, R5.2, R5.3, R5.5 and R5.6, the order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-007-5 M5 states “must,” but the measures in Table R5 state “may.” M5 should be revised to say “may.”
No
In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.
No
CIP-008-5 R1: Proposed revision to clarify: “Each Responsible Entity shall document one or more BES Cyber Security Incident response plan(s)…” CIP-008-5 M1.2 appropriately states that the entity shall document the guidelines or thresholds for determining if a BES Cyber Security Incident is also a Reportable BES Cyber Security Incident. It should be emphasized to auditors that this is an entity determination and should be judged in the context of the entity program. Further discussion in the Application Guidelines may also be helpful. CIP-008-5 R1.3: Proposed revision to clarify: 1.3 Requirement “Define, within the Incident Response Plan: …” CIP-008-5 M1 states “must,” but the measures in Table R1 state “may.” M1 should be revised to say “may.”
No
CIP-008-5 R2.1: The working of R2.1 is awkward. Proposed Revision: When a BES Cyber Security Incident occurs, follow the Incident Response Plan(s) and record any deviations from the plan. CIP-008-5 R2.2: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that a test-type implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and testing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. Proposed Revision: CIP-008-5 Rx: Implement the BES Cyber Security Incident response plan(s) so that they are in place upon the effective date of the standard. CIP-008-5 Mx: Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) on or before the effective date of the standard. CIP-008-5 Rx: Test the BES Cyber Security Incident response plan(s) at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise. CIP-008-5 Mx: Evidence may include, but is not limited to, dated evidence of testing of the BES Cyber Security Incident response plan(s) at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. CIP-008-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”
No
CIP-008-5 R3: Additional information is needed regarding the timeframes. While the discussion finds the time frames to be “feasible” if the entity program is clearly defined, it does depend on the incident envisioned. For instance, incidents concerning a protection system could meet the timeframe; however, an intrusion into an Energy Management System could be more involved and struggle to meet the timeframe. Please offer more insight. CIP-008-5 R3.1: Further clarification is needed on the intent of reviewing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that evidence of a review is required on the day the standard becomes effective. This poses a paperwork obligation of questionable value. The requirement should accept that the development of the plan that was implemented per R2 fulfilled the review for accuracy and completeness and remove the obligation to show evidence for an initial review. Proposed Revision:

CIP-008-5 R3.1: Review each BES Cyber Security Incident response plan for accuracy and completeness each calendar year following the effective date of the standard, not to exceed 15 calendar months between reviews, and update if necessary. CIP-008-5 M3.1: Evidence may include, but is not limited to, dated documentation of a review of each BES Cyber Security Incident response plan(s) at least once every each calendar year, not to exceed 15 calendar months, and an updated BES Cyber Security Incident response plan if necessary. CIP-008-5 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may." In reviewing CIP-008-5 in totality, Constellation is concerned that the requirements standards within CIP-008 and with EOP-004 may conflict or duplicate compliance obligations for cyber incidents. Constellation recognizes that both the EOP-004 and the CSO 706 drafting teams attempted to coordinate their efforts in order to streamline event reporting as a whole; however, the fact remains that there will be two standards governing reporting of cyber incidents. A possible solution would be to remove the cyber reporting requirements in EOP-004-2 and place them in CIP-008-5, thus requiring entities to have distinct incident reporting and response plans for cyber events and non cyber events.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

R1: Proposed revision to clarify: "Each Responsible Entity shall document one or more recovery plans…" CIP009 R1.4 – It is unclear from the Requirement if the intent is to require initial verification of the backup and restore processes when significant changes are made to the BES Cyber System (FERC Order 739) as the associated M1.4 seems to address FERC Order 748 to ensure verification that backups are successful and backup failures are addressed. R1.4 and M1.4 need clarification as to whether the requirement is for initial verification of backup processes upon significant system change or ongoing verification that backup operations completed successfully, or both. In addition, it's not clear how R1.4 and R2.2 differ. Clarification as to how the R1.4 requirement differs from R2.2 with regard to testing of information stored on backup media initially. CIP009 R1.5: Please clarify how "technically feasible" is defined in R1.5 and what actions are required if data is unable to be salvaged. For some devices, pulling a disk out to salvage it and replace would be acceptable. Other devices, such as network switches, do not have removal parts and when failed switch replacement is required. Anticipation of a TFE process is unsettling given the burdensome nature of the TFE process currently in place. Further consideration is needed to successful fulfill the security intent of these measures without undue burden. CIP-009-5 Tables in R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R1.1, R1.2, R1.3 and R1.5: The order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Please reorder CIP-009-5 R1.4: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems CIP-009-5 Table R1, 1.4 and 1.5 – The column headings are incorrect. All columns are titled "Part." CIP-009-5 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."

No

CIP009 R2.3: Please clarify what "representative environment" means. Our plans and tests are conducted in similar systems. This requirement depending on interpretation suggests that duplicate physical access control, monitoring systems and Energy Control System environment to allow to fully exercise recovery. Further, what does full operational exercise mean? Do you have to assume a complete loss of the environment scenario? A redundant environment allows more flexibility for recovery plans. CIP-009-5 R2.1, R2.2 and R2.3: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that a test-type implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all

entities. The requirement includes two activities – implementing on the effective date and testing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. Proposed Revision for CIP-009-5 R2.1: CIP-009-5 R: Implement the recovery plan(s) referenced in R1 so that they are in place upon the effective date of the standard. CIP-009-5 M: Evidence may include, but is not limited to, dated evidence of implementing the BES recovery plan(s) on or before the effective date of the standard. CIP-009-5 R: Test the recovery plan(s) at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise. CIP-009-5 M: Evidence may include, but is not limited to, dated evidence of testing of the recovery plan(s) at least once every calendar year thereafter, not to exceed 15 months, by recovery from an actual incident, or with a paper drill or table top exercise, or with a full operational exercise. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings. Clarify in the same way for CIP-009-5 R2.2 and R2.3 CIP-009-5 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R2.1, R2.2, and R2.3: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems In addition, the requirements in the Tables should be stated as nouns rather than action items to follow the direction of CIP-009-5 R2. CIP-009-5 M2 states “must,” but the measures in Table R2 state “may.” M2 should be revised to say “may.”

No

CIP009-5, R3: While deadlines for reviews and updates are useful, they should not trump operational priorities, workforce burden, cost implications and the reality of the review task. Thirty days in R3.2 is aggressive. With the complexity of these systems and the amount of documentation, the review process by all parties can take longer than 30 days and in some cases should in order to glean the relevant benefit from the review. Constellation proposes to increase the timing in CIP-009-5 R3.2 to 60 days. This change would also align with the time periods specified in CIP-008-5 R3.2 and 3.3 for the Incident Response drill and subsequent updates to the procedure. CIP-009-5 R3.1: Further clarification is needed on the intent of reviewing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that evidence of a review is required on the day the standard becomes effective. This poses a paperwork obligation of questionable value. The requirement should accept that the development of the plan that was implemented per CIP-009-5 R2 fulfilled the review for accuracy and completeness and remove the obligation to show evidence for an initial review. Proposed Revision: CIP-009-5 R3.1: Review the recovery plan for accuracy and completeness each calendar year following the effective date of the standard, not to exceed 15 calendar months between reviews, or when BES Cyber Systems are replaced, and document any identified deficiencies or lessons learned. CIP-009-5 M3.1: Evidence may include, but is not limited to, dated documentation of a review of the recovery plan(s) each calendar year, not to exceed 15 calendar months, or when BES Cyber Systems are replaced, including documentation of any identified deficiencies. CIP-009-5Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-009-5 R3.1, R3.2, R3.3, R3.4 and R3.5: The order of the “associated” systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems Medium Impact BES Cyber Systems at control centers - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems CIP-009-5 Table R3, 3.4 and 3.5 – The column headings are incorrect. All columns are titled “Part.” Typo in CIP-009-5 M3.2: "of the" is stated twice in a row.

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP010 R1.4 and R1.5 – The requirements in R1.4 and R1.5 for verification that cyber security controls are not adversely affected appear to be redundant. Please clarify the differences between the requirement in R1.4.2 ("…verify these required controls and the BES Cyber System availability are not adversely affected") and the requirement in R1.5.2 ("…ensure that required cyber security controls are not adversely affected…"). CIP010 R1 - As currently written, this requirement will most likely require manual tracking of changes to the system rather than encouraging use of automated systems to discover configuration and detect unauthorized changes. Additional refinement to the language is needed to accommodate and encourage progress in change management mechanisms. Tables in CIP-010-1 R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R1.1, R1.2, R1.3 and R1.4, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may."

No

CIP-010-1 R3.1 and R3.2: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that an assessment implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and assessing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. CIP-010-1 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R2.1, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."

No

CIP-010-1 Tables in R3 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R3.1 and R3.4, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-010-1 M3 states "must," but the measures in Table R3 state "may." M3 should be revised to say "may."

No

In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

CIP-011-1 R1.3: Further clarification is needed on the intent of implementing the plan(s) initially versus once every calendar year. As currently written, the requirement suggests that an assessment implementation is required on the day the standard becomes effective. The implications of such an imposition are significant since Day 1 is the same day for all entities. The requirement includes two activities – implementing on the effective date and assessing the plan(s) each calendar year. The two requirements should be delineated and potentially put in two separate requirements. CIP-010-1 Tables in R1 apply to only High and Medium impact assets. If possible to clarify this aspect in the

requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R1.1, R1.2 and R1.3, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-011-1 M1 states "must," but the measures in Table R1 state "may." M1 should be revised to say "may." CIP-011-1 Table R1, 1.2 and 1.3 – The column headings are incorrect. All columns are titled "Part."

No

CIP-010-1 Tables in R2 apply to only High and Medium impact assets. If possible to clarify this aspect in the requirement it would prevent a paperwork burden that may be required to signify that the requirements do not apply to Low impact assets. In CIP-010-1 R2.1 and R2.2, the order of the "associated" systems is confusing. Please reorder as follows: High Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets Medium Impact BES Cyber Systems - Associated Physical Access Control Systems - Associate Electronic Access Control or Monitoring Systems - Associated Protected Cyber Assets CIP-011-1 M2 states "must," but the measures in Table R2 state "may." M2 should be revised to say "may."

No

Comments: In general, the VSL should relate to reliability and not administrative errors. Further, the severity level thresholds in the VSLs do not seem related to reliability and there is insufficient discussion of the threshold justification. Please provide additional detail on the justifications behind this approach. The vegetation management VSL model may offer an alternative model to follow.

No

The implementation plan is confusing and does not address certain situations. Constellation proposes revisions to simplify some aspect, address voids and remove references to language in other standards: Proposed Effective Date for Version 5 CIP Cyber Security Standards Responsible Entities shall comply with requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1, and the Definitions of Terms Used in Version 5 CIP Cyber Security Standards as follows: 1. 18 Months Minimum – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.2 2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities. 3. Newly Registered Entities3 – Version 5 CIP Cyber Security Standards shall become effective 18 months from the Entity's registration date. (Footnotes: 2= In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4. 3= A newly Registered Entity is one that has registered with NERC on the date that Version 5 CIP Cyber Security Standards receive applicable regulatory approval or thereafter) Changes Resulting in a Higher Categorization and Newly Commissioned Assets Scenario Compliance Implementation New High Impact BES Cyber System Upon Commissioning New Medium Impact BES Cyber System Upon Commissioning Newly categorized High Impact BES Cyber System from Medium Impact BES Cyber System 12 months for new requirements Newly categorized Medium Impact BES Cyber System from Low Impact BES Cyber System 12 months for new requirements Responsible Entity Identifies first Medium or High Impact BES Cyber System Add 12 months from time above Additional Guidance and Implementation Time Periods for Disaster Recovery A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003-5 R2. The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full

implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed. However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Additional Comments Submitted:

Organization	Yes or No	Additional Comments Received
Midwest Reliability Organization	Affirmative	The standards drafting team has achieved great strides in fulfilling the industries obligation to FERC Order 706. CIP Reliability Standards V5 adequately address the security control of access points to the control systems used to secure the reliable operation of the electric grid.
NorthWestern Energy	Negative	NorthWestern Energy supports the proposed Issue/Solution below: Issue: As currently drafted Version 5 of the CIP standards: o Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. o Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. o Exceeds FERC's 706 order without justification or improving the security of the BES. o Many of the draft requirements add significant bureaucracy without adding security. The industry needs focus on improving security of the BES and not the security of individual assets or the appearance of security through the addition of administrative requirements. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: o Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed in Version 5 o Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. Â¶253-258, 270-27 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. Â¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. Â¶294-297 o Not exceed FERC Order 706: o Â¶284: "... there is no formally accepted method for identifying critical cyber assets before us at this time ... we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o Â¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access ... We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: o That identifies which assets in CIP-002-4 are High Impact and o Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o

Organization	Yes or No	Additional Comments Received
		Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. o Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described suggested above and meet FERC Directives in order 706.
Volkmann Consulting, Inc.	Negative	The industry has already approved Version 4 and has gauged its impact and has started to prepare for implementation. Version 4 meets the FERC 706 order and should be given an opportunity to be implemented and evaluated before rushing to implement a comprehensive change to the industry. Version 5 standards go beyond FERC Order 706. The focus of the change to Version 5 should be to meeting the rest of the 706 order, not expanding it. More definition is need around 15 minute failure period and impact. Many small entities' performance of a particular BES Reliability Operating Services has little or no impact to the operation of the BES. Yet failure of a BES Cyber asset may impact their ability to perform the BES Reliability Operating Services and hence subject to the CIP standards. Low Impact category is discriminatory towards smaller entities because it will capture facilities that when similarly situated in a larger entity would not be included in the low category because it does not impede the larger entity's ability to performance the service. The Low category was not prescribed by the FERC 706 Order. For that reason and the above discussion, Low Impact should be eliminated in this round of standard drafting and be part of a larger FERC NOPR process. Much of the fear and possible negative votes is the uncertainty of meeting a very complicated set of standard. The SDT should consider recommending to FERC that enforcement of the standard coincide with completing and mitigating an initial Compliance Audit.
Lakeland Electric	Negative	Transmission Owners do not have Control Centers (TOPs-have Control Centers).
Muscatine Power & Water	Negative	Understanding that CIP version 4 has been approved by the NERC BOT and awaiting approval from FERC, MPW recommends that CIP-002-5 be placed on hold at this time. Our industry has approved CIP-002 Version 4 and the terms "Critical Assets" and "Critical Cyber Assets" are well known terms within our current Cyber Security plans. This proposal meets the main FERC goal of including more Critical Assets without requiring a reduction in reliability by forcing entities to retool their existing programs from scratch. As currently drafted, Version 5

Organization	Yes or No	Additional Comments Received
		of the CIP standards: Â· Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES Â· Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls Â· Does not consider that smaller Entities have a much lower impact on the BES Â· Greatly exceeds FERC's 706 order without justification Concerning CIP-002-5 Attachment 1, MPW can easily see that there is some stratification afforded to TOP and GOP Control Centers, based on voltage levels, total MW, total MVAR, number of Transmission lines, Blackstart Resources, etc, for being considered High Impact, Medium Impact, or Low Impact. While the SDT has acknowledged there are some distinct differences between larger and smaller TOP's and GOP's, MPW wants to point out that not all Balancing Authorities are created equally. Does anyone think that the smallest BA in North America, serving 38 MW of load, has the same Reliability Impact as a BA serving 10,000 MW, or more, of load? Does it really improve the reliability of the BES to have ALL those smaller BA Control Centers carry the same High Impact Rating? In addition, MPW agrees with all the comments submitted by the MRO NSRF.
Salmon River Electric Cooperative, Alameda Municipal Power, City of Lodi, California	Negative	We believe the drafting teams work is very valuable and provides a good basis for appropriately allocating responsibilities according to the impact to the BES. However we feel additional work is needed due to a discrepancy between the definition of BES Cyber Assets and the applicability to entities with UFLS or UVLS equipment. Definition of BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset. Applicability: Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or regional Reliability Standard o A UVLS program required by a NERC or regional Reliability Standard o A Special Protection System or Remedial Action Scheme required by a NERC or regional Reliability Standard o A Transmission Protection System required by a NERC or regional Reliability Standard o Its Transmission Operator's restoration plan Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS program required by a NERC or regional Reliability Standard o A UVLS program required by a NERC or regional Reliability Standard The discrepancy exist because (1) The definition states "The timeframe is not in respect to any cyber security events or incidents,

Organization	Yes or No	Additional Comments Received
		but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES." (2) LSE's and DP's with UFLS equipment are required to comply with the proposed CIP Standards over BES Cyber Assets when these devices are not consider BES Cyber Asset per definition. (3) These devices sense a system condition and do not send or receive instructions. In fact in some regions a UFLS device is not required to be a cyber-equipment type. For example, in the NPCC region an electro-mechanical relay can be used to fulfill an organizations UFLS program requirement. Proposed recommendation: Modify the applicability. "Load Serving Entities and Distribution Providers with a load shedding program that is activated through receipt of an instruction to its cyber processor to operate."
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
NorthWestern Energy	Negative	NorthWestern Energy supports the proposed Issue/Solution below: Issue: As currently drafted Version 5 of the CIP standards: o Would significantly increase cost without a commensurate increase in the reliability, safety, or security of the BES. o Create significant complexity, confusion, and administrative burden regarding the identification of Critical Cyber Assets, the definition of terms, and implementation of Cyber Controls. o Exceeds FERC's 706 order without justification or improving the security of the BES. o Many of the draft requirements add significant bureaucracy without adding security. The industry needs focus on improving security of the BES and not the security of individual assets or the appearance of security through the addition of administrative requirements. Proposed Solution: 1. Retain CIP-002-4 as approved by the industry in 2010. It is filed with FERC; industry and NERC comments on the FERC NOPR recommended FERC approval. This will: o

Organization	Yes or No	Additional Comments Received
		Eliminate the confusing and complicated process developed to identify BES Cyber Systems proposed in Version 5 o Meet FERC's 706 for CIP-002-1: o Industry approved guidance documents for identifying Critical Assets and for identifying Critical Cyber Assets. Â¶253-258, 270-27 o CIP-002-4 replaces the Critical Asset guidance and aligns with FERC's affirmation that the applicable responsible entities are responsible for identifying Critical Assets. Â¶319-321 o CIP-002-2 added senior manager approval of risk-based methodology. Â¶294-297 o Not exceed FERC Order 706: o Â¶284: "... there is no formally accepted method for identifying critical cyber assets before us at this time ... we decline to direct that such a method be incorporated into the CIP Reliability Standards at this time." o Â¶285: "CIP-002-1 provides that a critical cyber asset must either have routable protocols or dial up access ... We do not find sufficient justification to remove this provision at this time." 2. Develop a new standard for High Impact Assets: o That identifies which assets in CIP-002-4 are High Impact and o Clearly states the extra protection required for High Impact Assets: o The Draft version 5 identifies eight extra protections, most are in response to FERC Order 706. o Provides opportunity for a separate implementation timeline for the additional controls that apply only to High Impact assets. o Provides flexibility in adjusting controls on High Impact assets. In the future only one standard has to be modified. o Entities that do not have High Impact assets will not have to sort through all the standards and RSAWs to assure compliance and security. 3. Develop a separate standard for the Low Impact assets or abandon this concept. o Lows were not directed by FERC Order 706 nor included in the SAR. o A separate standard provides full transparency in the stakeholder process. o This is a scope expansion not supported by many in the industry. o Cost and compliance concerns with lows include whether lows have to be listed. This is a derivative of which controls are selected and how they are designed and audited. 4. Revise CIP-003-5 through CIP-011-5 and Definitions to reflect changes described suggested above and meet FERC Directives in order 706.
Manitoba Hydro	Negative	Please see comments submitted in electronic commenting form. In addition, Manitoba Hydro has the following general comments on CIP Version 5: -The Application Guidelines section provides no indication of how binding this section is. In fact, including it within the standard carries the impression that the Guidelines are more binding than before. In order to clarify that the Guidelines have not become more mandatory than today, this section should reinstate a Preamble with the following words: "Guidelines provide suggested guidance on a particular topic for use by BPS users, owners, and operators according to each entity's facts and circumstances and do not provide binding norms, establish mandatory reliability standards, or create parameters by which compliance to standards is monitored or enforced." -"Initially upon the effective date "in all Standards means beginning on the effective date. As written, action required "initially upon effective date" must be performed ON the effective date. This may be an unintended consequence of the wording. Was the intent "on or before" the effective date? If "on or before the effective date" is not the intent, then the statement "initially upon the effective date" is unnecessary since all requirements

Organization	Yes or No	Additional Comments Received
		for all standards must be implemented upon the effective date. -"All Responsible Entities" used in the Applicability column of the requirement table is confusing. Are these the entities identified by Functional Entities in Section 4 Applicability, or are the "All Responsible Entities" defined by the bullets in Section 5 Background Applicability? To maintain consistency and clarity with all the other requirements, we suggest replacing "All Responsible Entities" with the specific Cyber Assets in scope, for example, BES Cyber Assets. -Measures in the Requirement Table are supposed to indicate the body of evidence for the requirements, but as currently written, “may include” allows that the evidence may not include any of the items in the list. If there are some characteristics or criteria which are expected as part of the body of evidence, such as descriptions, signatures or dates, which are independent of the evidence types, such as paper records, electronic files or computerized systems, then these characteristics or criteria should be indicated in the measures as “Evidence shall include, ...”, instead of “Evidence may include, ...”. If the body of evidence is expected to include the listed items, we suggest changing the word “may” to be “shall”. -Introduction - Applicability Section: The phrase “designed, installed and operated for the protection or restoration of the BES” is used in Sections 4.1.2, 4.1.6, 4.2.1 and 4.2.2. Is this phrase necessary? Are some of the facilities not designed, installed and operated for such purposes? If the phrase is retained, is it clear which facilities are applicable? In 4.1.2, 4.2.2 a restoration plan is referenced, but is a restoration plan a “system or program”. Also, can a facility be “part of” a restoration plan? -4.1.2: We suggest adding clarity by changing "Its Transmission Operator's" to "The Distribution Provider's Transmission Operator's". -4.2.2: We suggest adding clarity by changing "Its Transmission Operator's" to "The Distribution Provider's Transmission Operator's". -Background: the meaning of three terms is explained, but it is not clear why these are not simply added to the list of defined terms. Are these meanings binding on NERC? Also, the distinction between “processes”, “plans” and “programs” is unclear. If programs and plans are types of documented processes, this should be stated. Background - Applicability Section: -High Impact BES Cyber Systems (for CIP-003-5 through CIP-011-1): We suggest changing "... each BES Cyber Systems ..." to "... each BES Cyber System ..." We suggest moving the sentence "Responsible Entities can implement ... across multiple BES Cyber Systems." to the Applicability section, just before the sub-bullets. This sentence is more general guidance, since it applies to not only High Impact BES Cyber Systems, but also Medium Impact BES Cyber Systems. This also adds consistency to the wording of the local definitions in Standards CIP 003 5 through CIP-011-1. -Medium Impact BES Cyber Systems: We suggest changing "Systems" to "System". -Medium Impact BES Cyber Systems with External Routable Connectivity: The meaning of "... directly accessed through External Routable Connectivity" is unclear. If this is an exclusion, does it only apply to Medium Impact BES Cyber Systems with External Routable Connectivity? -Low Impact BES Cyber Systems with External Routable Connectivity: We suggest changing "... each Low Impact BES Cyber Systems ..." to "... each Low Impact BES Cyber System ...". For clarity, we suggest changing” ... High or Medium" to” ... High Impact or Medium Impact". -Associated Electronic Access

Organization	Yes or No	Additional Comments Received
		Control or Monitoring Systems: We suggest changing "... BES Cyber Systems." to " ... BES Cyber System." -Associated Physical Access Control Systems: We suggest changing "... BES Cyber Systems." to "... BES Cyber System." -Associated Protected Cyber Assets: We suggest changing "... BES Cyber Systems." to "... BES Cyber System." -Electronic Access Points: This local definition is different than the proposed NERC Glossary of Terms definition. If the intent is to address associated Electronic Access Points, then to provide clarity and consistency with the other local definitions, we suggest changing this local definition title to "Associated Electronic Access Points". If "associated" was not intended, then this definition should not differ from the proposed NERC Glossary of Terms definition. -Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries: This local definition is only referenced in CIP-006-5 and should not be included as a local definition in any standards where it is not used. Only local definitions which are used in a specific standard should be included as a local definition of that specific standard. Compliance -1.1 - Compliance Enforcement Authority: should read "Compliance Enforcement Authority shall be the Regional Entity, or' and then go on to list the 3 other options in the bullets. The second bullet - the words 'to be responsible for compliance enforcement' could be replaced with 'to serve as the Compliance Enforcement Authority'. -1.2 - Evidence Retention: It is not clear how a Responsible Entity can retain data "for the duration of a regional or CEA investigation". The term "investigation" can include a compliance audit, a spot check or compliance investigation. The latter 2 monitoring tools can be initiated at any time by the CEA. -Requirement Section: all requirements should refer to applicable "requirements" in a table, rather than "items" in a table.
Baltimore Gas & Electric Company	Negative	Baltimore Gas and Electric Company would like to thank the Standard Drafting Team for their tremendous effort in developing the CIP standards. This is a complex and challenging endeavor. While BGE is voting negative at this time, BGE remains optimistic that the ongoing stakeholder process can refine the language into an approvable set of standards. The items of concern behind the negative vote are spelled out in the comments submitted by Constellation Energy on our behalf. Extensive input is provided on the definitions. Because the definitions apply to the suite of CIP standards, they must be acceptable in order for the standards to be acceptable. Further input is provided on the specific standards in the comment form as well. Where possible, Baltimore Gas and Electric proposed revisions. It is critical that the standard language include clear and objective measures that minimize potential differences in perspective when judged for compliance. We support the pursuit of quality security measures that ensure BES reliability, but are sensitive to overly burdensome compliance obligations. Thanks again to the drafting team.
Liberty Electric Power	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since

Organization	Yes or No	Additional Comments Received
LLC		the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Power Energy Group LLC, Volkmann Consulting, Inc.	Negative	The industry has already approved Version 4 and has gauged its impact and has started to prepare for implementation. Version 4 meets the FERC 706 order and should be given an opportunity to be implemented and evaluated before rushing to implement a comprehensive change to the industry. Version 5 standards go beyond FERC Order 706. The focus of the change to Version 5 should be to meeting the rest of the 706 order, not expanding it. By mixing High, Medium and Low Impact requirements with the context of each standard creates a very complicated set of standards to administrate and to evaluate, especially in an audit environment. Reaching consensus and implementation of important High and Medium requirements may be impeded by failure to reach agreement on the Low Impact. It is recommended to segregate the requirements into High, Medium and Low standards, so that standard is only applicable to a particular level of Impact. More definition is need around 15 minute failure period and impact. Many small entities' performance of a particular BES Reliability Operating Services has little or no impact to the operation of the BES. Yet failure of a BES Cyber asset may impact their ability to perform the BES Reliability Operating Services and hence subject to the CIP standards. Low Impact category is discriminatory towards smaller entities because it will capture facilities that when similarly situated in a larger entity would not be included in the low category because it does not impede the larger entity's ability to performance the service. The Low category was not prescribed by the FERC 706 Order. For that reason and the above discussion, Low Impact should be eliminated in this round of standard drafting and be part of a larger FERC NOPR process. Much of the fear and possible negative votes is the uncertainty of meeting a very complicated set of standard. The SDT should consider recommending to FERC that enforcement of the standard coincide with completing and mitigating an initial Compliance Audit.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
Portland	Negative	PGE takes cyber security very seriously, especially as it relates to the critical infrastructure

Organization	Yes or No	Additional Comments Received
General Electric Co.		necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. While PGE supports the overall goals of the Version 5 standards, PGE is voting NO because the standard is worded in a way that PGE believes could create confusion and goes beyond the scope of what FERC required in Order No. 706. For additional information, please see PGE's separately submitted comments.
Liberty Electric Power LLC	Negative	In addition to the survey comments, the inclusion of the following sentence in the compliance measures section needs to be removed to make the standard acceptable: For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit. There is no BES reliability benefit for six years of documentation on many of these requirements. In those cases where there is such a benefit, the standard should be written with a six-year retention requirement.
NRG Energy, Inc.	Negative	3) Under R3 TFEs would still be required under the medium or high impact levels unless these systems are upgraded or replaced.4) If a high or medium impact system is required to alert in real time for events that necessitate a real time event in R4.2, why is necessary to review a sampling every two weeks under R4.5? 5) Under R5.2, the senior manager or delegate may be too removed from the actual access control process to authorize individuals and provide access permissions for various accounts. 6) CAN-0017 is in direct conflict with R5.5 which allows either technical or procedural controls for enforcement of password parameters. CAN-0017 forces TFEs unnecessarily. 7) Under R2, Assessments on Vulnerability notices may take more than 30 day period. 8) What is the CIP Exceptional Circumstance definition? It is not listed
Southwest Transmission Cooperative, Inc.	Negative	On page 39 of the application guidelines in section 1.2, Component should be made lower case. Part 5.5.2 needs to be refined further. It needs to be clear that maximum complexity regarding character types in the password applies if the BES Cyber System cannot support at least three character types. We suggest appending "if less than three character types" to the end of the requirement for further clarity. Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed.
Kansas City Power & Light	Negative	Proposed standard introduces additional uncertainty, confusion and misunderstanding.

Organization	Yes or No	Additional Comments Received
Co.		
Hydro-Québec TransÉnergie	No	since there is no place for on general comments, see responses in the to the last question (49)Under "BES Reliability Operating Services" o “Identify and monitor flow gates” under “Managing Constraints” appears to be missing its bullet o Recommend that “Change management” under “Situational Awareness” be clarified to changes in the BES instead of IT change management o Recommend clarification that “Facility” is the NERC Glossary Term -- in “Facility operational data and status” under “Inter-Entity Real-Time Coordination and Communication”o Request clarification on the scope of this “Operational Directives”. Does it include company messaging system? Two way radios? What is the relationship with the new COM-002?o Request clarification that these Coordination and Communications are limited to Reliability not Market Systems o recommend that each BES Reliability Operating Services have a beginning paragraph that clearly associates that service to the BES like the "Dynamic Response to BES Conditions" o For clarity, recommend stating which Functions are associated with each BES Reliability Operating Services instead of forcing everyone to interpret
Pacific Northwest Small Public Power Utility Comment Group		The comment form provided no room for comments not addressing particular requirements, so we are listing our more general comments here.From the webinar we understand that where the requirements refer to tables where none of the table entries applies to an entity, the requirement itself is not applicable. Since this is not the general case for the relationship between requirements and sub-requirements in NERC standards, we suggest explicitly stating that this is how it works in the CIP standards.We find the Applicability-Facilities Section (4.2) in CIP-003 to be confusing, since all the requirements of this standard appear to apply to the applicable entities and not to facilities. Suggest removing the 4.2.1 through 4.2.3, or stating more clearly how the facilities affect the requirements.The background section of CIP-003 goes into great detail regarding the table format while CIP-003 itself does not follow this format. Please remove or rewrite this section.The very last statement of the guideline section of CIP-005 references a document we are not familiar with. Please provide a complete reference or link to its location.

Additional Comments Submitted:

Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)
Corresponding additional information provided:

In addition to the background mapping matrix, the CSWG is also providing a narrative introduction to the methodology used to develop the mapping and prepare our "Official Comments:"

The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has developed a mapping between NERC CIP v5 requirements and the high-level security requirements (HLRs) in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, *Guidelines for Smart Grid Cyber Security*. The NISTIR 7628 is available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

This mapping identifies any gaps between CIP v5 and the NISTIR 7628 HLRs and recommendations to the CIP drafting team to consider. The complete mapping (Excel file) will be submitted to the CIP drafting separately as a reference document. Some sections of the comment form have been left blank because no gaps or recommendations were identified.

The CIP-002-5 criteria provide a sound approach for identifying low, medium, and high impact systems within the BES. This three level approach aligns well with the three level approach (i.e., low, moderate, and high) used within the NISTIR. Most requirements in the current CIP drafts are applicable to both medium and high impact systems as a bundled pair and they are silent on their applicability to low impact systems. In contrast, the NISTIR uses a graded requirement approach that specifies baseline controls that apply at low impact levels and then specifies strengthened controls for moderate impact and even stronger controls for high impact levels. The CIP version 5 standards will be significantly strengthened if they were to incorporate a similar graded approach when applying requirements.

Please see the Excel Spreadsheet attached to this document for review.

_____

Xcel Energy
Alice Ireland
Question 16

16. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Comments: Under the proposed CIP-004-5, attestations from contractors or service vendors for personnel risk assessments (PRAs) are explicitly permitted as proof that a PRA was completed prior to granting a contractor or vendor employee access to the various systems and assets covered by the Standard. We would like to request consideration for also including as acceptable evidence attestations from entities who share access to covered assets within a shared facility, such as a substation. We request the addition of language to Part 5.1, which describes the acceptable evidence of compliance with this obligation, to state that "evidence may include, but is not limited to . . . Dated documentation or attestations from ***contractors, service vendors or entities with shared access at a facility*** verifying that personnel risk assessments were conducted pursuant to CIP-004-5 R4 before access was authorized."

_____

Pacific Northwest National Laboratory
David McKinnon, Sam Clements and Paul Skare

See attachment

END OF REPORT

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Tel: (509) 372-4210
Fax: (509) 372-4353
MSIN: K1-85
paul.skare@pnnl.gov

January 3, 2012

Laura Hussey
Standards Process Manager
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA

Dear Laura,

I wish you a successful 2012! During GridEx, you invited me to provide comments on NERC CIP v5. We had a parallel request from DOE, so we are able to provide you both with the comments.

David McKinnon, Sam Clements and Paul Skare from PNNL all contributed to this review. We realize that there is an electronic response form as well as a document form that are being used to collect comments on this draft standard. As we attempted to use these tools we felt that our comments did not fit well with the confines of the provided forms and thus decided to provide our comments as follows. You will find our responses in two categories 1) general comments that apply to the standards as a whole, and 2) specific comments for each of the individual standards. We did not spend the time to wordsmith or format to great lengths, so please excuse any vagaries. Our spirit in the review was to genuinely have impact to improve the final product NERC puts out. We hope that you find them useful and are happy to discuss further if you have questions.

General Comments

With NERC CIP v5, we believe a graded security approach with low, medium and high impact on the BES is a sound approach, but have found it mostly focused on medium and high impact systems, and mostly the medium and high impact systems are bundled as a pair. For example, some password requirements are given for medium and high impact systems, but the draft is completely silent about what should be done for low impact systems. There is no reason not to mandate a no default password policy for ***all*** systems within the BES. Yes, there might be a few cases where legacy systems

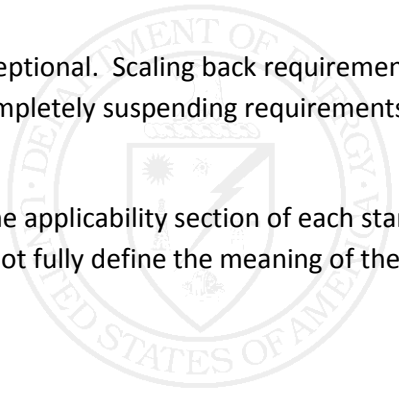
do not support anything but hard-coded defaults, but these could be documented en masse as exceptions (with associated compensating controls) rather than let these exceptions be used as an excuse to allow a poor password policy.

In an effort to reduce the burden to industry we recommend including a grandfather clause that provides certain exceptions for legacy low-impact systems (such as those that do not have external computing interfaces or capabilities).

As noted, the systems are graded into low, medium, and high, but the requirements/controls are not applied in a graded three-tier approach. Most requirements lump high and medium into one category and ignore low. Ideally we should have requirements that get successively stronger as we migrate from low to medium to high.

There are a number of concerns that either exist in multiple places throughout the CIP standards or are applicable to the standard as a whole they include:

- Consistency of the capitalization of terms
- Consistency in the use of the terms Cyber Asset and Cyber System
- Consistency in the use of the terms Cyber access and electronic access
- Section 4.2.4.2 of many of the requirements use the term Electronic Security Perimeters. Has this been deprecated?
- We disagree with Section 4.2.4.2 as an exemption - Communication links should be protected between ESPs
- As defined, CIP Exception circumstances are not that exceptional. Scaling back requirements within an exceptional circumstance is acceptable, but completely suspending requirements is not.
- Include a definition of terms section to the standards. The applicability section of each standard defines how the term applies to that standard but does not fully define the meaning of the term.



CIP-002-5

4.1.2 How are smart grid devices being operated by Distribution Providers?

- Battery Storage is another question that is not addressed
- Other smart grid assets (100KV+)

4.2.4.x Cyber Assets should be prefaced by BES
Should the last paragraph on page 7 say “cyber security plan”?

CIP-003-5

4.2.4.4 What is the definition of Cyber System vs. Cyber Asset? There is a need for consistency in use – especially in the tables.

5. Background – It seems this entire section is predicated upon a table which is missing. There is no table [Table Reference] pg 7 and under Applicability there is no table to aid in understanding of all the different “Applicability Columns”

R2 Should include a Procurement Policy requirement

R2 Should include a Resiliency Policy requirement

R2 1.5 System Security: Should include third-party, outsourcing, and availability or be considered as separate topics.

Guidelines
R2 2.1 Personnel Security: Should explicitly include subcontractors and outsourced services

R2 2.3 Remote Access should be moved into System Security

Include language in contracts that requires vendors, contractors, or consultants adhere to the Responsible Entity’s policies and controls.

R2 2.7 Recovery Plans should include a prioritized recovery strategy

CIP 004-5

Purpose: Should also include the case where one organization has equipment in another organizations facility (i.e. Substation)

R3 The wording of the requirement is confusing. The measure for 3.1 does a better job defining the requirement than the requirement.

CIP 005-5

R1 1.2 The requirements column should state “Control and secure all connectivity through the use of identified Electronic Access Points (EAPs). “

R1 1.4 Eliminate the “where technically feasible” loophole. The statement should simply be “Perform authentication when establishing dial-up connectivity with the BES Cyber System.”

R1 1.4 Dial-up access for either non-interactive or interactive sessions should be authenticated. As written, 1.4 only protects non-interactive sessions.

R2 Eliminate the “where technically feasible” loophole. The statement should simply be “Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items.”

NEW: As written, low impact systems do not have to be protected with passwords, nor are the users required to be authenticated. Requirements for low impact systems should be added.

CIP 006-5

M1. Typo: - As stated “Evidence must includes…” should be “Evidence must include…”

R1 1.5 Clarification needed with respect to the applicability column as to what impact level the associated physical access control systems apply. Explicitly state that this applies to all systems.

R3 3.1 High and medium impact systems should have their associated physical access control systems monitored (and tested) more frequently that once every 24 calendar months. Testing frequency should be dependent upon the impact level (i.e. annual testing of a control center is not too frequent).

CIP 007-5

The requirements in this section should follow a graded approach to match the impact level of the various systems where the lower the impact level the more time or leniency is afforded to meet the requirement.

R2 Patch management is optional for low impact systems. Even these systems should have patches applied, but perhaps in a less timely manner than is required for medium and high impact assets.

R3 Malicious code protection is not required for low impact systems. Even these systems should be monitored/protected.

R4 Once again, low impact systems are not included. Security event monitoring should also apply to low impact systems.

R4 4.5 Two week lag before logs from high impact systems have to be reviewed. The reviews should be more timely, especially if only one calendar day is given to rectify issues discovered. We saw in GridEx how timeliness is important in this area.

R5 Password management is not specified for low impact systems. No guidance is given regarding sharing/reusing passwords between systems.

R5 5.4 Eliminate the “where technically feasible” loophole. The statement should read “Procedural controls for initially changing default passwords unless the default password is unique to the device or instance of the application…”

R5 5.6 Eliminate the “where technically feasible” loophole.

CIP 008-5

Seem OK. However, the definition of a reportable incident seems a bit vague.

CIP 009-5

No comments.

CIP 010-5

R1 1.2 Worded poorly. (Currently: Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.) Should more clearly state that (pre) approval is needed for configuration management changes.

R2 2.1 Caveat of "where technically feasible" applies to both medium and high impact systems. Compensating controls should be applied to high impact systems when built-in monitoring of baseline changes is not technically feasible.

R3 3.3 Change in phrase order makes the requirement easier to understand "Perform an active vulnerability assessment prior to adding a new Cyber Asset to a Cyber System or Electronic Access Control or Monitoring System, except for CIP Exceptional Circumstances.

CIP 011-5

No uniform requirements for how BES Cyber System Information is to be handled. Is it business sensitive, official use only, etc? Furthermore, does the level of protection vary based upon whether the information is about high impact or medium impact systems?

Missing a statement about how one is authorized to view BES Cyber System Information. How does one get added to the list of those with a "need to know" the information? Especially regarding external entities such as vendors, contractors, DOE, NERC, etc. the aspect of trust and the needed controls for trusted parties would be useful.

Sincerely,

Mark Morgan
Advanced Power and Energy Systems
Pacific Northwest National Laboratory