Individual or group. (119 Responses)
Name (77 Responses)
Organization (77 Responses)
Group Name (42 Responses)
Lead Contact (42 Responses)
Question 1 (106 Responses)
Question 2 (107 Responses)
Question 3 (0 Responses)
Question 3 Comments (119 Responses)
Question 4 (100 Responses)
Question 5 (102 Responses)
Question 6 (100 Responses)
Question 7 (102 Responses)
Question 8 (100 Responses)
Question 9 (101 Responses)
Question 10 (0 Responses)
Question 10 Comments (119 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
No comment
Yes
Yes
Yes
Yes
Yes
Yes
No comment
Individual
Monica - TEST
TEST
Yes
Yes
this is a test to add comments to a field.
Yes
Yes
Yes
Yes
Yes
Yes
test
Individual
John Falsey
Edison Mission Marketing & Trading
Yes
Yes

Yes
No
Yes
No
Yes
Yes
CIP-003-5 R2-I agree with Cyber systems in the Medium and High categories need documented policies, but not for the low category
Group
Northeast Power Coordinating Council
Guy Zito
No
No
Request clarification on the Applicability of Distribution Providers (DP) and Load Serving Entities (LSE). 1. Does 4.1.2 mean that any DPs owning assets in 4.2.2 need to comply with these CIP Standards? 2. Does 4.1.6 mean that LSEs owning assets in 4.2.1 need to comply with these CIP Standards? 3. Does 4.2.2 mean that only these DP assets are covered by these CIP Standards? 4. Does 4.2.1 mean that only these LSE assets are covered by these CIP Standards? 5. Does the DP's third bullet in 4.2.2 apply to only protection systems, not UFLS or UVLS since those load shedding systems are covered by the DP's first bullet? Note the NERC definition of "protection systems" includes load shedding systems, which generates this question. 6. Section 4.2 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. Request clarification on High Impact 1.3 and 1.4's use of "associated data centers". Are these the "computer rooms" that service a Control Center? Request clarification on the Standard Drafting Team (SDT) expectations on Medium Impact 2.1. Does the SDT expect that the "aggregate highest rate net Real Power capability of the preceding 12 months" will not flip flop on this threshold? In other words, does the SDT expect these asset to remain on one side or the other of this threshold? Recommend a change to R1's VSLs since Lower and Severe use 100 or more High and Medium BES Cyber Systems while moderate and High uses BES Cyber Assets. Request clarification and consistency. Recommend BES Cyber Assets so that ISOs can easily hit their thresholds. Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: "Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; " Suggested rewording: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; Requirement 1.3 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: "Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;" Suggested rewording: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;
Yes
Yes
Yes
Yes
No
No
Recommend changing M5 from "signed" to "approved" since some companies use other approval processes. Also these Measures criteria need to be aligned with the Requirements. Measure M5 includes "to approve or authorize specifically identified items" while R5 states "and approved by the CIP Senior Manager". Request a re-written M6 since it appears to add a new Requirement--"that

within 30 days of discharging the delegated authority". Recommend updating CIP-003 R2's Violation Risk Factor in the Table of Compliance Elements. That VRF is "medium" while the Requirements and Measures show R2 as "low".
Group
AEP Standards based SME list
Gerald Freese
Yes
Yes
No
No
Yes
Yes
Yes
CIP-003: 1. R2 – What level of detail is required in the cyber security policy for Low impact BES Cyber Systems? How strict must the security program defined in this policy be? There are no requirements in CIP-004-CIP-011 to use as guidance. With the existing Version 3 standards Responsible Entities cyber security policies are reviewed by auditors to determine if each of the CIP-004-CIP-009 requirements are repeated word for word from the standard; presumably this will be expected by the auditors for High and Medium BES Cyber Systems under R1. What will be used as guidance under R2? In addition, the following is a previous comment that still has outstanding issues: 2. AEP believes the inclusion of the word "implement" in CIP-003-5 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. 3. (1) R1 – The implementation and documentation of the items 1.1-1.10 that are required to be defined in the cyber security policy are also implemented as part of CIP-004-CIP-011 compliance. This represents double jeopardy. (2) R2 – What level of detail is required in the cyber security policy for Low impact BES Cyber Systems? How strict must the security program defined in this policy be? There are no requirements in CIP-004-CIP-011 to use as guidance. With the existing Version 3 standards Responsible Entities cyber security policies are reviewed by auditors to determine if each of the CIP-004-CIP-009 requirements are repeated word for word from the standard; presumably this will be expected by the auditors for High and Medium BES Cyber 4. 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. 5. In CIP-003-5 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.
Individual
Brian Evans-Mongeon
Utility Services Inc.
No
No
The following comments concern the Applicability section of all of the CIP standards CIP-002-5 through CIP-009-5, CIP-010-1, CIP-011-1. (1) Use of "Facilities" (1.a) Section 4.2 is titled "Facilities" with a capital F. The capitalization designates this section as a defined NERC Term. This may be viewed as applying the standard to a broader area than intended, and not to only those facilities identified within section 4.2. Modifying the language from "Facilities" to "Systems covered by this Standard" would alleviate the confusion. (1.b) The use of "BES Facilities" is inappropriate as it is not a

defined term. The definition of “Facilities” refers to BES Elements making the use of “BES Facilities” redundant. (1.c) Section 4.2.4.1 again states “Facilities” with a capital F. In this case it is seems that the NERC defined term is the intent, and not the meaning throughout the rest of section 4.2. This inconsistence will invariably lead to some level of confusion. (2) Applicability of LSE’s: LSEs, as determined by NERC in 2008, do not own or have physical assets. Because no assets are actually owned, LSE’s should be removed from the applicability section of the standard. If it is determined that an LSE does own physical assets are these standards only applicable to those assets identified in 4.2.1 (3) Protection Systems inclusive of UFLS and UVLS: The DP’s third bullet in 4.2.2 does not clearly apply to only transmission Protection Systems, excluding UFLS or UVLS since those load-shedding systems which are covered by the DP’s first bullet. Note the NERC Definition of "Protection Systems" includes load-shedding systems and PRC-005-2 will group UFLS and UVLS systems alongside other Protection Systems. Clarification is required to ensure UFLS and UVLS systems under 300MW are removed from applicability. We recommend revising the third bullet to read "A Protection System (other than a UFLS or UVLS System) that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard." (4) To make it clear that the standards apply only to DP owned systems listed in section 4.2.2, suggest adding the following in the Exemptions section: “4.2.4.4 Cyber Assets that are owned by Distribution Providers or Load Serving Entities and that are not associated with the Facilities, Systems and equipment described in 4.2.1 or 4.2.2.” (7) R1.1 Utility Services support the comments made by Massachusetts Municipal Wholesale Electric Company in that R1.1 appears to require the entity to maintain a list of “Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.” This seems to be inconsistent with what is stated in the Rationale and the Guidelines, which only refer to identifying BES Cyber Assets and BES Cyber Systems. We suggest that the SDT clarify the intent and the auditable requirement by adding an explanation to the Rationale, Guidelines or M1. (6) R2 - It is unclear exactly what is to be reviewed. The rationale for R2 starts with “The lists required by Requirement R1 are reviewed”. The bullet for R1.3 states “shall default to the category of low impact and do not require discrete identification”. Our understanding is that “discrete identification” is synonymous with “list”. It seems that based on R1.3 a list would not be created for Low Impact but per R2 this non-existent list must be reviewed. It may be interpreted that the only way to review a blank list is to review a list of all cyber systems and then justify why each system is either not listed as a High, Medium or Low asset. Recommend that the annual review requirement be added to R1.4 and clarify that the review is of the “identification” process and resulting lists.
Yes
Yes
Yes
Yes
Yes
Yes
(1) The Violation Risk Factor stated in CIP-003-5 R2 should agree with the VRF listed in the Table of Compliance Elements. (2) It should be clarified that the contents for the policies listed in R1 and R2 are not required to include elements that maybe detailed in other CIP standards. I.e.. The R2.4 Incident response to a BES Cyber Security Incident does not require the elements and timelines contained in CIP-008-5. (3) Utility Services agrees with and supports the comments submitted by MMWEC concerning R1.1.
Group
Snohomish County PUD
Benjamin Beberness
Yes
Yes
Impact Rating Criteria: Medium Impact Rating 2.5 – Snohomish would like clarity on how the ”Weight Value per Line” is applied. Medium Impact Rating 2.10 – The CIP-002-5, 2.10 wording is confusing and should be clarified - would CIP-002-5, 2.10 apply to an RE with a load over 968 MW in the Western Interconnection just because their UFLS scheme requires the arming of 31% of the load-meeting the 300 MW armed load threshold? The electric industry is confused on how to interpret the UFLS/UVLS thresholds in CIP-002-5, 2.10 and there are a number of interpretations being discussed

in various forums which highlights the need for clearer language. Public Utility District No. 1 of Snohomish County (“SNPD”) interprets the latest CIP-002-5, 2.10 language “…Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW…” to mean a registered entity can arm 300 MW of load and over in its UFLS/UVLS program, if the System or group of Elements are installed at numerous circuits, feeders, or station (less than 300 MW individually) where a failure of the System or group of Elements is not under a common control system (or power source/battery) the CIP-002-5 would not apply. SNPD requests that the SDT comment on whether the interpretation above is accurate. Furthermore, SNPD ask that an example be added to the Application Guidelines for 2.10. The example should highlight a UFLS or UVLS program that meets or exceeds 300 MW but is separated into multiple System or group of Elements where all System or group of Elements are less than 300 MW individually and therefore would not meet the CIP-002-5, 2.10 thresholds. Secondly, because UFLS and UVLS requirements are addressed in the family of PRC Reliability Standards SNPD supports removing the UFLS, UVLS, and other safety net schemes from the family of CIP Reliability Standards. Medium Impact Rating 2.11 – SNPD disagrees with the CIP-002-5, 2.11 as it dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria (“SCRC”), section III (d), uses the same criteria to define both Transmission Owner (“TO”) and Transmission Operator (“TOP”) . In addition, the application of this criteria, especially as to under what circumstances an entity is a TO and not a TOP is not defined and is not consistent through the regions. SNPD supports removing section 2.11 as there is no “reliability based” justification that registration as TOP justifies a Medium Impact Rating. If they registration thresholds were removed from section 2.11 SNPD would change its vote to affirmative. General comment: If a TO is also a GO and either the TO or GO requirements result in a medium or high impact rating, it is not clear whether the impact rating applies to all Cyber Assets that support the TO and GO operation or just the category that triggers the high or medium impact rating. The SDT should clarify this concern. The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the current or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version 5 CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the BES. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD’s customers are exposed to all disturbances on the main grid. However, SNPD also supports efficiency and spending significant resources with little to no benefit is not beneficial to the reliability of the BES or to the Level of Service (“LOS”) SNPD provides its customers.
Yes
No
Yes
Yes
Yes
Yes
CIP-003-5 R2 NIST clearly outlines what should go into a cyber security program. Snohomish would recommend that NIST is referenced. Additionally, cyber security policies should include the life cycle of a cyber asset: Pre-purchase • Vendors and utilities follow secure development life cycle • Utilities ensure contractual language regarding security in contracts • Utilities utilize security best practice through RFP and contract negotiations. o Include language in contract stating that the software will be tested and security incidents will be categorized. o Include contractual language that states security vulnerabilities based on their category must be resolved prior to go live. o Etc. Implementation • Utilities utilize security best practice through project lifecycle. o Test for security vulnerabilities o Treat as defects and ensure that system does not go live with any critical issues. o Etc. • Document the security design and architecture of the system • Utilities utilize security best practice through project lifecycle. Monitor/control/ Incident response • Document your security monitoring process and demonstrate implementation • Document the security controls and demonstrate implementation •

Document how the organization will respond to a cyber incident and exercise the plan.
Individual
Anthony Jablonski
ReliabilityFirst
ReliabilityFirst votes in the affirmative for the standard but offers the following recommendations regarding the Violation Severity Levels. CIP-002-5 1. VSL for Requirement R1 a. Requirement 1, Part 1.4 starts off with the words “Review (and update as needed) the identification…” and the associated VSL only states the “…failed to update…” For consistency with the requirement, ReliabilityFirst recommends modifying the VSL to state “…failed to review (and updated as needed)…” This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. 2. VSLs for Requirement R2 a. The VSL for Requirement R2 uses the phrase “…failed to complete its annual review…” though the associated requirement itself states “…shall have its CIP Senior Manager or delegate approve the identifications…”. For consistency with the requirement, ReliabilityFirst recommends modifying the VSL to begin with the following: “The Responsible Entity failed to have its CIP Senior Manager or delegate approve the identifications…” This recommendation is based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement.
ReliabilityFirst votes in the affirmative for the standard but offers the following recommendations regarding the Violation Severity Levels. CIP-003-5 1. VSL for Requirement R3 a. The VSL introduces more detail then what is stated in the associated Requirement R3. Based on the FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. For consistency with the requirement, ReliabilityFirst recommends modifying the VSL as follows: “The Responsible Entity failed to identify a CIP Senior Manager by name.” 2. VSL for Requirement R6 a. For consistency with the other VSLs, ReliabilityFirst recommends modifying the beginning of the VSLs as follows: “The Responsible Entity failed to…” Also, the term “effective date” in the VSL is not referenced anywhere within Requirement R6. ReliabilityFirst recommends modifying the two VSL as follows: i. High VSL – The Responsible Entity failed to document a change to one of the delegations within 30 calendar days of the change. ii. Severe VSL - The Responsible Entity failed to document a change to the CIP Senior Manager, OR more than one of the delegations within 30 calendar days of the change.
Individual
Jianmei Chai
Consumers Energy Company
No
Yes
R1 & R1.4 - “Review” has been added to R1 (R1.4) thus requiring excessive documentation that such review was completed for any and every change in facilities, regardless of whether it is obvious that some changes will not result in a change in identification or categorization. Eliminate the word “Review” from R1.4 since the goal of R1 is simply to “Update as needed the identification…”. A review will still be necessary to identify whether an update is needed, but documentation of the review itself for any and every change in facilities would not be implied. Section A, paragraph 4.2 - The SDT needs to clarify the “Applicability” such that a registered entity, such as a Distribution Provider or Load Serving Entity, only needs to evaluate those assets specifically associated with its registration. Section A. 4.2.1 and 4.2.2 seem to imply this, but Section B, R1 does not provide any specific direction limiting a DP or LSE’s applicability. Section A, paragraph 4.2.2, third (unnumbered bullet) - The requirements for Distribution Providers to include facilities containing “A Protection System that applies to Transmission …” is a new unsubstantiated requirement for Low Impact systems, and inconsistent (omitted) with the Medium Impact requirements for all other entities in Attachment 1, Section 2. The requirement should be deleted, or if such systems are to be included, these need to be better defined and only those that reach the level of impacting one or more Interconnection IROLs should be considered.
Yes
No
Yes

Yes
Yes
Yes
R2.4 - This Requirement essentially implies that Low Impact assets need to have in place system(s) to monitor or somehow detect potential cyber security incidents in order to respond to the incidents. Although an entity may choose to handle such a response in a variety of ways, there is no need to have this detailed in a policy or procedure for low impact assets.
Group
NESCOR/NESCO
Annabelle Lee
Phrasing around the term "adversely impact" have been addressed in this new draft. However, it still may be helpful to provide some context around the meaning of "adversely impact". It is understood that in may not be practical given the variables one might need to consider.
No
No
No
R1: This requirement continues to list a series of policies that do not clearly identify what actual components of such security policies categories would be essential to help assure that an expected security state is achieved and maintained. The policy levels do not provide enough granularity to assure that there is a consistent and common approach to security policies. The standard could be modified to require entities to not only address the topics identified in the version 5 requirement, but to address them in a manner that reflects a clear relationship of policy and underlying process and/or control framework to the types of BES assets being afforded the protection of the Policy. R2: The security policies listed in this requirement should be applicable to all assets regardless of impact. Not including physical control policies and security awareness for high and medium impact assets does not match common security practices. It also does not seem to be a practical or sensical approach to dismiss assets not identified as medium or high from policy categories listed in CIP-003 R1. The standard should be modified to expand Cyber Security Policy to all levels of BES Cyber Systems, requiring the policy enumeration of protective measures afforded to operational assets. 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. (1) Organization stance on use of wireless networks (this would be optimally addressed in CIP005) (2) Monitoring and logging of ingress and egress at Electronic Access Points (this is in CIP007 R4.1.1) (3) Maintaining up-to-date anti-malware software before initiating interactive remote access (is in CIP007 R3.4) (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) (5) Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating interactive remote access (this would be optimally addressed in CIP005) (6) 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) (7) 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) (8)Availability of spare components (this was in CIP v1-v4, but doesn’t appear to be in CIP v5) (9) Break- fix processes (this would be optimally addressed in CIP010 R1.x)
Individual
Scott Bos
Muscatine Power and Water
No
Yes
For Criteria 2.11 - A BA or TOP may only provide a very small number of individual functions as described within the Functional Model based on the amount of CFRs and JROs that NERC has accepted. Not all BA's and TOP's have the same impact on the BES as a larger BA or TOP. As written,

2.11 will require every BA and TOP that is registered as such as being in the “medium” category. This one size fits all approach is not practical or logical. As stated in FERC Order 706, paragraph 253, FERC clearly speaks of being flexible “However, we are persuaded by commenter’s that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity.” We recommend that BA’s be viewed as in Attachment 1, CIP-002-4 brightline criteria 1.17.
Yes
No
Yes
Yes
Yes
Yes
[Proposed Change] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is.
Group
ACES Power Marketing
Jason Marshall
No
No
(1) We thank the drafting team for restructuring the standard to focus on identifying Facilities and Elements that meet the criteria in Attachment 1 first and then subsequently the supporting Cyber Systems. We think this is a better approach than attempting to evaluate all Cyber System first. The previous approach would have compelled an inventory of every potential Cyber System or Cyber Asset supporting the registered entity’s Facilities and Elements. This new approach does not require such an inventory. (2) Conceptually, we agree that a review should be conducted for changes to the BES Elements or Facilities for the impact on identification of Facilities and equipment per Requirement R1 Part 1.3. However, we are concerned that “change to BES Elements or Facilities” is not well defined and that a registered entity will have to inventory all changes to demonstrate if the modification caused a “change in the identification or categorization of BES Cyber Systems from a lower to higher impact category.” By “change to BES Elements or Facilities”, we assume the drafting team is primarily referring to a change in transmission system topology and addition or retirement of Facilities. Many other changes would not be included. For example, changing the ratio on a CT or replacing a relay would not qualify as a change under Part 1.4. We suggest the drafting team modify Part 1.4 to clarify that it is only those changes that affect transmission topology or are equipment additions/retirements that are included. Additionally, we suggest the drafting team expand the Application Guidelines section to fully explain its intent. (3) Requirement R2 and its associated measurement are not in alignment. The requirement compels the CIP Senior Manager or delegate to “approve the identifications required by Requirement R1 at least once each calendar year”. It does not compel the CIP Senior Manager or delegate to “review and update, where applicable, the identification and categorization” as stated in the Measurement M2. While we agree that it would be difficult to approve without conducting a review, we do not believe the intent for Requirement R2 should be for the CIP Senior Manager or delegate to perform the update as suggested in the measure, particularly considering that Part 1.4 already requires an update for changes to BES Elements and Facilities. (4) “Categorization” is not consistently used in the requirements and measures. Requirement R2 specifically uses the term “identifications” and the associated measurement uses the terms “identifications and categorization”. Is there a difference? “Categorization” is also not used in Requirement R1. For consistency, we suggest using the same term consistently throughout all the requirements and measures. (5) The purpose statement uses the term adverse impact. Because the term is very similar to the NERC defined term Adverse Reliability Impact, we suggest a footnote is needed to clarify that the drafting team is not intending to use Adverse Reliability Impact and indeed intends an impact that is less than an Adverse Reliability Impact. (6) We disagree with including LSE as an applicable entity. Per the NERC functional model, LSEs do not own or operate UFLS or UVLS relays. Page 26 of the Reliability Functional Model Technical Document makes this clear with the statement, “Unlike the Distribution Provider, the Load-Serving Entity does not have Bulk Electric System assets (“wires”) but does take title to energy.” The only role that is given to the LSE in the

Reliability Functional Model is to “participate in under-frequency load shedding systems and under-voltage load shedding systems through identification of critical customer loads that are to be excluded from load shedding systems”. They are given no role to own, install or maintain UFLS or UVLS. They simply assist in the identification of critical loads to help ensure they are not inadvertently included in the UFLS or UVLS program. Because the standard only envisions inclusion of LSEs due to UVLS and UFLS, their complete removal from the standard is warranted. (7) Use of Systems is not consistent with the NERC Glossary definition throughout many sections of the standard and application guidelines. The NERC Glossary defines System as: “A combination of generation, transmission, and distribution components.” In section 4.2.2, how can a Distribution Provider have a System when two (generation and transmission) of three required elements to meet the definition are not included? Use of “System” in the first bullet under section 4.2.2 clearly does not intend the NERC Glossary definition but rather a computer or control system. It appears that a wholesale find and replace was performed on “system” between versions which may have contributed to this problem. There are many other instances in the Application Guidelines requiring the use of System that is questionable as well. (8) Use of language “required by a NERC or Regional Reliability Standard” used throughout Applicability Section 4.2.2 (Distribution Providers) is problematic and vague. The first bullet refers to UFLS or UVLS relays that are required. The second bullet refers to Special Protection System or Remedial Action Schemes that are required. Finally, the third bullet refers to Protection Systems that are required. There are currently no enforceable standards that explicitly require a UVLS, UFLS, Protection System or Special Protection Systems. Protection Systems are such a basic necessity that it is not necessary to have requirements to install Protection Systems. At best, FAC-001-0 requirements compel Transmission Owners to have facility connection requirements for system protection but it only applies to new interconnections. The Commission only recently approved PRC-006-1. It is the only NERC standard that could be pointed to as requiring UFLS. While there are some standards such as the TPL family that could be viewed as indirectly requiring some Protection Systems, UFLS, UVLS and Special Protection Systems to meet performance requirements, no specific type is required. For instance, are overload relays required, distance relays or both? These decisions are governed by a registered entity’s protection philosophy and not any specific standard. Also, a Distribution Provider could argue that no Protection System they have installed is required by a standard but that they have agreed with their Transmission Owner to install a Protection System on the low side of a distribution transformer because it is more cost effective. It is possible this standard could incent them to resist these configurations in the future. (9) It is not clear why “Bulk Power” is capitalized in the second paragraph of the Rationale box for R1. (10) We recommend that Measurement M1 be clarified that the “list of changes to the BES” per Part 1.4 may be an acknowledgement that there were no changes. (11) What is the justification for the values used for the VSLs in Requirement R1? For example, how were 40 Facilities and 100 Cyber Systems arrived at for the Lower VSL? A justification needs to be provided? Why not use 80 Facilities and 200 Cyber Systems? (12) For Requirement R2, the language of the VSLs is not consistent with the requirement. The requirement only requires “annual” approval. It does not explicitly require a “review”. “Review” is added to the VSL which makes the VSL inconsistent with the FERC guideline that prohibits the VSL from modifying the requirement. (13) It is not clear why “associated data centers” was added to the four high impact criteria. The appropriate Cyber Systems from the “associated data centers” will already be included through identification of Cyber Systems in Part 1.2 and 1.3 of Requirement R1. Those Cyber Systems in these “associated data centers” will be identified because they support the ability of System Operators to perform the “functional obligations of the” (identified in Attachment 1 Criteria 1.1 through 1.4) Transmission Operator, Balancing Authority, Reliability Coordinator and Generator Operators. (14) While we agree with the 15 minute limit for Cyber Systems, it is not clear how its inclusion in Attachment 1 is helpful or accomplishes the intent of the drafting team. The criteria in Attachment 1 is applied to “Facilities, Systems, or equipment” through Part 1.1 of Requirement R1. It is not applied to the Cyber Systems identified in Parts 1.2 and 1.3 of the requirement. Thus, the 15 minutes appears to be inadvertently applied to the “Facilities, Systems, or equipment” when it was intended to be applied to their supporting Cyber Systems. (15) 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. This needs to be further clarified. (16) It would be helpful if the application guidelines clarify how the Reliability Coordinator,

Transmission Planner or Planning Coordinator will notify the Generator Owner, Generator Operator, Transmission Owner and Transmission Operator that their equipment meets criteria 2.3 and 2.6. (17) Criterion 2.8 needs supporting explanation in the Application Guidelines explaining how the Transmission Owner will determine that a generator it does not own or operate meets the criteria in Part 2.3. Otherwise, it is not clear how the Transmission Owner will know that its interconnection equipment to the generator should be included in this Medium Impact Rating. (18) We thank the drafting team for mitigating some of the risks surrounding inclusion of Blackstart Resources and Cranking Paths by moving them to the low impact category. However, we simply do not believe they need to be included. When a restoration plan is implemented, manual switching and operation is usually necessary. It is highly unlikely that a cyber security incident would occur because many communication paths will be down forcing entities to rely on radio communications. Continuing with their inclusion at any level will likely lead to erosion of the number of Generator Operators willing to offer this service. (19) Cranking Paths are not included in the current Bulk Electric System (BES) definition, are not included in the recently approved definition, and have been removed (as presented by the BES SDT Chair at the April 11 and 12 Standards Committee meeting) from the SAR for the phase 2 modifications to the BES definition. Since NERC legal staff recently confirmed at the April 11 and 12 Standards Committee meeting that standards are generally written for the BES, inclusion of Cranking Paths would deviate from this guidance by drawing in non-BES equipment. Cranking Paths can include sub-transmission and even distribution equipment. (20) Use of “regional load shedding program” in Attachment 1 Criterion 2.10 is problematic. There are currently no enforceable standards for regional load shedding programs. Also, the recently Commission approved PRC-006-1 places the responsibility for establishing a UFLS program on the Planning Coordinator. Planning Coordinator areas do not necessarily follow regional boundaries. (21) In the Application Guideline section regarding reliability operating services, many of the services are attributed to incorrect Functional Entities. In the Dynamic Response section, LSE is incorrectly attributed to under and over frequency relay protection and under and over voltage relay protection. Software used to calculate ACE is incorrectly attributed to the RC. RC’s don’t calculate ACE but gather ACE through ICCP from the BAs. In the Controlling Voltage section, DPs are incorrectly included. No NERC standard gives a DP responsibility for voltage. By including DPs, there is an implication that distribution equipment is intended to be included. In the Restoration BES section, off-site power for nuclear facilities is attributed to the TOP when the NUC-001 standard more broadly describes a transmission entity which includes other Functional Entities besides the TOP. In the Inter-Entity Coordination section, the TOP and GOP should not be included in scheduled interchange as they have no role in interchange scheduling. Because there could be some disagreement over which Functional Entities apply to each reliability operating service and the list of issues we identified is not exhaustive, we recommend removing all references to Functional Entities as the simplest solution. (22) There is a statement in the first paragraph of the “Applicability to Distribution Providers and Load Serving Entities” section of the Application Guidelines that states the qualifications for inclusion of the Distribution Provider are based on requirements applicable to Distribution Providers in EOP-005 and registration. This statement could actually be contradictory to Applicability section 4.2.2 which includes more applicability than just restoration per EOP-005. The statement should either be deleted or further explained. (23) We believe the statements beginning on page 26 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 identified as High Impact, this delegation should not have an impact on the TO’s 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 issue in their delegation agreement. Second, the TOP likely does not own these BES Cyber Assets at the TO but rather the TO likely owns them. 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 it is not owned by the TOP, it is not a TOP asset and, thus, not a TOP BES Cyber Asset. Third and final, this is a registration issue that should not be addressed in cyber security standards but in the registration criteria. (24) Page 27in 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 units through

Category D contingencies to its regulator, and, thus, there likely will not be any. (25) On page 28 in the Application Guidelines section, there is an explanation that Attachment 1 Criterion 2.4 excludes 500 kV collector buses. These 500 kV collector buses are part of the Generator Interconnection Facility. While we agree with the intent, this exclusion must be explicitly included in Criterion 2.4. Because the Commission has defined the requirements are the standard, the requirement needs to stand alone. Since the requirement does not reference the Application Guidelines but only the criteria in Attachment 1, we are concerned if Criterion 2.4 is not modified to account for this exclusion, the exclusion will not be considered by compliance and enforcement personnel. (26) The Application Guidelines on page 30 state the highest MW rating for the preceding 12 months will be used for Attachment 1 criterion 2.10 regarding load shedding systems. Rating is not the right word. Rather, the highest hourly integrated load is more correct. Instantaneous load should not be considered.
No
No
No
No
Yes
Yes
(1) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-003-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding Background Section 5: The second paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter. (3) Regarding Question 4 (CIP-003-5 R1): The Guidelines and Technical Basis section of the Standard for R1 states that, “The Responsible Entity should consider the following for each of the required topics in its cyber security policy…” Any number of dictionaries define “should” as the past tense of “shall” which is used to express obligation, duty or expectation. A synonym of “should” is “must.” None of the bullets listed under the required topics in the Guidelines and Technical Basis section for R1 are included in the actual Requirement R1. Using the word “should” in this section implies that Responsible Entities must consider each of the items listed for the required topics, hence, creating requirements within the Guidelines and Technical Basis section of the Standard. If the intent of the SDT is to make the items requirements, the items should be moved to R1. This will reduce compliance risk by leaving no doubt as to the minimum amount of information that is to be included for each topic. (4) Regarding Question 4 (CIP-003-5 R1): Part 1.5 needs to be clarified that the NERC Glossary definition of System does not apply. (5) Regarding Question 4 (CIP-003-5 R1): The application guidelines for interactive remote access regarding inclusion of language in contracts with vendors, consultants and contractors should be modified. The guidelines state that the language should require them to adhere to the responsible entity’s Interactive Remote Access controls. While we agree, in general, that contracts should reflect this language, the guidelines should be clear that this only applies to contracts executed after the enforcement date of this standard. Applying this standard to existing contracts could compel the responsible entity to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such as those with EMS vendors. (6) Regarding Question 5 (CIP-003-5 R2): Why does Requirement 2 state that it applies to BES Cyber Systems not identified as high and medium impact? Wouldn’t it be simpler to state that it applies to low impact BES Cyber Systems? (7) Regarding Question 5 (CIP-003-5 R2): 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. (8) Regarding Question 7 (CIP-003-5 R4): While the application guidelines are clear that electronic approval is acceptable, the measurement may create the impression that a workflow showing review is not sufficient to indicate CIP Senior Manager approval. Our concern is that an auditor may expect a “wet ink” signature per bullet 2 of the measurement. The measure should make clear that electronic approvals through tools such as workflows are acceptable and “wet ink” signatures are optional. (9) Regarding Question 9 (CIP-003-5 R6): Four VSLs could and should be written based on the number of days late that the

change to CIP Senior Manager or delegates was documented. (10) Regarding the Application Guidelines: The paragraph under Requirement R3 should apply to what is now Requirement R4 as a result of re-ordering the requirements from the previous draft. In the previous draft R3 requires the review and approval of the cyber security policies by the CIP Senior Manager at least once each calendar year, not to exceed 15 calendar months… This is now Requirement R4.
Group
PPL Corporation NERC Registered Affiliates
Stephen Berger
No
Yes
1.) The standard CIP-002 R1 still states that entities do not have to identify your Low Impact assets; however, in CIP-003 R2 entities still have requirements that must be applied to them. In CIP-003 R2 it also states an inventory list is not required, but PPL Affiliates question how the auditors will treat this, as well as future CAN's that may state you need to have a list for them to audit. 2.) The proposed criteria for selecting high, medium, and low impact facilities can inappropriately make Distribution Providers and Load Serving Entities subject to the standards. PPL Affiliates suggest that the standard note that the 300 MW is calculated as total potential load shed that can occur without operator involvement. Only single circuit interruptions or automated schemes that are capable of shedding more than 300 MW of load without system operator intervention should be subject to the standard. Therefore, PPL Affiliates suggest the following changes in the Distribution Provider and Load Serving Entity sections to address this concern: • The draft standard states the DP and LSE may be considered medium impact facilities if: Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES: o A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more. As used in this requirement, the definition of common control system should distinguish between automated load shedding schemes that may result in a load-shed level of 300 megawatts in the aggregate across multiple facilities and both operator-initiated load shedding and single breaker/feeder control/protection systems. o A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard o A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard Load Serving Entity: o 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. The LSE should be removed from the applicability (remove entire Applicability section 4.1.6 and 4.2.1) of CIP Version 5. 4.) PPL Affiliates are concerned with the VSLs • The VSLs for R1 apply varying levels of penalties for "incorrectly" classifying facilities as high and medium impact facilities. In fact, if 15% of the facilities are not identified or incorrectly categorized a severe violation level would exist and subject the responsible entity to potentially large fines. • PPL Affiliates are concerned that the standard does not identify who will do a review of the classification of facilities. Leaving the review to the auditor can result in severe penalties if they find a categorization is inappropriate. • In many if not most instances there is no cookie cutter approach to system design and operation which drives the categorization of facilities. Each responsible entity will make their classification of each facility based on system designs and operational considerations that are unique to their system and may likely differ among entities. The standard should not allow the auditors to dismiss the knowledge used to make the unique categorization levels. • PPL Affiliates believe the standard should be modified to remove the ability of the auditor to disregard categorizations made by responsible entities based on their first hand experience. If a baseline categorization is made (see above) the auditor should not be able to question a categorization but can review it for completeness. If a categorization change is ultimately made the auditor should not claim a violation of the requirement has occurred and no penalty should be assessed. • PPL Affiliates suggest removing from the VSL penalties for R1 for "incorrectly" classifying facilities. There is flexibility in the definition of High and Medium Impact facilities and the standards appear to recognize that system design and operation are in many instances not identical across the industry. A medium impact facility in one utility may be a high in another due to design and operation. Giving the audit

team the ability to change classification and then assess potentially a severe violation determination along with penalties is not appropriate for at least the short run where responsible entities are gaining experience in how the audit teams are viewing classifications. Different audit teams may view each classification differently. At least in the short run an “incorrect” classification of a facility should not be viewed as a violation. That language should be removed from the VSL table.
Yes
No
Yes
Yes
Yes
Yes
1.) PPL Affiliates require clarification on the R2 expectations of “documented cyber security policies” for the specific requirements of low impact assets which are not defined in the details in CIP-005, CIP-006, and CIP-007 whereas high and medium impact assets are. CIP-003 R2 should therefore explicitly clarify these expectations of low impact assets. 2.) PPL Affiliates have concerns with R2, and support the associated EEI comments noted below: EEI comments: EEI members are concerned regarding the potential need to discretely demonstrate compliance at the equipment level. The requirements are framed in a way that may lead an auditor to require discrete identification to adequately demonstrate compliance. This provides conflicting messages that could impede approval of protection controls for BES Cyber Systems used within High and Medium Impact facilities. Propose changing "For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics" to "For BES Cyber Systems used in facilities not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics:
Individual
Marcus Freeman
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency
No
Yes
The revised applicability criteria (located at Sections 4.2.1 and 4.2.2) for Load-Serving Entities (“LSEs”) and Distribution Providers (“DPs”) that may have under-frequency load shedding (“UFLS”) devices installed within their electric systems remain confusing and should be further clarified. Many LSEs and DPs participate in regional UFLS programs but contribute less than 300 MW of load shed (indeed, many such entities’ individual peak loads may be substantially less than 300 MW). Participation by these entities in regional UFLS programs may arise because a regional program directly requires LSEs and/or DPs to have UFLS programs. It may also arise because a contractual agreement between the LSE/DP and its Transmission Operator or Transmission Service Provider requires the LSE/DP to install UFLS relays and participate in the Transmission Operator’s or Transmission Service Provider’s UFLS program, which itself may have been developed to comply with a regional UFLS obligation and shed more than 300 MW of load, including a portion of the LSE/DP load. As currently proposed, the applicability criteria for LSEs and DPs suggests that their participation in any required regional program that sheds 300 MW or more subjects them to CIP-002-5, irrespective of whether equipment actually owned or operated by the LSE or DP itself is capable of shedding at least 300 MW. NCEMPA understands that the Standards Drafting Team has attempted to clarify this issue by adding the phrase “under a common control system” to the applicability language. However, “common control system” has not been defined or explained, and this terminology may have different meanings to different protection system engineers. If the applicability language related to UFLS equipment is not clarified, LSEs and DPs may not know what their compliance obligations are with respect to CIP-002-5, and Regional Entities may interpret and apply the applicability language differently in different regions or mistakenly apply the criteria to LSEs and DPs that the Drafting Team intends to be excluded from CIP-002-5. To remedy the ambiguity in the currently-drafted applicability criteria, NCEMPA and NCMPA1 suggests that the following formulation of the DP/LSE applicability language be adopted: Ownership or operation of equipment or devices that are (i) configured to perform automatic under-frequency or under-voltage Load shedding, without human operator initiation, (ii) capable of shedding a total of 300 MW or more of the LSE/DP’s load, and (iii) required

for compliance with a NERC or Regional Reliability Standard governing under-frequency or under-voltage Load shedding. Conforming changes to reflect the above-referenced modification to Section 4 should also be reflected in Attachment 1, Part 2.10. Additionally, examples of different load shed configurations would aid the industry in understanding the intended scope of the applicability criteria. The examples should make clear that only LSEs/DPs that are individually capable of shedding at least 300 MW of load are considered within the scope of CIP-002-5. Additionally, a second criterion applicable to DPs is unclear. Specifically, Section 4.2.2 provides that DPs with a "Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard" are subject to CIP-002-5. The specific Protection Systems that this criterion is intended to describe should be further explained. NCEMPA is aware that some industry participants may misinterpret this criterion to pertain to any transmission Protection Systems that are tested and maintained under PRC-005. However, PRC-005 does not require the installation of Protection Systems; rather, it requires Protection System testing and maintenance. Absent further explanation regarding the nature of this criterion, it should be eliminated. Finally, to the extent that the Drafting Team intends to retain the current applicability language and, consequently, for LSEs and DPs that own/operate relays that shed less than 300 MW of load to be subject to CIP-002-5, NCEMPA and NCMPA1 urges the Standards Drafting Team to revise Attachment 1 to classify Cyber Systems associated with UFLS/UVLS equipment as Low Impact, rather than Medium Impact. There is no obvious justification for small LSEs/DPs to be subject to the full panoply of requirements that apply to owners of Medium Impact assets.
Individual
Frank Dessuit
NIPSCO
No
No
1.1, 1.2 and 1.3 – The term "Used for" should be replaced with "that entity deemed essential". 1.4- This standard should state "new or changes to a modified criteria rating needs to be compliant within 60 days of going into production". M1- The measure and the requirement should read: "a list of changes to the BES (with a date for each change) that cause a change in the impact rating of the Facilities, Systems, or equipment from a lower to a higher impact category." R2- Rationales should not be formally incorporated into the standard. Information in the rationale should be addressed as part of a non-binding informational document, e.g., a FAQ process. The rationale conflicts with the requirement time frames. (1 year vs 15 months).
Yes
Yes
Yes
Yes
Yes
Yes
Group
BC Hydro
Patricia Robertson
No
No
1) The new "bright line" method complicates the process the Registered Entities will need to go through to identify those cyber assets that are critical to the reliability of the BES. It limits the Registered Entity's ability to apply rational judgement in identifying CCAs that was available in versions 1 to 3. 2) The high and medium impact asset descriptions, in general, need to be rewritten. Upon initial review, BC Hydro found it difficult to understand what assets would need to be identified based on the new criteria. It is recommended that one or two examples be provided for each as to what types of assets the criteria is referring or provision of a guideline document. 3) The term "adversely impact" is not clearly defined. 4) Suggest changing wording "would, within 15 minutes,

adversely impact" to "could adversely impact." There is a significant difference between would and could. At what point does the clock start ticking to determine the 15 minute timeframe? 5) The "15 minute" time limit seems arbitrary; how was this number arrived at; why not 20 minutes? 6) The term "interconnection" needs to be more clearly defined. 7) Prescribing calendar year not to exceed 15 months overrides an entities own definition of annual per NERC's CAN-008 and could lead to violations
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Heather Laws
Portland General Electric
No
Yes
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. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes
Yes
Yes
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. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
Yes
Yes
Yes
No
No
No
No
Although IESO agrees with the requirements outlined in CIP-003, R3, we believe the definition of the NERC Senior Manager needs to include the ongoing compliance related responsibilities of the role, specifically to identify the operation and maintenance of the standard requirements. IESO believes

that the CIP-003-5, R6, M6 needs to be clarified and reworded.
Individual
Cristina Papuc
TransAlta Centralia Generation LLC
No
TransAlta recommends removing the criterion 2.11 (2), “control an aggregate highest rated net Real Power capacity of the preceding 12 calendar months equal to or exceeding 300MW or more of BES generation”, because TransAlta does not believe that there are technical basis provided consistently to categorize the generation Control Center as the medium impact. The details are, 1. TransAlta believes “The value of 300 MW is the same value used for UFLS and UVLS” as mentioned in the guidelines and technical basis section of CIP-002-5 (the first paragraph in Page 28), is inappropriate justification for medium impact. 300 MW number in the UFLS and UVLS is irrelevant to the impact level of generation Control Center. As TransAlta commented on the draft 1, “The UVLS and UFSL are triggered by the voltage and frequency, not directly by the generation loss.” In the draft 1 comment records, Robert Mathew from Pacific Gas and Electric Company also raised the same issue about using 300MW, i.e. “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.” 2. In the SDT response to the TransAlta requests for additional clarify, it says “The intent of this criterion is to include all generation Control Centers.” However, there is no technical justification of this intent in any document. Without technical justification, TransAlta does not agree to this intent. 3. The intent to categorize all generation Control Centers as medium impact has the technical deficiency. The loss of a single 500MW unit generation (not meeting any criteria 2.3 and 2.6) controlled by a control room would have a low impact according to the criteria 3 while a loss of Control Center controlling 300MW generation(not meeting criteria 2.3 and 2.6) would have a medium impact according to the criterion 1.12. This does not make sense in regards to the loss of generation capacity. 4. In the SDT response to the TransAlta requests for additional clarity, the second sentence is confusing when talking about excluding some Control Centers. On one side, it recognizes these facilities as generation Control Centers “because they control geographically dispersed locations”. On the other side, these facilities “function more as a single generation facility control room”. So are these facilities really generation Control Centers or control rooms? This response creates more confusion between the Control Center and control room. 5. There is no consistency in justification of generation Control Centers as medium impact. In the SDT response to the TransAlta requests for addition clarity, the 300MW is picked for the purpose to excluding certain generation Control Centers, “…300MW specifically in consideration of those generation Control Centers….” However, in the guidelines and technical basis section, the 300 MW is picked, “the same value used for UFLS and UVLS.” So the reasons to pick 300MW are not consistent.
Group
IRC Standards Review Committee
Christine Hasha
No
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding CIP-002-5, question 3. The IRC respectfully provides these additional comments. Regarding Requirement 1, the IRC requests that specific language be added describing the standards applicable to third party functions, and information within those standards, that are relevant to criticality determinations under CIP-002-4 Attachment 1 criteria 2.3 and 2.6. This will facilitate uniform application of criticality determination under Attachment 1 criteria 2.3 and 2.6, which, in turn, will support efficient and effective application of CIP-002-5.
Yes
Yes
Yes
Yes
Yes
Yes

The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding CIP-002-5, question 10. The IRC respectfully provides these additional comments. Regarding CIP-003-5 R3 (question 6), the IRC requests revising the measure to, “Evidence may include, but is not limited to, a dated approval by the CIP Senior Manager, listing named personnel, by name or title, who are delegated the authority to approve or authorize specifically identified items.” Approved is the term used in the requirement language. Regarding CIP-003-4 R4 (question 7), the IRC requests revising item 2 in the measure to, “A dated approval by the CIP Senior Manager for each cyber security policy that indicates annual approval.” Approval is the term used in the requirement language.
Group
Texas RE NERC Standards Review Subcommittee
Brenda Hampton
No
No
(1) The Background section or Application Guidelines of CIP-002-5 should provide more discussion and detailed examples of the BES Cyber System concept. Multiple examples should be provided to address typical Responsible Entity configurations. This broader understanding will aid personnel in compliance decisions and, later, in the appropriate development of Reliability Standard Audit Worksheets (RSAWs). (2) We agree with the SDT that there is no need to have a discrete list of Low Impact Cyber Systems/Assets as stated in R1.3. However, the wording in Attachment 1 is in conflict with R1.3. To resolve the contradiction and provide clarity, revise R1 and Attachment 1 as follows. In Requirement R1.2, add qualifier “For each High Impact Facility, System or equipment, identify…” In Requirement R1.3, add qualifier “For each High or Medium Impact Facility, System or equipment, identify…” On Attachment 1, under High Impact Rating (H), change “Each BES Cyber System used by and located at” to “The following Facilities, Systems or equipment”. Under Medium Impact Rating (M), change “Each BES Cyber System, not included in Section 1, above, associated with the following” to read “Facilities, Systems or equipment, not included in Section 1, above, associated with the following”. Under Low Impact Rating (L), remove “Each BES Cyber System associated with:”. Once a facility is identified as Low Impact, there should be no need to further identify individual Cyber Systems in that facility as High, Medium, or Low. (3) Revise Attachment 1, Item 2.8 “Transmission Facilities providing the generator interconnection…” to read “generation interconnection facility…” This term was developed under Project 2010-07. This is an important distinction as Transmission Facilities are subject to all TO/TOP requirements, while a generation interconnection facility is subject only to a selected subset. (4) Attachment 1, Item 2.11 (2) should be removed. Item 2.11 (2) classifies “Control centers and associated data centers not included in the High Impact Rating (H), above, that…control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” Inclusion of these control centers has been justified by the drafting team as analogous to the automatic load-shedding item (2.10), although in the source direction, not the sink. However, the difference is extensive. A compromised automated load shedding system will lead to an immediate loss in service. A generator control center can deploy other compensating measures before the impact is noticed. In addition, the loss in 300 MW of load has deep historical ties to reliability – a connection captured in DOE and NERC Disturbance reporting. Conversely, the loss of generation is historically tied to Interconnection reserve capability – which aligns with the 1500 MW number used in Item 2.1. We have not seen data that indicates that a control center controlling 300 MW of aggregated generation poses an additional reliability risk that would justify the cost of implementing over 100 CIP requirements. Furthermore, we have not seen a FERC directive calling for it. We recommend that the sentence be stricken to allow the industry to focus on the truly critical systems. Further, we agree with the concepts discussed in TransAlta Centralia Generation’s request for clarification. Justification and supporting information should be provided when identifying specific thresholds of MW capability or other similar criteria in defining BES Assets.
Yes
No
No
Yes
No

No
(1) Consider changing the word “topics” in R. 1 and other places to “elements” since the 10 identified areas are elements of the Cyber Security Program. (2) In Requirement R1, 1.10, consider changing the word “declaring” to “identifying”. (3) In Requirement R2, replace “BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics:” with “Each Responsible Entity shall implement one or more documented cyber security policies to address the following topics for BES Cyber Systems of low impact:” (4) To reduce ambiguity in determining reasonable evidence for meeting requirement R2, consider adding additional detail to M2 such as: M2.1 Evidence may include, but is not limited to, policies that address periodic high-level training, less formal reviews with appropriate personnel, or the posting of cyber security policies on the corporate Intranet site/company bulletin boards. M2.2 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict physical access. M2.3 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict electronic access. M2.4 Evidence may include, but is not limited to, policies that address identification and reporting of BES Cyber Security Incidents. (5) Consider combining the R6 content applicable to naming the CIP Senior Manager with R3. This will eliminate ‘double jeopardy’ concerns where failure to adequately document changes will now result in the violation of only a single requirement. Suggested wording: “Each Responsible Entity shall identify a CIP Senior Manager by name. Any changes to the CIP Senior Manager shall be documented within thirty calendar days of a change.” (6) Consider combining the R6 content associated with delegations with R5 to eliminate ‘double jeopardy’ concerns. Suggested wording: “Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager. Each Responsible Entity shall document any changes to delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator.”
Individual
Steven Powell
Trans Bay Cable
No
Yes
Criteria 2.11 categorize all TOP Control Centers as Medium impact on BES. This criteria is too inclusive and includes control centers of low impact TOP’s. This result in the applicability of security controls that are not at all aligned with the risk that these control centers (dispatch control centers) could have on the BES. To avoid this situation 2.11 should align with 2.5 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 3000 (see 2.7) the control centers should not be designated as Medium impact. Therefore 2.11 would read 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 2.5.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
G. Copeland
Pattern
Yes
We are concerned with Attachment 1, 2.11 - Control Centers and associated data centers controling and monitoring generation resources at an aggregate rated net RealPower capability of 300MW or

more of BES generation appears not sufficiently justified. If a control center were to monitore and control 10x (aggregate) 30 MW generation facilities that are interconnected to the BES system (although it is currently not clear if this meets the term "BES generation") it is not clear how such a Control Center becomes critical enough to the BES to be rated at medium impact particularly if all of these facilities are intermittend resources and neither facility would even be considered critical enough on its own that it had to be on the NERC Compliance Registry. And even if the (IPP) facilities are large enough in scale to meet NERC registration criteria they are usually still not critical enough for the individual region/are to have a significant impact since the individul facility cannot guarantee generation/capacity due to the nature of the fuel source. None of these IPP facilities are considered reliability facilities (Reliability Must Run, Resource Adequacy facilities, Black Start etc) and since Black Start Resources are rated as Low Impact it becomes even more difficult to follow the argument that an aggregate 300 MW of generation at a Control Center is a sound technical justifiction as criteria for Medium Impact Rating. It is also difficult to understand the justification how a Control Center of aggregate 300 MW IPP resources can compare to the impact a TOP/BA Control Center has on the BES. Finally, the loss of a single 500MW unit generation (not meeting any criteria 2.3 and 2.6) controlled by a control room would have a low impact according to the criteria 3 while a loss of Control Center controlling 300 MW generation(not meeting criteria 2.3 and 2.6) would have a medium impact according to the criterion 1.12. This does not make sense in regards to the loss of generation capacity. Since the term Control Center is not in the current NERC Glossary I would appreciate to maintain in the draft standard a reference/ clarification on generation Control Center, control room and "controling" generation to help clarify which facilities would fall under the category defined by 2.11.

No

Yes

Individual

Chris de Graffenried

Consolidated Edison Co. of NY, Inc.

1. Section 4.2 of CIP-002-5 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. 2. Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1: FROM: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; 3. Requirement 1.3 of CIP-002-5 should be revised to use the same language as Attachment 1: FROM: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

Individual

Edward Bedder

Orange and Rockland Utlities Inc.

1.Section 4.2 of CIP-002-5 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. 2.Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1: FROM: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; 3.Requirement 1.3 of CIP-002-5 should be revised to use the same language as

Attachment 1: FROM: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; TO: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;
Individual
Michael Jones
National Grid
No
Yes
We recommend the following wording for R 1.2 (we moved “high impact to be in front of Facilities): 1.2. Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the high impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We recommend the following wording for R1.3 (we moved “medium impact” to be in front of Facilities): 1.3 Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the medium impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We also recommend that the CIP Process Flow on the last page be updated to show clearly that the identification of BES Cyber Assets should occur first, followed by identification of BES CYBER Systems.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
No
Yes
(1) Section 4.2.2, last bullet: All single points of failure in the cranking path should be protected from the black start resource (or injection point if the entity relies on cranking power from an adjoining entity) to the generation unit(s) to be started. Additionally, this section needs to be clarified as necessary to ensure that a Responsible Entity that elects to receive electric power from a neighboring entity as opposed to providing its own black start resource views the cranking path generation source as the point of injection (typically a tie substation) into the Responsible Entity’s transmission or distribution system. (2) Section 4.2.4.2 attempts to define exemptions for communication links, but fails to include the exclusion of end points to those circuits (see CIP-005/R1.3). (3) Throughout the standards, the phrasing “would affect” or similar is used. The requirements should be prospective and use the phrase “could” instead of “would.” The impact of a failure or compromise cannot always be predicted with certainty and entities could use the phrasing to argue that certain BES Cyber Systems do not meet the bright line criteria based on that lack of certainty. Use of “could” is consistent with the application guideline for R1 where the entity is expected to assume the vulnerability exists and that the probability is 100%. The standard needs to be precise in that regard; entities are not held to the expectations found in guidance. (4) The last paragraph on Page 7 leaves it up to the entity to determine the level of granularity when identifying the BS Cyber Systems and instructs the entity to take into consideration the operational environment and scope of management. First of all, what is reasonable? Left to the discretion of the entity, grouping of assets may be unreasonable, such as declaring the entire sets of unrelated assets in a data center as a BES Cyber System. Second, how is the operational environment and scope of management evaluated? Is this an auditable expectation?

(5) The SDT continues to insist there is no need to identify the low impact BES Cyber Systems and their associated Cyber Assets (e.g., R1.3). This causes an auditability issue. The auditor will want to understand all of the BES Cyber Systems and associated Cyber Assets evaluated by the entity in order to verify all high and medium impact BES Cyber Systems have been properly identified and classified. This can only be accomplished by having the entity produce a comprehensive list. (6) The example of “Electronic Access Control or Monitoring Systems” references Certificate Authorities. As strictly stated, this could be problematic if the entity relies upon a commercial Certificate Authority. In the same definition, it would be helpful to refer to the SIEM, SEIM, and SIM in addition to the SEM. Finally, in the same definition, it would be helpful to refer to “intrusion protection systems” as well. (7) The definition of Protected Cyber Assets should include local attached storage, network attached storage (NAS) and storage area networks (SAN). (8) In R1, reference is made to a time horizon. Please footnote the reference. (9) R1.1, R1.2, and R1.3 should also require the identified items to be documented. R1.4 allows identification information to be updated within 60 days of placing the element or facility into service. If this is a planned change, the identification should be completed as part of the planning and preparation prior to the operational or in-service date. (10) R1.4 includes a condition where the BES element or facility change causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. You have to complete the R1.1, R1.2, and R1.3 identification in sequence, hence the condition is problematic. It would be better to require the identification process review to be performed and in a separate sentence, require the update if the condition is met. (11) M1 should require all changes to be documented to ensure nothing has been overlooked. (12) The rationale for R2 stipulates the lists from R1 are to be “reviewed.” This is inconsistent with the actual requirement to “approve.” (13) M2 references “review and update.” This is not in the requirement. (14) In the VSL for R1, the failure to identify even one “High” impacting BES Cyber System should be a “Severe” violation due to the potential risk. (15) The reference to “review” in the R2 VSL is not a requirement found in the language of R2. (16) Criteria 2.1 of Attachment 1 refers to an impact in 15 minutes. This is going to be very difficult for the entity to demonstrate during an audit. (17) Instead of referring to a 15 minute interval in Criteria 2.2 of Attachment 1, simply refer to BES Cyber Systems that operate the reactive resource(s). (18) Is the transmission facility referenced in Criteria 2.8 of Attachment 1 a substation (or switchyard) or something more granular? (19) Criteria 2.9 uses the phrase “would” instead of “could.” (20) In the guidance discussing Restoration of the BES, should “Coordination” be the responsibility of GOPs, TOPs, and RCs? (21) The first bullet in the guidance for the overall application of Attachment 1 allows the entity to determine the grouping of facilities. Entities should be required to group all facilities in a substation into one set for transmission. (22) The threshold in criteria 2.1 of Attachment 1 should regionalize the threshold to more approximately reflect regional operational conditions. (23) The criteria for categorizing a control center does not take into consideration the interconnectivity of the BES Cyber Systems as required in the FERC order approving Version 4 of the CIP standards. Any BA, TOP, or GOP control center that uses ICCP to exchange data with other entities should be categorized as High. The concept of mutual distrust does not work because ICCP communication is over a trusted path and there are sufficient vulnerabilities in the ICCP foundational code to be a high risk. (24) How was 1000 MVARs “deemed” to be reasonable? (25) for restoration facility criteria, consider categorizing black start resources required for starting adjoining entities “medium” while leaving self-starting entity’s black start resources as low. (26) Facilities in the cranking path for system restoration that are single points of failure should be categorized as Medium impact. (27) The criteria needs to address the situation where the Responsible Entity elects to receive cranking power from a neighboring utility as opposed to self-providing with its own black start generation resource. In that instance, the entity’s cranking path must be understood to begin at the point of injection, typically a tie substation, and not at a defined generation resource.
Yes
No
No
No
No
Yes
(1) R1 needs to be clarified that the cyber security policies need to support the requirements by meeting or exceeding the expectations of the requirement and not be contrary to the requirement elements. (2) R3 needs to be clarified as to whether the Senior Manager can be self-appointed. (3)

The appointment of the Senior Manager still needs to include the title or position of the individual to prevent ambiguity when there are multiple personnel with the same name. (4) An organization chart as evidence (referenced in M3) is not sufficient to document the appointment of the Senior Manager. In the absence of a specific “CIP Senior Manager” or similar title, there is no way to determine who the Senior Manager is on the organization chart. Additionally, as organization charts tend to regularly change, a dated organization chart does not adequately identify the date of appointment. This example of evidence should be removed from this requirement. (5) The Responsible Entities need to fully understand that the suggested evidence in M4 requires a dated signature, either physical (“wet ink”) or electronic, demonstrating the review and approval. An entry in the revision history typically precedes any approval action and therefore does not by itself adequately demonstrate approval or attest to such action. (6) R5 needs to be modified to require the delegation document to include the specific scope of the delegation. Doing so would then comport with the example evidence found in M5, which references “specifically identified items.” (7) The VSL for R4 needs to include a condition where not all of the security policies have been reviewed, irrespective of the approval of any of those reviewed. The Severe VSL language includes the condition where Responsibility has not reviewed the policies *AND* the Senior Manager had not approved all of the policies within the required time period. Perhaps the “and” should be changed to “or”. (8) The guidelines for R1 should include instructions that a high-level policy document should include referential links to the additional documentation for continuity and completeness. (9) It is not appropriate for the guidelines to instruct the independent auditor on how to audit the requirement. R2 requires the implementation of documented policies. Auditor discretion is necessary to determine how to audit compliance with the requirement to document and implement cyber security policies that meet the minimum expectations defined in the requirement. (10) The guideline for R5 references “delegation of the delegation authority.” This does not comport with the requirement itself, which requires all delegations to be approved by the Senior Manager. (11) The guidance regarding delegations of authority should include comments on documented revocation of delegated authorities and the need to specify the scope of the delegated authority.
Individual
Mario Lajoie
Hydro-Quebec TransEnergie
No
Yes
(1) No need for a bullet in 1.3 as it is a single element, not a list. HQT proposes that the text be included in the above section (2) Table of Compliance Elements - Moderate and High VSL - Entities with fewer than 40 facilities identified in R1 : 4 or 6 facilities not identified fall outside of the given intervals (“more than two, but fewer than four” and “more than four, but fewer than six” should be changed to “more than two but less than or equal to four” and “more than four, but less than or equal to six) (3) Table of Compliance Elements : Language added for RE with fewer or greater than 40 facilities in R1 is inconsistent with existing language. Recommend change to existing language to account for the shift from identifying BES Cyber Sytems to identifying Facilities (4) Attachment 1 parts 1.2 and 1.4 : Request clarification to whether or not the 1500 MW refers to criterion 2.1. If so, it should point directly to that criterion. (5) Attachment 1 parts 2.1 and 2.2 : The 15 minutes criterion is arbitrary, hardly measurable and adds confusion to whether or not a Cyber Asset should be considered. HQT recommends to remove the last sentence regarding the 15 minutes OR provide entities with a clear and repeatable methodology as a guideline to identify such systems. HQT considers that interpretation of those criteria can greatly differ from different entities which is not faithful to the “bright-line” concept. A bright-line criterion should not leave room for interpretation (6) Attachment 1 part 2.2 : It should specify “in absolute value” or “maximum variation of reactive power” to account for facilities that have for instance synchronous condenser (e.g. how a -250 to +300 MVAR nameplate value should be considered). (7) Attachment 1 part 2.3 : Considering there is no NERC standard requiring the PC or TP to inform GO and GOP of such facilities, how this criterion can be applied. HQT considers that this is not a “bright-line” criterion and recommends to remove it OR provide entities with a clearly defined and consistent way of identifying such facilities.(8) Attachment 1 part 2.10 : Considering multiple ways to apply or interpret this criterion, HQT recommends to specify the way to measure the load shedding capability by proposing this wording "Each System or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, with an aggregate lowest rated net Real Power capability

of the preceding 12 calendar months equal to or exceeding 300 MW or more, implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program.". Rationale: A facility should be considered medium impact BES Asset when its minimum shedding load capability is kept all year long over 300 MW, meaning we can always rely on at least 300 MW as the last layer of defense to avoid collapsing of the grid.
Yes
Yes
Yes
Yes
Yes
Yes
We agree with the comments provided by the NPCC TFIST
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
No
Yes
Yes
Yes
Yes
R2: to match the rest of the proposed language, the VRF for R2 should be “Lower” to match the standard language (p. 9) and in the text it should also be changed to “Lower” instead of “Medium” (p. 14).
Group
NRG Companies
Alan Johnson
Yes
No
Revise Attachment 1, Item 2.8 “Transmission Facilities providing the generator interconnection…” to read “generation interconnection facility...” This term was developed under Project 2010-07. This is an important distinction as Transmission Facilities are subject to all TO/TOP requirements, while a generation interconnection facility is subject only to a selected subset. Attachment 1, Item 2.11 (2) should be removed. Item 2.11 (2) classifies “Control centers and associated data centers not included in the High Impact Rating (H), above, that…control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” We have not seen data that indicates that a control center controlling 300 MW of aggregated generation on more than one physical footprint (such as control of small remote sites which would be low impact) poses an additional reliability risk that would justify the cost of implementing over 100 CIP requirements. . Furthermore, we have not seen a FERC directive calling for it. We recommend that the sentence be stricken to allow the industry to focus on the truly critical systems. Finally, for generation control centers the BES Cyber systems should be considered only if they are shared at the central location, and not inclusive of all systems resident within the control center. This should be empirically clear.
Yes
No
Yes
Yes
No

No
In Requirement R2, replace “BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics:” with “Each Responsible Entity shall implement one or more documented cyber security policies to address the following topics for BES Cyber Systems of low impact:” Requirement 2 does not provide any specifics for providing guidance for compliance and/or audit. To reduce ambiguity in determining reasonable evidence for meeting requirement R2, consider adding additional detail to M2 such as: M2.1 Evidence may include, but is not limited to, policies that address periodic high-level training, less formal reviews with appropriate personnel, or the posting of cyber security policies on the corporate Intranet site/company bulletin boards. M2.2 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict physical access such as card key, special locks, security personnel, or other authentication methods. M2.3 Evidence may include, but is not limited to, policies that address operational or procedural controls which restrict electronic access from public or other less trusted network zones through proxy servers, DMZ, password protections, or other authentication methods. M2.4 Evidence may include, but is not limited to, policies that address identification of BES Cyber Security Incidents and the reporting of cyber intrusions to ES-ISAC.
Individual
Eric Scott
City of Palo Alto
Section 4.2.2, Bullet 3 states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” Palo Alto is a small entity which has no critical cyber assets. Palo Alto is concerned that this language may be intrepreted such that Palo Alto could be determined to have critical cyber assets. Palo Alto requests that the SDT clarify which “Protection Systems” it is referring to in this bullet. Palo Alto requests that for each "Protection System" the SDT identify the NERC or Regional Reliabity Standard that establishes the requirement for each "Protection System" and that this information be included in the guidance.
Yes
Individual
Ed Nagy
LCEC
No
No
Comments: 1) Attachment 1 criterion 2.11 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 2.11 could be aligned with criterion 2.5 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: 2.11. Control Centers not included in High Impact Rating (H), above, that (1) perform the functional obligations of the Balancing Authority (2) perform the functional obligations of Transmission Operator with a “total weighted aggregate value” that exceeds 3,000 for ALL Transmission Facilities controlled by the Control Center per criterion 2.5; or (3) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation. The point that must be stressed here is that if ALL of the Transmission Facilities being operated by the Transmission Operator COMBINED DO NOT justify a BES impact rating of Medium, how can the Control Centers be considered Medium impact? Comment: 2) Attachment 1 criterion 2.10 should include the word AND after the first portion of the criterion that details the capabilities of the system to qualify for inclusion under this criterion. (e.g. automatic load shedding, common control system, without human operator initiation). Without making this change, there is a chance that this criterion will be misinterpreted to include a collection of discreet relays who’s sum exceeds 300MW which is not the intent and has been verified by NERC. For example: 2.10 Each System or group of

Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more AND implements Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program. Comments: In CIP-002-5 Attachment 1 section 2.11 the term “associated data centers” has been introduced without it being clearly defined. One might assume that this is referring to the data centers that contain BES Cyber Systems and Assets only but this is not clear. Data centers that are owned by the entity but do not contain BES Cyber Systems or Assets could be interpreted by an auditor as being “associated” due to network connectivity that exists outside of the ESP. Recommend removing the term “associated data centers” from the standard as it does not add any additional value or context that is not already addressed by other ESP & PSP requirements.
Yes
No
Yes
Yes
Yes
Yes
Comments: Requirement 1.10 was added to address CIP Exceptional Circumstances. This definition is defined but is too broad. It includes safety related issues and response by emergency services for example. It is difficult to determine the appropriate scope of what should be included in the security policies as a result of this.
Individual
Robert Mathews
Pacific Gas and Electric Company
No
Yes
Attachment 1 Criteria 2.11 is not acceptable because there is no technical basis for the 300 MW threshold for inclusion of Control Centers and associated data centers as Medium under 2.11 “2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” Rationale: The 300 MW of generation threshold in 2.11 is apparently derived from the 300 MW in 2.10 relating to UFLS/UVLS. 300 MW of generation should not be equated to 300 MW of UFLS/UVLS. While the loss of load may have similar impacts as loss of generation in a general sense, equating the “last ditch efforts to save the BES” provided by UVLS/UFLS is not in the same as any loss of load or any loss of generation. Automatic Generation Control (AGC), spinning reserve, etc. are mechanisms to make up for lost generation, which are not “last ditch”. Suggest Standard Revisions: 2.11. Control Centers and associated data centers not included in High Impact Rating (H), above, that perform the functional obligations of Balancing Authority or Transmission Operator.
Yes
Yes
Yes
Yes
Yes
Yes
Guidelines and Technical Basis for R1.4 Bullet 3 on page 18 still includes egress. Suggest striking egress to conform with changes to CIP-006.
Group
Duke Energy
Greg Rowland
No
Yes
(1) Section A Introduction. 1. Title currently says, “Cyber Security – BES Cyber System Categorization”. This is not the same as the heading in the document which says, “Cyber Security – BES Cyber Asset and BES Cyber System Categorization”. Duke suggests changing the title in A1 to

read the same as the header. (2) Section A Introduction. 4.2.4.3 currently says, “In nuclear plants, the Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.”. This incorrectly assumes that all regulated devices by the NRC are inside the boundaries of a nuclear plant. Duke suggests rewording to the following, “The Systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.”. This will provide the exemption for any devices regulated by the NRC, regardless of their physical location. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (3) Section A Introduction. Background section “Reliable Operation of the BES”. The sentence “In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functional entities in the NERC Functional Model” is incorrectly stated. The NERC Functional Model identifies functions and not functional entities. Duke suggests rewording this sentence to read, “In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to the reliability tasks identified for functions in the NERC Functional Model.”. (4) Requirement R1 - It would be helpful to clarify that BES Cyber Systems inherit their impact rating from the facility by describing them as “BES Cyber Systems of a high impact facility”, for example, rather than “high impact BES Cyber Systems”. This will avoid the confusion of whether a Cyber System requires its own impact rating independent of the facility. By Enhancing the CIP process flow on page 33 to indicate that the assets inherit the impact of the facility, there may be greater industry approval. As it currently exists, the process flow has as its first box the identification of BES Cyber Assets and BES Cyber systems. This first box should capture the identification of facilities that satisfy the impact criterion. Duke supports EEI’s suggestions that this process flow be enhanced, and possibly moved to the requirements section to provide a prescriptive methodology to ensure this “facilities first” approach provides clear directives to the industry. (5) Requirement R1 - Rather than the current approach to identify “Facilities, Systems, and equipment,” modify this to identify High Impact Sites, Medium Impact Sites with all BES Sites not identified as High Impact or Medium Impact being identified as Low Impact. For Low Impact, maintaining inventories at the site level would avoid the concern that discrete equipment identification is required. Duke supports EEI’s comments on this. (6) Requirement R1.3 – Duke suggests that the bulleted item that appears in R1.3 should be removed. With the proposal in (5) stated above, if the Low Impact Sites have already been identified, there is no need to have a requirement NOT to list the BES Cyber Systems at those sites. The requirement should only be that Low Impact Sites have been identified, therefore discrete identification of the Low Impact BES Systems would never need to be addressed. (7) Requirement R1.4 – Duke suggests deleting this requirement. The current wording of R1.4 would require the full list of facilities and systems to be reviewed every time a change is made to BES Elements or Facilities. In a larger company, this is a continuous process and would require constant review of the lists. Duke feels that the Implementation Plan adequately covers the need to monitor for entities to monitor for changes to their BES Elements or Facilities such that compliance can be met for any newly categorized BES Cyber System. (8) Measure M1. Duke suggests that the standard verbiage in front of every measure be changed from “Acceptable evidence includes, but is not limited to” to “Non-prescriptive examples are”. Duke believes this more adequately demonstrates that the measures are examples, and should not be the minimum which would be needed to demonstrate compliance with any particular requirement. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (9) Attachment 1, statement under Header 1 “High Impact Rating”. Duke suggests that the following sentence be removed, “Each BES Cyber System used by and located at:” as Duke is proposing, per (5) above, that sites be assessed against the criteria within Attachment 1. (10) Attachment 1, statement under Header 2 “Medium Impact Rating”. Duke suggests that the following sentence be removed, “Each BES Cyber System, not included in Section 1, above, associated with the following:” as Duke is proposing, per (5) above, that sites be assessed against the criteria within Attachment 1. (11) Attachment 1, Criterion 2.1. This criterion currently contains information for assessing BES Cyber Systems, which is no longer appropriate, per Duke’s proposal in (5) above, when categorizing sites. Duke suggests that the language, “For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equate or exceed 1500 MW in a single Interconnection.” be removed. This 15 window is already implied in the definition of BES Cyber Assets and doesn’t need to be re-stated here. (12) Attachment 1, Criterion 2.5. It is unclear how to treat a double circuit line in this criterion. Please clarify how a

double circuit line (i.e., two circuits connected between the same substations and referred to as a line) should be treated when calculating the “aggregate weighted value” of a Transmission Facility. If the intent was to assign weight per each circuit, change the last sentence of the criterion to “The aggregate weighted value for a Transmission Facility is determined by summing the “weight value per circuit” shown in the table below for each circuit leaving the station that is connected to another Transmission station or substation”. Change the title of the second column in the table to “Weight Value per Circuit”. (13) Attachment 1, Criterion 2.3. The phrase in this criterion, “in the planning horizon of more than one year” is confusing – it is not clear when the one year is measured from. Duke proposes the phrase to change to “with a duration of more than one year in the planning horizon.”. (14) Attachment 1, Criterion 2.10. The wording in this criterion changed from “Each System or Facility” in version 4 to “Each System or group of Elements”. This could be read to include individual, unconnected relays that have a common trip set point. Duke suggests the following rewording to clarify it is control system and not individual relays. “Each System or group of Elements that performs automatic Load shedding under a single common control system (excluding individual, unconnected relays), without human operation initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS), as required by its regional load shedding program. (15) Attachment 1, statement under Header 3 “Low Impact Rating”. Duke suggests that the following sentence be removed, “Each BES Cyber System, associated with:” as Duke is proposing, per (5) above, that sites be assessed against the criteria within Attachment 1. (16) Attachment 1, criteria 3.2 and 3.3. Duke suggests moving these criteria back to the Medium Impact classification. Duke does not agree with the assertions that having this criteria in Medium Impact would cause entities to remove facilities from their restoration plans in order to lessen the compliance burden associated with CIP. Duke believes that the basis for the impact any facility has on the reliability of the BES, should be unassociated with the compliance aspects. Blackstart resources should be appropriately represented as having a medium impact to the overall reliability of the BES.
No
No
No
No
No
Yes
(1) Requirement R1.3. The list of sub-requirements under R1 all appear to align with the set of CIP standards with the exception of R1.3. Interactive Remote Access is covered under the other sections like “Electronic Security Perimeters” and “System Security” and should need to be called out specifically. Duke suggests removing R1.3 as a way to better align this list with the remainder of the CIP standards. (2) Requirement R2. Duke suggests rewording this requirement for better readability. Rather than stating the requirement as a negative, Duke suggests the following replacement language, “For Low Impact BES Cyber Systems, each Responsible Entity shall implement one or more documented cyber security policies that addresses the following topics.”. (3) Requirement R2. Duke suggests rewording the last statement of the requirement, after the sub-requirements have been listed to, “An inventory, list, or discrete identification of Low Impact BES Cyber Systems is not required.” Without the “Low Impact” phrase, this could incorrectly be applied to any BES Cyber Systems which is assumed to not be the intent. (4) Requirement R3. Duke suggests rewording this requirement to “Each Responsible Entity shall identify the role of CIP Senior Manager by name.” Duke is suggesting this change as the current wording may be interpreted to mean that auditors would be looking for someone with the job title of CIP Senior Manager. Entities should be given the explicit permission to identify the CIP Senior Manager by role at a minimum, without necessarily creating a title. (5) Measure M3. The guidance portion related to M3 provides some details that Duke suggests would be better included in the actual language of M3. This language is referring to the guidance that dated/signed approvals, designations, etc can be electronic or hardcopy. (6) Measure M4. Duke recommends that consistency be applied to the way measures are formatted throughout the standard. Currently, some are bulleted (implying an OR statement in between them) and some are numbered (implying an AND statement in between them). If measures are intended to be non-prescriptive, all measures should be written consistently with bulleted items and “or” statements placed at the end of every bullet. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (7) Requirement R5. Duke is concerned with the last phrase of the requirement reading, “and approved by the CIP Senior Manager”. The current language suggests that the CIP

Senior Manager would have to approve his/her own delegations, while it should be implied that the naming of a delegation carries with it the approval of CIP Senior Manager. Duke suggests rewording this phrase to “as approved by the CIP Senior Manager” to lessen the burden of documenting an additional approval that shouldn’t be required.
Individual
Martyn Turner
LCRA Transmission Services Corporation
Yes
Yes
Yes
No
Yes
Yes
Yes
Yes
R2: to match the rest of the proposed language, the VRF for R2 should be “Lower” to match the standard language (p. 9) and in the text it should also be changed to “Lower” instead of “Medium” (p. 14).
Individual
Michelle R D'Antuono
Ingleside Cogeneration LP
No
Yes
Ingleside Cogeneration supports the greater part of the categorization criteria supplied in CIP-002-5-Attachment 1. However, we have a few major concerns which prevents us from entering a “yes” response in our ballot. The first is there should be one additional category added to the CIP Version 5 Standards, which should be “No Impact”. In the SDT’s Consideration of Comments document, the justification for eliminating this category was that it was a key feature of the NIST Risk Management framework. However, FERC Order 706 paragraphs 25 and 233 do not require strict adherence to NIST, only that the ERO strongly consider their application with respect to BES cyber security. We believe that the size and variety of programmable devices that support BES facilities is far outside of the practical application of the NIST framework – which should be directed at the most vulnerable systems first. Otherwise industry and compliance resources will be overwhelmed with tracking adherence in small systems, to the detriment of the larger ones. In addition, the text in Item 2.8 calls for a Medium-Impact categorization of certain “Transmission Facilities providing the generator interconnection…”, this terminology is inconsistent with that developed under Project 2010-07, which uses “generation interconnection Facility” instead. This is an important distinction, because a Transmission Facility is subject to every TO/TOP requirement, while a generation interconnection Facility is subject to a special subset only. It took a long time for the GOTO team to craft acceptable language, and we recommend it to be used here. We also disagree with Item 2.11, which assigns a Medium-Impact rating for “Control Centers and associated data centers not included in High Impact Rating (H), above, that: … control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” This has been justified by the drafting team as analogous to the automatic load-shedding item (2.10), although in the source direction, not the sink. However, the difference is extensive. A compromised automated load shedding system will lead to an immediate loss in service. A generator control center can deploy other compensating measures before the impact is noticed. In addition, the loss in 300 MW of load has deep historical ties to reliability – a connection captured in DOE and NERC Disturbance reporting. Conversely, the loss of generation is historically tied to Interconnection reserve capability – which aligns with the 1500 MW number used in Item 2.1. We have not seen data that indicates that a Control Center controlling 300 MW of aggregated generation poses an additional reliability risk that would justify the cost of implementing over 100 CIP requirements. Furthermore, we have not seen a FERC directive calling for it. We recommend that the sentence be stricken to allow

the industry to focus on the truly critical systems.
Yes
No
Yes
Yes
Yes
Yes
Ingleside Cogeneration LP is very supportive of the reduction in the requirements applicable to Responsible Entities with identified Low-Impact BES Cyber Systems. The volume of new CIP policies that will be need to be developed and implemented is enormous – and should be approached at a high level initially. Over time, future versions of CIP-003 can require more detail, provided they are vetted through the Standards Development Process. However, we are concerned that there is too much leeway for interpretation in the language of the requirements and the associated text in the "Guidelines and Technical Basis". R2 only calls for policies which "address" four specific topics in Low-Impact policies, but no limits are given. The guidelines express the intent to "outline a set of basic protections", but is offset by a statement that "cyber security policy must cover in sufficient detail the 4 topical areas". In order to eliminate any ambiguity which will serve to incentivize the development of CANs, we suggest the following language to be added to R2.1 through R2.4: 2.1 Cyber security awareness. Acceptable policies will address periodic high-level training, less formal reviews with appropriate personnel, or the posting of cyber security policies on the corporate Intranet site/company bulletin boards. 2.2 Physical access control. Acceptable policies will address operational or procedural controls which restrict physical access such as card key, special locks, security personnel, or other authentication methods. 2.3 Electronic access control. Acceptable policies will address operational or procedural controls which restrict electronic access from public or other less trusted network zones through proxy servers, DMZ, password protections, or other authentication methods. 2.4 Incident response to a BES Cyber Security Incident. Acceptable policies will address high-level training to identify BES Cyber Security Incidents and the reporting of cyber intrusions to ES-ISAC.
Individual
Joe Petaski
Manitoba Hydro
No
Yes
"…associated data centers" in Attachment 1 -1.1, 1.2, 1.3 and 1.4 are unclear. It needs to clarify what degree of the communication or connection between associated data centre and a control centre is deemed to be an associated data centre, otherwise, it can be very broad.
Yes
Yes
Yes
Yes
Yes
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Group
Arizona Public Service Company
Janet Smith
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Michael Schiavone
Niagara Mohawk (dba National Grid)
No
Yes
We recommend the following wording for R 1.2 (we moved “high impact to be in front of Facilities): 1.2. Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the high impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We recommend the following wording for R1.3 (we moved “medium impact” to be in front of Facilities): 1.3 Identify each BES Cyber System and its associated BES Cyber Asset(s) used for the medium impact Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; We also recommend that the CIP Process Flow on the last page be updated to show clearly that the identification of BES Cyber Assets should occur first, followed by identification of BES CYBER Systems
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Yuling Holden
PSEG
No
Yes
Attachment 1 section 1.4 and 2.11 contains the undefined word “control.” PSEG believes “control” must be clarified to ensure it is consistent with the description under the BES reliability operating service “Monitoring and Control” in the latest version of CIP-002-5, p. 23. The Control Center definition, which uses the phrase “monitor and control,” should also capture aspects of in a manner consistent with what is included under Monitoring and Control service (i.e. all methods of operating breakers and switches, SCADA, and substation automation). Additionally, in the CIP-002-5 v5, p. 24, the BES reliability operating service “Situational Awareness,” as written, could inadvertently capture monitoring and alerting activities that are performed for general management and economic / market

decision making. For example, monitoring EMS status information and alarms by areas that do not have the physical or automated control of the equipment; and the authority to change a generating asset's output should be excluded to ensure they are not inadvertently captured in the application of this standard.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Jonathan Appelbaum
United Illuminating Company
Yes
Yes
UI Agrees with EEI Consensus comments. In addition for R1.4 does within 60 days mean plus or minus 60 days or at least 60 days prior to being placed into operaton. Second Comment is referring to Guidance in CIP-002 for identifying Transmission Owner assets that are being used by a Transmission Operator to perform the TOP functional obligation. (1) UI believes the guidance should be specific as to whether the performance of remote switching by a Transmission Owner from its control center under the direction of the Transmission Operator is performing a functional obligation of the TOP. (2) Similarly, in an Emergency the TOP may direct its Transmission Owners and Distribution Providers to perform manual load shed, would this cause the Transmission Owner Control Center to come into scope as performing a functional obligation of the TOP. (3) If Data from a medium impact substation passes to Transmission Owner data center on the Transmission Owner network, and is then sent to an ICCP server to its TOP and RC is the data center performing the functional obligation of the TOP. Third Comment relates to Technical Guidance for the application of CIP-002 which should provide increased clarity on the acceptability of segmenting facilities at a single site to achieve tiering of impacts. The present explanation on page 25 of 33, first bullet, describes separating transmission equipment from distribution equipment. The explanation should allow for separation of Transmission Facilities as well. For example, assume a transmission substation where two 500 kV lines connect, two 345 kV lines connect and six 115 kV lines. The 500 kV lines would cause the site to be categorized as Medium Impact. We propose that only the 500 kV Facilities would be categorized as Medium Impact and the 345 kV Facilities and 115 kV Facilities would be Low Impact. With proper cyber network segmentations it is achievable to separate the BES Cyber Systems associated with the 500 kV medium impact facilities from the BES Cyber Systems associated with the 345 kV and 115 kV Low impact facilities.
Yes
Yes
Yes
No
Yes
Yes
UI concurs with EEI consensus comments. In addition, R1 requires implementation of the Policies. The entire suite of CIP standards is the implementation of processes to comply with the standards and the Policy. Implementation of Interactive Remote Access Policy required by CIP-003 1.3 is what the Requirements in CIP-005 and CIP-007 is accomplishing. If the other CIP standards were not in existence then we can understand the need to require implementation of the Policies. The requirement requires proof of implementation which means duplicating the evidence submissions for the entire sutie of CIP Standards.The Rationale box states this requirement is about demonstrating management's supports the cyber security program. The Guidelines does not clarify or explain what implementation means. UI suggests the phrasing Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall have one or more documented cyber security policies that

address the following topics. For R2 it is appropriate to keep implementation because the other CIP Standards do not address BES Cyber Systems associated with Low impact Facilities. For R4 We believe the use of reviewed and approved is unnecessary. We believe that the requirement should only be for approval. The completion of the review is attainment of the Senior Manager's approval. We do not believe that the drafting team desired to track the review periodicity separate from the approval periodicity.
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Attachment 1, parts 1.2 and 1.4, contain the words "generation assets that meet criteria 2.3, 2.6, and 2.9". However, some of the assets mentioned in criteria 2.6 and 2.9 are not "generation" assets and therefore would be unintentionally excluded from parts 1.2 and 1.4 if the current wording is retained. We suggest changing "generation assets" to "assets" in parts 1.2 and 1.4 of Attachment 1.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Alice Ireland
Xcel Energy
Yes
Yes
No
No
Yes
Yes
No
Yes
1) R1 (and R2) it's unclear what 'implement' entails (do we need to provide evidence of communication, training? – those aren't listed in M2). 2) R1 Our company has a limited set of Policies, instead putting detailed information into standards and procedures that are in force through a Policy. We would like the flexibility to cover R1.1-R1.10 through a combination of policies and standards. 3) R5 please define 'where allowed by the CIP standards'. It is unclear where it is required to have formal delegation, and where it is obvious that the Sr. Mgr. will not be performing the function (for example, approval of access to systems and provisioning which are performed by a separate group of individuals who may or may not report, operationally, to the Sr. Mgr). 4) R1.10 'provisions for declaring' CIP Exceptional Circumstances should be clarified to not imply that we list all possible scenarios where we would invoke CIP Exceptional Circumstances. Suggest instead 'process for declaring' which would focus on how to communicate and document the circumstances and rationale for declaring at the time of the event.
Group
PNGC Comment Group
Ron Sporseen
Yes
Yes

The PNGC Comment Group is in agreement with NRECA's comments on CIP-002 and CIP-003: 4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying “that are part of a Load shedding program” implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW “program” and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. NRECA recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. Under the inclusion threshold for DP, 4.2.2, third bullet, states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” NRECA recommends that the following language be added to the end of that bullet; “, and where the Protection System is connected to a supervisory control system providing remote operation capability.” This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. Attachment 1 2.10 – see comment above 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for NRECA. It will be difficult to support CIP-002-5 without this revision.
Yes
Yes
Yes
Yes
Yes
Yes
CIP-003 – Ballot Recommendation – Negative R2 – NRECA is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, NRECA requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance.
Individual
Russ Schneider
Flathead Electric Co-op
Yes
Yes
Under the inclusion threshold for DP, 4.2.2, third bullet,: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” Flathead requests that this be clarified to only include configurations “, and where the Protection System is connected to a supervisory control system providing remote operation capability.”
No
No
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
No
Yes
BPA recommends the SDT replace “…affect the Reliable Operation of the BES” in the definitions, background, guidelines, and wherever possible throughout the standard with “…prevent the entity from maintaining the reliable operation of the BES.” The latter is a much more succinct requirement because it allows for the use of the word “prevent” to establish a threshold. The terms “affect” or

“negatively impact,” which are inconsistently used throughout the standard are vague, and subject to interpretation. BPA approves of the 15 minute window to help define the Real-Time environment and was only able to understand the intent of the SDT by reading page 32 of the SDT’s reply to previous comments. BPA recommends the language used to articulate the Real-Time window of 15 minutes, found on page 32 of the SDT’s reply to previous comments, be used in the definitions, background and guidelines document. BPA recommends the SDT create a term (e.g. Critical Asset, BES Asset, or something similar) for the phrase “Facilities, systems or equipment that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria.” This would make the definitions easier to read, and facilitate discussion and documentation requirements. BPA recommends the SDT consider that the process for identifying BES Cyber Assets is typically different in Control Centers than in the field. Control Centers will identify BES Cyber Systems (e.g. information systems like SCADA and AGC) first, and then identify the BES Cyber Assets that those systems comprise. While field sites will typically identify BES Cyber Assets first, and then group those Cyber Assets into BES Cyber Systems. These “BES Cyber Systems,” in many cases, will be little more than collections of devices organized by type; they may be geographically separated with no connectivity or limited serial connections. BPA HAS CONCERNS with: 1) Potential problems emerging from using the same term (i.e. BES Cyber System) to describe two disparate structures with intrinsically different characteristics. 2) The inability to apply controls intended for BES Cyber systems that are information systems on BES Cyber Systems that are collections of standalone devices (relays, telemetry, GPS) which meet the definition of BES Cyber Asset, but can only be accessed physically (i.e. non-routable, non-dial up accessible) or via point-to-point serial connection. BPA believes these devices must be secure and questions whether a “one size fits all” approach is the most efficient and effective use of the standard. Would it not make more sense to tailor a portion of the standard to these types of devices specifically? BPA recommends that the SDT provide clarity on what is included in the “Facilities, systems, equipment” specified in Attachment 1. There is also an inconsistency between this phrase in the definitions and Attachment 1; “Systems” being capitalized in the former and not the latter. BPA requests the SDT address an apparent conflict between the BES Cyber Asset definition and the CIP-002 guidelines. The proposed definition of BES Cyber Asset focuses on real-time by applying to cyber assets that would adversely impact BES operations (via Facilities, Systems or equipment) within 15 minutes if destroyed, degraded, or otherwise rendered unavailable when needed. In the CIP-002-5 Application Guidelines, “Current Day and Next Day planning” systems are included in the Situational Awareness component. As the 15 minute window pertains to the Cyber Asset, rather than the asset itself (i.e. Facilities, Systems or equipment), any Cyber Asset that would be included in a “Current Day and Next Day planning” system would not meet the current criteria for a BES Cyber Asset, unless such a planning horizon was 15 minutes or less.
Yes
No
Yes
Yes
Yes
Yes
R1 provides a list of mandatory topics on which BPA is to write policy. The guidelines provide more granular topics that BPA is to address. BPA believes that it should be able to have a cyber security program which includes policies that are relevant to our environment. Should BPA’s policies encompass some or all of the topics listed in the standard, than that is what BPA believes is needed to maintain and secure our environment. BPA does not favor requirements that are seemingly in place for the sake of compliance. BPA recommends removing the list of mandatory cyber security policy topics and associated granular requirements in listed in the guidelines. Regarding R2 – BPA recognizes that CIP version 5 does not require low impact systems to be documented. How is BPA to certify the application of these polices on systems which are not required to document? For example, BPA’s access control policy for Low impact system could state that we require strong passwords however, if are not required to have a list of these systems, how can BPA be held accountable in ensuring the policies are being applied? Therefore, BPA recommends removing R2 from the CIP-003 version 5 standard OR require low impact systems to be documented in regard to R2 accordingly.
Individual
Larry Watt

Lakeland Electric
No
No
"Please see comments submitted by FMPA through the formal comment process."
Yes
No
No
No
No
No
"Please see comments submitted by FMPA through the formal comment process."
Individual
David R. Rivera
New York Power Authority
No
No
NYPA agrees with NPCC comments, plus - In Attachment 1, please clarify 'Functional Obligations' (1.3) and 'Data Center' (1.4). Can we have clarification on what is meant by 'Associated Contingencies' in reference to the derivation of IROL (2.6)?
Yes
Yes
Yes
Yes
No
No
NYPA agrees with NPCC comments
Individual
Ron Donahey
Tampa Electric Company
No
No
Tampa Electric supports the Edison Electric Institute (EEI) comments especially related to the identification of Low Impact BES CS at a Facility level. Listing all the Cyber Assets associated with a Low Impact Facility as this would add administrative burden and not provide additional BES CS security or BES reliability. Tampa Electric offers these changes to CIP-002 with the following additional clarifications and suggestions: Q1. 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.? This could be handled through the definition or guideline. Q2. Tampa Electric provides 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.
Yes
No
No
No

No
No
Tampa Electric supports the comments submitted by EEI. In addition, Tampa Electric suggests that there is a clerical error in the Introduction, section 4.2.4 where it provides exemptions from CIP-002-5. This would seem to reference exemptions from CIP-003-5. We request additional clarification for M2 to describe what would be sufficient in terms of evidence? We note that the R4 rationale is a sentence fragment (ends at 'proving'). We suggest that the SDT review the R4 rationale: this requirement is for approval but the R4 rationale calls for availability of the policy to all personnel. For R5, please clarify if the standards state which can be delegated? Tampa Electric suggests that the VRFs – R2 should be Lower as they apply for lower impact systems. In the Application Guidelines R3, should this reference R3 or R5?
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Request clear definition of "BES Element". General comment to all Measures - Remove the" not limited to" clause. These are examples of proof of compliance. This might be taken by auditors to mean must. This should include the word "example". R1.3 - How do you prove a Low impact facility classification with no discrete identification process? Attachment 1, 2.3 - Should there be a megawatt qualifier? Attachment 1, 2.11 - Replace 300 MW with 1500 to be consistent with other standards. Attachment 1, 3.2 - Change to blackstart resources not otherwise classified as high or medium is low.
Yes
Yes
Yes
No
Yes
Yes
CIP-003-5 R4 as stated doesn't clearly define the extent to which policies will have to be signed by the CIP Senior Manager. Without clear guidance this may lead to signatures on all implementing policies throughout the company. This could delay updates and implementation. Delegation should be allowed beyond an overarching policy. R1 and R2 state each Responsible Entity shall implement one or more documented cyber security policies that address select topics and M1 and M2 states Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics. Does this mean that the Senior Manager must approve all cyber security related processes, procedures, and plans in addition to the high level cyber security policy? R1.3 - Delete interactive remote sessions this is included in 1.2. R3 - Allow to define CIP senior manager by name, title or role instead of just name. R4 - This is the only area CIP senior manager cannot delegate authority. Add delegate authority.
Individual
Thomas Washburn
FMPP
See FMPA comments for all of the CIP V5
Individual
Annette Johnston
MidAmerican Energy Company
No
No
GENERAL COMMENTS: (1) ANNUAL: MidAmerican Energy proposes the text for all annual requirements be revised to reduce the administrative burden of tracking two dates, which would be necessary based on the draft 2 language of "at least once each calendar year, not to exceed 15 calendar months…" The following proposed text would allow entities to track one date instead of two

for its annual reviews: “once each calendar year or a period not to exceed 15 calendar months.” (2) BLACKSTART/CRANKING PATH UNITS: We understand the rationale behind removal of the blackstart and cranking path units by deleting 2.4 and 2.5 from the CIP-002 Attachment 1. We think it will be critical to include technical and risk-based justification for not “lessening” the standard by making this change. CIP-002 R1 COMMENTS: (3) MidAmerican Energy Company supports the MRO NERC Standard Review Forum’s proposed solution that clarifies the flow for identifying BES Cyber Systems. It is important to note that the proposal supports and does not change the SDT’s desired flow for identifying BES Systems, does not change the outcome for identified high and medium BES Cyber Systems and does not change the SDT’s identification of blackstart resources and cranking paths as low. The proposal retains Attachment 1 high and medium unchanged. The proposal supports SDT’s intent that lists of low Cyber Assets are not required. (4) The proposal first identifies BES Sites (a new definition), some of which would be identified as low and used for the CIP-003 R2 programmatic controls for lows. The proposal bounds the scope for lows by defining low BES Sites positively (what they are) instead of in the negative (what they are not) and revises part 3 of Attachment 1 for lows accordingly. The proposal leverages lists entities need to have for Operating and Planning Reliability Standards so that new development is not required for the proposed BES Sites. (5) The proposed draft 3 approach addresses industry confusion with draft 2 for clarity of flow of identifying BES Cyber Assets and BES Cyber Systems subject to CIP. The proposed wording more closely follows the description of flow in version 4. Stated again, the proposed wording does not change the SDT’s intended flow and is offered constructively for consideration to resolve confusion over the wording of the flow in draft 2. (6) The proposal is offered to help gain approval of CIP-002-5. The proposal also supports EEI’s key issues strategies: defines low impact at a site level, proposes language to address zero-defect requirements, differentiates VRFs by BES Cyber System impact categories and refines “annual.” (7) A summary of key proposed draft 3 CIP-002 requirements follows, along with measures, VRFs, VSLs and rationale. (8) BES SITE: Substations 100kV and above, generating units above (insert # to set the floor) MW (MVA?), control centers and backup control centers used by NERC certified operators to support the real time operations of the interconnected Bulk Electric System, Blackstart Resources, Cranking Path and initial switching requirements. [Note to SDT: The lists are based on existing lists entities need for Operating and Planning Reliability Standards applicable to their NERC registration criteria.] (9) FLOW FOR PROPOSED CIP-002-5 DRAFT THREE: R1. Select BES sites. ** R2. Identify high impact Facilities, systems or equipment at BES sites on the R1 BES Sites list using Att 1 Part 1. Identify the high impact BES Cyber Assets used by the high impact Facilities, systems, equipment in R2. ** R3. Identify medium impact Facilities, systems or equipment on the R1 BES Sites list using Att 1 Part 2. Identify the medium impact BES Cyber Assets used by the medium impact Facilities, systems, equipment in R3. ** R4. Identify BES Sites on the R1 BES Sites list that are not included in high or medium. These BES Sites are low. ** R5. Identify the Electronic Access Control or Monitoring Systems and the Physical Access Control Systems. ** R6. Identify Protected Cyber Assets. Assign medium or high. ** R7. Senior manager approve lists in R2-R3 once per calendar year or not to exceed 15 months between approvals. (10) RATIONALE FOR FLOW CONSTRUCTION: Senior manager approval of highs and mediums corresponds to existing requirements for approval of Critical Cyber Assets in version 4. (Note: Flow is proposed as separate Rs, but could be constructed as sub-requirements.) R5 and R6: CIP versions 1-4 identified the following: ESP control or monitoring (CIP-005); noncritical (CIP-005); and PSP authorize or log (CIP-006). CIP version 5 draft two assumes identification of EACs, PACs and Protected Cyber Assets in CIP-003 through -011, but technically does not identify them anywhere in CIP-002 through -011. Propose identification of these in CIP-002. Propose all EACs and PACs are medium, even if associated with high. Inherently, they should not have a 15 minute impact on the grid directly. Differentiating these systems between high and medium causes further complexity without a commensurate increase in security. Some devices that are included as Cyber Assets in these systems are not all capable of the additional controls applied to high and would require TFEs for the high controls and/or create additional work, much manual, without commensurate increase in security. (11) ATTACHMENT 1: 3. Low Impact Rating: R3.1- Substations 100kV and above and not included in medium or high; R3.2: Generating units __ MW (or MVA?) and above and not included in medium or high. (insert # to set the floor – number may be higher than but should not be lower than the minimum aligned with NERC Registration Criteria.); R3.3: control centers and backup control centers used by NERC certified operators to support the real time operations of the interconnected Bulk Electric System and not included in medium or high; R3.4: Blackstart Resources and not included in medium or high; R3.5: Cranking Path and initial switching requirements and not included in medium or high. (12) CONTINUOUS IMPROVEMENT vs. ZERO

DEFECT: Include language in the requirement(s), except senior manager approval, that aligns with prior FERC orders speaking to cultures of compliance that implement, detect, correct and prevent. “The Responsible Entity shall update list(s) as necessary, and review list(s) once each calendar year or not to exceed 15 months between reviews. Each Responsible Entity shall implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations, per se.” NIST 800-53 minimum assurance requirements for security controls emphasize continuous improvement, expect “expeditious” correction (“timely” for lows) and do not expect perfection. The NIST 800-53 quote is included at the end of these comments. It is also proposed in response to FERC’s order on find, fix and track. In paragraph 81 (included at the end of these comments), FERC asked industry for proposals to revise or remove requirements to focus resources on serious risks to reliability. It also aligns with preliminary efforts to move toward more risk based auditing. (13) VRFs FOR CIP-002: Separating requirements, allows different VRFs for different requirements. No high VRFs are proposed based on a review of all VRFs for all Reliability Standards. High impact category is proposed for medium VRF. All else is proposed for lower VRF. (14) VSLs for identification: Lower-Did not take corrective action, if needed, that may prevent recurrence of flaws; Moderate- Did not correct flaws detected; Higher: Did not measure performance to detect flaws; Severe- Did not implement. (15) VSLs for Senior Manager approval: Lower-Failed to complete senior manager review according to Requirement R7 for more than 30, but less than 41 calendar days; Moderate- Failed to complete senior manager review according to Requirement R7 for more than 40, but less than 51 calendar days; Higher- Failed to complete senior manager review according to Requirement R7 for more than 50, but less than 61 calendar days; Severe-Failed to complete senior manager review according to Requirement R7 for more than 60, calendar days. (16) NIST 800-53 Appendix E: Appendix E describes the minimum assurance requirements for security controls in low-impact, moderate-impact, and high-impact information systems. For security controls in low-impact systems, the emphasis is on the control being in place with the expectation that no obvious errors exist and that as flaws are discovered, they are addressed in a timely manner. For security controls in moderate-impact systems, in addition to the assurance requirements for low-impact systems, the emphasis is on increasing the grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to increase grounds for confidence that the control meets its function or purpose. For security controls in high-impact systems, in addition to the assurance requirements for moderate-impact systems, the emphasis is on requiring within the control, the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control’s effectiveness. There are additional assurance requirements available to developers/implementers of security controls supplementing the minimum assurance requirements for the moderate-impact and high impact information systems in order to protect against threats from highly skilled, highly motivated, and well-resourced threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above. (17) FERC order paragraph 81: The Commission notes that NERC’s FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently. (18) CIP possible violations were 91 percent of the FFTs in the order. CIP standards occupy 8 of the top 10 most violated standards slots.
No
No

Yes
No
No
No
(1) CIP-003 R1 REQUIREMENT: In its draft 1 comments, MidAmerican Energy proposed language closer to 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. In its consideration of comments, the standards drafting team stated it was attempting to bring the language in line with NERC Results Based standard format. However, draft 2 does not move toward results-based and, in fact, moves away from results based by becoming prescriptive with the enumerated topics. MidAmerican proposes deleting the enumerated topics in 1.1 through 1.10. Refer to “the CIP standards” (but not by number) to make the scope of the policies clear, but flexible enough if there are changes in the CIP standards in the future. Incorporate R4 into R1 and R2. MEC proposes the following language: “Document and implement a cyber security policy that represents management’s commitment and ability to secure its BES Cyber Assets. The Responsible Entity shall, at minimum, ensure the cyber security policy addresses the CIP standards, including provision for CIP Exceptional Circumstances. NEW R1.1. MidAmerican Energy proposes CIP-002 R4 be incorporated into R1 as a new R1.1. (2) CIP-003 R1 GUIDANCE: The guidance in the first paragraph is sufficient to meet the FERC directive. Delete the enumerated topics, which suggest far too much detail for a policy. (3) CIP-003 R2 REQUIREMENT: The following is proposed: “For low BES Sites each Responsible Entity shall: implement policies; measure performance to detect flaws in its policies; correct detected flaws in its policies expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations, per se. The following topics shall be addressed in policies …” (4) Restructure R2.1 to be the four programmatic controls and create a new R2.2 to cover the R4 approval (deleting draft 2 R4). (5) R2.1.1 AWARENESS: This is acceptable if CIP-002 is changed to require identification of BES Sites, and this is applied at the site level for lows. (6) R2.3: Qualify electronic access control for external routable connectivity or dial up accessibility. This prioritizes resources on the higher risk areas. (7) R2.4: MidAmerican Energy proposes limiting this requirement to “incident response” and delete the phrase “to a BES Cyber Security Incident.” This requirement still refers to “BES Cyber Security Incident,” but “BES” has been removed from the glossary term. Low impact does not require PSPs or ESPs, but the definition of a Cyber Security Incident is specific to an incident that compromises or was an attempt to compromise an ESP or PSP. While it may be possible to have some type of incident response for low impact, it cannot be tied to the glossary term of Cyber Security Incidents because of the lack of ESPs and PSPs for low impact BES Cyber Systems. (8) CONTINUOUS IMPROVEMENT: MidAmerican Energy believes that version 5 of the CIP standards provides the opportunity to move toward results based standards that focus on continuous improvement for improving reliability rather than “zero defect” compliance. Throughout our comments, we provide suggested language to incorporate the concepts of measuring performance to detect flaws, correct flaws and take action that may prevent recurrence (if applicable for the flaw). The CIP standards were eight of the top 10 most violated standards in 2011, and 91 percent of the find, fix and track violations approved by FERC in March 2012. FERC invited NERC to revise or remove requirements that do not improve reliability. NIST 800-53 App. E Minimum Assurance Requirements recognize flaws will be discovered and focus on continuous improvement. Other federal regulators, including the EPA and NRC, do not enforce zero-defect forever compliance. MidAmerican Energy is proposing language be added to the R2 requirement statement that flaws that have been detected and corrected would not be violations. (9) CIP-003 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (10) CIP-003 R2 GUIDANCE: Revise to correspond to use of “low BES Sites” in proposed changes to R2. (11) CIP-003 R4 REQUIREMENT: Incorporate this into R1 and R2 as mentioned above, and delete R4. (12) CIP-003 R3, R5 and R6 REQUIREMENTS: ** CONSOLIDATE REQUIREMENTS: Only one requirement is needed to accomplish the reliability benefit of clear accountability within an organization for certain security matters. Combine requirements R3, R5 and R6 into one. ** ANNUAL: Revise the requirement to ““once each calendar year or a period not to exceed 15 calendar months.” (13) CIP-003 R4 REQUIREMENT: Incorporate this requirement into R1 and R2 and delete R4.
Group

FirstEnergy
Doug Hohlbaugh
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
FE suggests that the measure for M2 be adjusted to remove the phrase “or plans that demonstrate the implementation of the required topics”. The text seems to imply an auditor may be looking for specific application or implementation of the required R2 policies on individual low impact BES Cyber Systems even though a discrete list of those systems is not required. (Please see our comments in Form D question 16)
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No
Yes
(Comment 1) R1.1 appears to require the entity to maintain a list of “Facilities, Systems, or equipment that meet the criteria specified in CIP-002-5, Attachment 1.” This seems to be inconsistent with what is stated in the Rationale and the Guidelines, which only refer to identifying BES Cyber Assets and BES Cyber Systems. We suggest that the SDT clarify the intent and the auditable requirement by adding an explanation to the Rationale, Guidelines or M1. (The following comments 2 through 5 apply to section 4.2 for all of the CIP standards.) (Comment 2) Change “One or more of the Systems or programs” to “One or more of the FOLLOWING systems or programs.” (Comment 3) We support comments submitted by APPA for Question 3 regarding the Applicability section (especially with regard to the third bullet of 4.2.2) and Attachment 1. (Comment 4) We recommend the following addition to section “4.2.4 Exemptions” in order to clarify that only the systems specified under section “4.2” are in scope for DPs and LSEs: “4.2.4.4 Cyber Assets that are owned by DPs or LSEs and that are not associated with the Facilities, systems or equipment described in 4.2.1 or 4.2.2.” (Comment 5) Since the glossary definition of “System” is “A combination of generation, transmission, AND distribution components,” we question whether a DP or LSE would own a “System”. Please check each use of capitalized “System” in section 4.2, especially when used as “UFLS System” or “UVLS System”, in order to clarify applicability.
Yes
Yes
Yes
Yes
Yes
Yes
MMWEC agrees with and supports the comments submitted by APPA. We are concerned that R1.1 will present compliance challenges, since it is unclear what constitutes sufficient “implementation of the required topics.” More suggestions or examples in the Guidance section regarding the content of the policies for Low Impact entities may help.
Individual
Bob Thomas
Illinois Municipal Electric Agency
No
No

Illinois Municipal Electric Agency supports comments submitted by American Public Power Association and Florida Municipal Power Agency.
Yes
No
No
No
No
No
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Group
Dominion
Connie Lowe
No
Yes
- In CIP-002-5 Attachment 1, the threshhold in 2.11 should be changed to 1500MW to be consistent with other medium impact facilities (generation units). The language should be changed to: "2.11. Control Centers and associated data centers not included in High Impact Rating (H), above, that: (1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW or more of BES generation." -The Use Case: CIP Process Flow in the Application Guidelines of CIP-002 contains the term "External Connectivity" in the third and fourth process boxes. This term is not a defined term. The term either needs to be changed to "External Routable Connectivity" or the capitalization on the term removed.
Yes
Yes
No
No
Yes
Yes
CIP-003-R3 - R3 should be reworded to be "Each Responsible Entity shall identify a CIP Senior Manager by name, title, or role." in order to allow Responsible Entities additional flexibility and to reduce the impact of personnel changes on policy and procedure documentation. CIP-003-R4 - The introductory language in Measure M4 for 4.2 reads as though the two items identfied as expected evidence are optional. The introductory language to the measure should be changed to, "Examples of evidence include:".
Group
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)
David Dockery, NERC Reliability Compliance Coordinator, AECI
No
Yes
[Introduction, p 6, part 4.2.2 REPLACE: “A Protection System” WITH: “A Protection System (other than UFLS or UVLS Systems)” Rationale: AECI agrees that PRC-005-2 will likely classify UFLS and UVLS systems as Protection Systems. While the second bullet above demonstrates intent of this standard to be limited in scope to UVLS and UFLS Systems of sizes that would clearly impact the BES, this bullet could inadvertently include the remaining UVLS and UFLS unless specifically stated to exclude them.] [Introduction, p 6, part 4.2.4 ADD: “4.2.4.4 Cyber Assets that are owned by Distribution Providers or Load Serving Entities and that are not associated with the Facilities, Systems and equipment specifically described within parts 4.2.1 or 4.2.2 above.” RATIONALE: Further clarifies the CIP SDT’s intent of scope represented within parts 4.2.1 and 4.2.2, and aligns with the SDT’s earlier responses back to comments voiced concerning scope of the CIP Standards upon DPs and LSEs.] [Requirement R2, p 11, Measurement M1 REMOVE: “and update, where applicable” RATIONALE: AECI’s agrees with others in industry, that the CIP Senior Manager or delegate is likely not to be the individual(s) updating the identifications required by R1.]

[==========Begin Proposed block of changes========== [Introduction] [AECI is herein proposing several changes to CIP-002-5, Appendix 1, pp 17 & 18, parts 1.2, 1.3, & 1.4, 2.10, and 2.11, in order to resolve technical discrepancies in MW impacts, and in particular deal with part 2.11's implication that any BA or TOP of any size is at least a Medium Impact, as well as the part 2.11 implication that any 300 MW has Medium Impact upon the BES, which is simply not the case. Therefore, AECI suggests revising the Bright-lines for High Impact from 1500 to 3000 MW and controlling two or more elements. The Bright-lines for Medium Impact would be 1500 MW and controlling one or more elements. This will provide a more well-defined difference between High and Medium.] [In addition, part 2.10 changes deal with the same 300 MW impact issue, in addressing centralized UVLS and UFLS system impact sizing, differentiating the two. AECI recommends changing 2.10 as described below.] [All changes are detailed below.] [End Introduction] [Appendix 1, p 17, part 1.2 REPLACE: 1500 MW WITH: 3000 MW REPLACE: "one or more" WITH: "two or more" RATIONALE: Assess High Impact to twice that of Medium Impact potential] [Appendix 1, p 17, part 1.3 REPLACE: "one or more" WITH: "two or more" RATIONALE: Assess High Impact to twice that of Medium Impact potential] [Appendix 1, p 17, part 1.4 REPLACE: 1500 MW WITH: 3000 MW REPLACE: "one or more" WITH: "two or more" RATIONALE: Assess High Impact to twice that of Medium Impact potential] [Appendix 1, p17, part 2.10 REPLACE: "of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) " WITH: "of 800 MW or more implementing Under Voltage Load Shedding (UVLS) or implementing Under Frequency Load Shedding (UFLS) within a single Interconnection in excess of thresholds in Table X (Derived once from 5%-droop for peak Interconnection load 2012, constrained to 5% error) [[Table X [[Interconnection,UFLS MW Threshold, Notes]] [[Eastern, 1500 MW,(computed value of 4144 MW capped at 1500 MW)]] [[Western, 1400 MW,(computed value was 1437 MW)]] [[ERCOT,750 MW,(computed value was 772 MW)]] [[QUEBEC,300 MW,(computed value was 310 MW)"]]]] RATIONALE: 1) Assess threshold for UVLS, no greater than a single large 800 MWnet coal-fired plant, because UVLS impacts are more localized and so a commiserate threshold is prudent in order to avoid cascading outages. 2) Assess UFLS Medium impact MW threshold level commiserate with Interconnection impacts, where no more than 5% of an Interconnection's droop-characteristic governor-responses from nominal frequency to first-step UFLS relays per PRC-006 is allowed be risked within a centralized UFLS. However, the corresponding guidelines should note that, should an Entity's centralized UFLS system fail, they could individually be assessed a Severe VSL for under-performance, and their RC be assessed greater than Low VSL for their aggregate failure to perform per current VSLs for Requirement 9 of PRC-006-1, page 13. (While this 5% margin agrees with PRC-006 Low Violation Severity Level for Interconnection Impacts, that Entity's business risk of violation due to their UFLS system's failure, could be enormous under NERC Standard PRC-006.)] [Appendix 1, p 17, part 2.11 REPLACE: "(1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation." WITH: "(1) perform the functional obligations of Balancing Authority or Generation Operator, and control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW or more of BES generation, or (2) perform the functional obligations of the Transmission Operator, that includes control of one or more of the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10. RATIONALE: Align Medium impact Medium impact 1500 MW or Asset amounts. (And see AECI recommendations for Parts 1.2..1.4 High impact ratings.)] ==========End Proposed block of changes==========]
Yes
Yes
Yes
Yes
Yes
Yes
[FYI - p 9 R2 VRF is Low, but p 14 R2 VRF table indicates Medium but should be Low]
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
Yes

Yes
none
Yes
Yes
Yes
Yes
Yes
Yes
none
Individual
Richard Salgo
NV Energy
No
Yes
The SDT has made tremendous progress on this posting of CIP-002-5. The comments that follow are specific to the items in CIP-002-5 Attachment 1: 1.2: We recommend removal of reference to criteria 2.9 first because the use of SPS threshold is inappropriate for classifying a control center as High Impact, and second, a generating asset cannot “meet” criterion 2.9. Also, the list of criteria uses the word “and” (“2.3, 2.6, and 2.9”), which is to say that in order to qualify, it satisfies ALL of these three criteria. Did the SDT intend to use the word “or” instead of “and”? 1.4: Same comment as 1.2 above. 2.1: We are concerned about the use of the “preceding 12 months” when determining the capability of the subject generation. It would seem that a forward look is more appropriate given the nature of the subsequent requirements. 2.3: We appreciate the discretion being given to the PC or TP to determine and communicate Adverse Reliability Impact; however, we question whether there is any industry guidance for the PC or TP to make this determination in a consistent fashion. 2.4: We would like clarity, either through Guidance or preferably in the language of this item, that stations at the receiving end of a radial 500kV line are NOT included in criterion 2.4. Absent this clarity, the 500kV receiving station could be inappropriately classified as Medium Impact, when it’s purpose is clearly distribution (non-BES). Consistent with the Guidance Document Transmission section discussion regarding part 2.4, the receiving station should not be considered Medium Impact even though it contains 500kV elements. 2.6: We suggest additional clarity or guidance on the intent of “derivation” in this item as it refers to IROL’s. Suggest a re-write of this criterion, but since we have no clear understanding of the intent, we cannot suggest language. As written, we are unclear as to what “associated contingencies” is referring. 2.11: We are in disagreement with the 300MW threshold for a “control center” that controls BES generation. It is unclear whether this refers to the BA/TOP control center or if this applies to generating plant control rooms. In any event, the 300MW appears to be too low when compared with the 1500MW Medium Impact threshold for the generation assets themselves.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southern Company Services, Inc.
Antonio Grayson
No
Yes
(1) Regarding CIP-002-5 R1, the essentially real-time update of potentially huge lists is problematic. The requirement to review (and update as needed) the identification within 60 calendar days creates

challenges, particularly for utilities with large amounts of facilities or systems or those experiencing constant change. The implicit requirement of needing a master list of all “BES Changes” simply to prove the start time of a 60 day update period creates an extensive new documentation requirement that is unnecessary and overly burdensome. Southern suggests refocusing R1 towards security and/or reliability outcomes rather than maintaining extensive lists of assets and changes. In addition, Southern suggests changing the review and updating of lists to be an annual activity, as to differentiate this documentation exercise from other more security or reliability focused requirements found later in the requirements. Additionally, Southern recommends deleting R1.4. (2) Regarding CIP-002-5 R1, Southern strongly suggests that the SDT consider re-using lists, where possible, as required by other NERC reliability standards to promote consistency between the reliability standards in lieu of creating a documentation exercise that has the potential to create double jeopardy in other reliability standards. (3) Regarding CIP-002-5, on page 2 of 33, the footnote, “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” is an incredibly important aspect of applying the standards. Southern suggests that the footnote needs to be promoted into the actual text of the section Effective Dates on page 2. (4) Regarding CIP-002-5, on page 18 of 33, criteria 2.11 should be removed. The stated intention in the guidance is to eliminate "run of the river" hydro control room situations from being considered control centers, but the 300MW threshold is too low to accomplish this. Southern suggests an explicit exclusion of "run of the river" hydro control rooms in the definition of control center and then remove this criterion. The SDT can then determine whether the other control centers under 1500MW should fall into the medium or low impact category. (5) Regarding CIP-002-5, on page 19 of 33, criteria 3.2 and 3.3 should have the qualifier of “not otherwise classified as high or medium” as criteria 3.1 has. Blackstart units or cranking path substations could have met other High or Medium impact criteria and this appears to mandate that they be classified as Low impact. The facility definition should cover this occurrence. (6) The varying language regarding destroyed, degraded, or otherwise rendered unavailable and its variations found on pgs. 6, 8, 18(twice), 20 and 30 needs to be consistent. (7) Page 18, criteria 2.7 should be limited to NUC-001-2 R9.2.2 to scope the applicability of the requirements. Additionally, on pg. 19 Southern suggests adding "from Blackstart Resources to restoration unit switchyards" after "Cranking Path" in criteria 3.3 to provide additional clarity. (8) Regarding CIP-002-5, Southern suggests the following proposed solution to the auditing/evidence issues of Low Impact BES Cyber Systems. Southern suggests defining a new term “BES Site” to reduce the confusion regarding the already defined terms "Facility" and "System" in the NERC glossary that do not fit the concept these standards seem to address. "BES Sites” would be defined so that it refers to individual generation plants, dams, and renewable farms, transmission substations, and control centers; those classes of sites that we traditionally think of when applying the CIP standards. As a result, CIP-002 R1 can be rephrased with language similar to the following: “1.1 Identify the High Impact BES Sites that meet the criteria specified in CIP- 002-5, Attachment 1 – Impact Rating Criteria Parts 1.1 to 1.4 1.2 Identify the Medium Impact BES Sites that meet the criteria specified in CIP-002-5, Attachment 1 – Impact Rating Criteria Parts 2.1 to 2.11; 1.3 BES Sites which are not identified as High Impact or Medium Impact shall be identified as Low Impact BES Sites; 1.4 Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the High Impact BES Sites identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; 1.5 Identify each Medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Medium Impact BES Sites identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;” For Low Impact BES Sites, this would require the entity to maintain inventories at the "site" level (a list of all BES substations and <1500MW plants for example) and not the cyber device level. We could then propose to change the single low impact requirement in CIP-003 R2 to: “R2. The Responsible Entity shall implement one or more documented cyber security policies for each BES Site that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] . 2.1 Cyber security awareness; . 2.2 Physical access control; . 2.3 Electronic access control; and . 2.4 Incident response to a BES Cyber Security Incident.” This would allow for all BES Cyber Systems at all BES Sites to be implicitly covered by this one requirement. High and Medium Impact BES Cyber Systems would also be covered by the more detailed policy requirement (R1) and the remainder of CIP-003 to CIP-011. Accordingly, the evidence of implementation of the policy for Low Impact BES Sites would bes at a site level and not at an individual cyber asset level.

Yes
Yes
No
Yes
Yes
Yes
(1) Regarding CIP-003-5, Southern supports EEI expressed concerns about any language that would require responsible entities to demonstrate delegation all the way down to the equipment level. Delegation requirements for device level activities would be overly burdensome, would be a significant increase in required documentation, and offers no improvement to actual security or reliability. (2) Regarding CIP-003-5, R1.3, Southern suggests removing R1.3 concerning Interactive Remote Access as a discrete item. All the other subrequirements align with a CIP standard and this should be covered as part of R1.2. Southern views R1.3 as a subset of R1.2 which already covers remote access. (3) Regarding CIP-003-5, R2, Southern suggests the SDT consider the proposed “BES Site” concept proposed above and revising the language towards a defined Low Impact BES Site rather than a description based on what things are not as the current language reflects. (4) Regarding CIP-003-5, R3, Southern suggests allowing for the CIP Senior Manager to be designated by role or title rather than by the individual's name. (5) Regarding CIP-003-5, R4, Southern suggests clarifying that for other than R4, all other required activities of the NERC CIP Senior Manager may be delegated.
Group
MRO NSRF
Will Smith
No
Yes
1] The proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. The impact rating should align with the facility (BES Site) instead of the cyber asset. [R1 Proposed Flow] 1.1-Based on the definition for a BES Site, each entity should create a list of BES Sites. This step will determine for the entity, which sites have zero BES impact vs.which sites have an impact and will be later divided into high, medium, and low. The criteria for BES Site can also be considered the positive definition or threshold for Low Sites. These are sites that, based on the definition, will have some impact and require, at a minimum, programmatic protection at the Site level. There will be no need to identify the cyber assets associated with sites that have zero impact or those that remain in the Low category. All Sites will have the protections afforded the Low sites, but for those meeting the Medium and High criteria, additional protections are required, as well as the enumeration and classification of the cyber assets critical to providing the BES functionality of the location. After identifying the BES Sites, the Medium and High criteria must be considered for each Site. The following is a proposed flow for which the order can be modified while maintaining efficacy. 1.2- Based on the candidate list for sites with BES impact created from the execution of the first step, identify the High impact sites using the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the High Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (A) or without (B)External Routable Connectivity, those cyber assets used for Electronic (C) or Physical Access (D) Control or Monitoring, and those cyber assets connected within the same ESP (E) as the cyber assets necessary for the performance of the reliability function. 1.3 – Based on the sites that remain on the candidate list and are not High impact, determine the medium sites based on the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the Medium Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (F) or without (G)External Routable Connectivity, those cyber assets used for Electronic (H) or Physical Access (I) Control or Monitoring, and those cyber assets connected within the same ESP (J) as the cyber assets necessary for the performance of the reliability function. Note: There are 10 types of cyber assets positively identified through this process, each with varying levels of risk to the BES if compromised or rendered unavailable. This, potentially, creates more than 10 levels of protection to be enumerated throughout the rest of CIP-003 through CIP-011. For administrative ease, the MRO NSRF recommends grouping these types of cyber assets based on their actual level of risk in each scenario involving a potential

incident that is either cyber or physical in nature and based on the External Routable Connectivity. The rest of the Standards should be written to address each type or grouping of asset. Silence on any one type or grouping will lead to confusion regarding the necessary protective measures and commensurate improvement to security posture. 1.4 – Everything that made the initial candidate list requires protection of some sort, so if it didn't get picked for High or Medium, it gets assessed at Low, because it met the threshold criteria in the BES Site definition. Verbiage in the definitions and the requirements should support this process flow, which will allow the enumeration of High Sites, Medium Sites, and Lows Sites (since we all know a list is required to demonstrate even programmatic elements of CIP compliance). The lists of Cyber Assets will only be required at Medium and High Sites. If possible and feasible, the criteria for dividing the sites into those categories should be progressive in nature, allowing clear demarcation and rationale for the criteria chosen. Additionally, the rest of the Standards should address the requirements progressively for the asset types based on risk. The shift from the current draft to one with obvious progression throughout the CIP-002 methodology and again throughout the rest of the Standards will allow for ease of application at each entity. The current draft does not provide the entities with clear understanding of the order and rationale for identifying the scope of applicability for the CIP Standards, and the MRO NSRF feels that the entities can't be successful with the current format. [2] Change the CIP-002 VSLS to reflect "BES Sites" instead of "Facilities" as those would be the enumerated list. In its current state, it conflicts with the statement that low and zero impact sites do not require enumeration. [3] All VSLs should change the impact designation from cyber asset based to site-based. "High," "Medium," or "Low" designations should precede the word "Site" not "BES Cyber Asset" or "BES Cyber System." Please give consideration to the following suggestions: For Criterion 2.5 – Replace the latest revised wording with the following more accurate and precise wording of, "Transmission Facilities operated between 200 kV and 499 kV that are located at a single station or substation, which is connected to three or more other station or substations by lines operated between 200 kV and 499 kV and which possess an "aggregate weighted value" exceeding 3000. The "aggregated weighted value" of the station or substation is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line that is connected to another Transmission station or substation." This proposed wording properly associates the aggregated weighted value with a station or substation, not a Facility (e.g. BES line, transformer, or generator element). The proposed wording also qualifies that the applicable Facilities are the ones at the qualifying station or substations. In the case of an applicable transmission line, the criteria is only the portion of the line's Facilities at qualifying substation, not the portion of the line's Facilities at the other substation, unless the station or substation at the other end of the line also meets the aggregated weight value threshold. For Criterion 2.6 – Replace the unclear 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', which would be consistent with wording used in Criterion 2.8 and 2.9. The Facilities that could cause an IROL to be violated are usually different from the Facilities that IROL was developed to assure would not cause an unacceptable impact on the reliability of the BES when they are lost. For Criteria 2.11; Note that a BA or TOP may only provide a very small number of individual functions as described within the Functional Model based on the amount of CFRs and JROs that NERC has accepted. Every BA and TOP does not have the same impact on the BES as a larger BA or TOP. As written, 2.11 will require every BA and TOP that is registered as such as being in the "medium" category. This one size fits all approach does not work. Another concern with criteria 2.11 is that a TOP registered as a TOP does not "control" any "real power". As stated in FERC Order 706, paragraph 253, FERC clearly speaks of being flexible "However, we are persuaded by commenter's that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity." Recommend that BA's be viewed as in Attachment 1, CIP-002-4 brightline criteria 1.17.
Yes
No
Yes
Yes
Yes
Yes
(1) [Proposed Verbiage] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more

documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is. (2) [Proposed Verbiage] CIP-003 R2. For BES Sites identified as low impact, each Responsible Entity shall provide guidance with one or more documented cyber security policies that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] The programmatic elements identified in the sub-requirements may remain, as is. (3) VSLs should reflect the actual risk to the BES when one or more elements are missing. The absence of a program should be high or severe, but the lack of discrete components should start at Low. Please note that the above changes apply to structure and not content of what the SDT is intending to accomplish.
Individual
Steve Karolek
Wisconsin Electric Power Company
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms. (2) Enhancing the CIP process flow on page 33 to indicate that the assets inherit the impact of the Facility, there may be greater industry approval. As it currently exists, the process flow has as its first box the identification of BES Cyber Assets and BES Cyber systems. This first box should capture the identification of Facilities that satisfy the impact criterion. This process flow should be enhanced, and possibly moved to the requirements section to provide a prescriptive methodology to ensure this "Facilities first" approach provides clear directives to the industry. (3) We feel the wording of requirement 1 with respect to planned in service time of 6 months introduces additional documentation requirements of what is planned and additional requirements to ensure the plans are followed. These additional requirements do nothing to enhance the reliability of the BES.
Yes
No
Yes
No
No
Yes
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms. (2) We are concerned about the level of delegation which needs to be specifically delegated by the CIP Senior Manager. This should be limited to high-level delegations of responsibility. Specific assignment of duties at the "worker" level is best done by supervisors and managers of the related processes. (3) Wisconsin Electric recognizes that not all BES Facilities have a "high" or "medium" impact on the BES and that there may be Cyber Assets and/or Cyber Systems located at those facilities. However Wisconsin Electric believes that the industry does not at this time have consensus on how to identify, classify and secure those Cyber Assets and Cyber Systems. In the interest of moving this version of the standard forward, we believe that all requirements not applicable to those Cyber Assets and Cyber Systems essential to the functional obligations performed at "high" or "medium" impact BES Facilities be removed from the standards and dealt with in a future version. (4) Guidance for physical security includes the phrase "and egress". Since the requirements for exit readers have been removed with this draft, the wording with respect to egress should also be removed.
Group
Western Area Power Administration
Brandy A. Dunn
No
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 “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. c) Attachment 1, 2.5: The discussion in the Application Guidelines under transmission part 2.5 (page 29): 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. d) Attachment 1, 2.9: 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. e) Attachment 1, 2.10: 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 should not be necessary to declare each of the relays and therefore each substation as medium assets.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Ralph Meyer
The Empire District Electric Company
No
Yes
We need a clear definition of dial-up to eliminate the confusion of what dial-up includes and what it does not include; for example leased lines to modem banks should not be included. Without a clear definition auditors could interpret devices that are used for point-to-point communication over leased lines as dial-up and include these devices as dial-up assets under the CIP standards.4. Need clarity on which Transmission Owners’ control centers who are not Operators will be classified as High Impact. Attachment 1-Item 1.3 – uses the term “functional obligation”. This term is not defined. Also not clear is the meaning of –to control- an asset.
Yes
Yes
Yes
Yes

Yes
Yes
Low Impact BES Cyber Systems: EDE propose removing BES Cyber Systems used within Low Impact facilities from the current draft 2 standards to provide consistent standards at a later date. This will ensure BES Cyber Systems used within High and Medium Impact facilities will achieve the benefit of the enhanced standard unimpeded from Low Impact concerns. R5 : What is meant by the words “specific actions”? This is not in the definitions and we suggest striking the words “specific actions” as it is too subjective to audit. There is a clerical error in the Introduction, section 4.2.4 where it provides exemptions from CIP-002-5. This would seem to reference exemptions from CIP-003-5. R2 VSL:b. Given the R2 requirement for BES Cyber Systems used within Low Impact facilities, the VSL should be shifted to the left to use Lower/Moderate VSLs. Per the subjects covered within CIP-003, there are no direct impacts on BES reliability should a policy clerical error occur or Senior Manager designation not be captured adequately.
Individual
Daniel Duff
Liberty Electric Power LLC
Yes
Yes
2.11 generation control centers (with) 300 Mw of Real Power. No technical basis for choosing 300 Mw. No indication as to why a facility which serves as a control room for 350 Mw from units at remote locations would have a greater impact on BES than a 1000 Mw facility at a single location.
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Please give consideration to the following suggestions: For Criterion 2.5 – Replace the latest revised wording with the following more accurate and precise wording of, “Transmission Facilities operated between 200 kV and 499 kV that are located at a single station or substation, which is connected to three or more other station or substations by lines operated between 200 kV and 499 kV and which possess an “aggregate weighted value” exceeding 3000. The “aggregated weighted value” of the station or substation is determined by summing the “weight value per line” shown in the table below for each BES Transmission Line that is connected to another Transmission station or substation.” This proposed wording properly associates the aggregated weighted value with a station or substation, not a Facility (e.g. BES line, transformer, or generator element). The proposed wording also qualifies that the applicable Facilities are the ones at the qualifying station or substations. In the case of an applicable transmission line, the criteria is only the portion of the line’s Facilities at qualifying substation, not the portion of the line’s Facilities at the other substation, unless the station or substation at the other end of the line also meets the aggregated weight value threshold. For Criterion 2.6 – Replace the unclear 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’, which would be consistent with wording used in Criterion 2.8 and 2.9. The Facilities that could cause an IROL to be violated are usually different from the Facilities that IROL was developed to assure would not cause an unacceptable impact on the reliability of the BES when they are lost.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form A.
Group

Edison Electric Institute
David Batz
(1.)Change time frame in all affected standards to read 'once each calendar year OR a period not to exceed 15 calendar months '. The affected standards are CIP-004 R3.2, R6.6, R6.7; CIP-007 R5.6; CIP-008 R2.1, R3.1; CIP-009 R2.1, 2.2; CIP-010 R3.1; and CIP-011 R1.3. (2.)Rather than the current approach to identify 'Facilities, Systems, and equipment,' modify this to identify High Impact Sites, Medium Impact Sites with all BES Sites not identified as High Impact or Medium Impact being identified as Low Impact. For Low Impact, maintaining inventories at the site level would avoid the concern that discrete equipment identification is required. (3.) We need a clear definition of dial-up to eliminate the confusion of what dial-up includes and what it does not include; for example leased lines to modem banks should not be included. Without a clear definition auditors could interpret devices that are used for point-to-point communication over leased lines as dial-up and include these devices as dial-up assets under the CIP standards.; (4.)Need clarity on which Transmission Owners' control centers who are not Operators will be classified as High Impact. Attachment 1-Item 1.3 - uses the term 'functional obligation'. This term is not defined. Also not clear is the meaning of -to control- an asset. The example to demonstrate the confusion is a Transmission Owner Control Center that can remote open/close breakers but only under the direction of the Transmission Operator. The Transmission Owner does not have the functional obligation of the Transmission Operator and the Transmission Operator has the Operating Authority over the breakers. Suggest that clarity in 1.3 can be obtained by restating as: perform the functional obligations of the Transmission Operator for the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.1., and adding to the technical guidance clarification that a Cyber System that can remote operate assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10 where the Entity is not performing the functional obligation of a Transmission Operator are Medium impact. This comment also applies to Attachment 1 - Item 2.11.
(1.)Low Impact BES Cyber Systems a. The current wording reflects an attempt by the CIP SDT to provide 'protection' from discrete identification of low impact BES cyber systems, yet the requirements are (still) framed in a way that would require discrete identification to adequately demonstrate compliance. This provides conflicting messages that would impede approval of protection controls for BES Cyber Systems used within High and Medium Impact facilities. (2.) Throughout the standard, references to Low/Medium/High Impact should be applied to facilities and not BES Cyber Systems. Per CIP-002 Attachment A, it is the facilities which determine the Impact and not the BES Cyber System. Rather than the existing R1 language 'Each Responsible Entity for its high impact and medium impact BES Cyber Systems,' use 'Each Responsible Entity for its BES Cyber Systems used in high impact and medium impact facilities.' This will clarify the facility first approach. (3.) There is a clerical error in the Introduction, section 4.2.4 where it provides exemptions from CIP- 002-5. This would seem to reference exemptions from CIP-003-5. (4.) R2 a. Original language - For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: b. Proposed change - For BES Cyber Systems used in facilities not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: c. Rationale: The shift of impact ratings to facilities supports the process in which facilities determine impact. (5.) R2 VSL a. The Table of Compliance Elements references a Medium VRF whereas the requirement identifies a Low VRF. b. Given the R2 requirement for BES Cyber Systems used within Low Impact facilities, the VSL should be shifted to the left to use Lower/Moderate VSLs. Per the subjects covered within CIP-003, there are no direct impacts on BES reliability should a policy clerical error occur or Senior Manager designation not be captured adequately. (6.) R3 - The R6 content applicable to R3, requiring the documenting of changes to the Senior Manager within 30 days, should be included within R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation of a single requirement. (7.)R4 - VSLs a. Propose framing review violations as lower/medium VSLs as follows: i. Lower - Policies have not been reviewed within 30 days of annual review time periods ii. Medium - Policies have not been reviewed within 60 days of annual review time periods b. For Policy approval: iii. High - Policy has not been approved within 30 days of annual approval timelines iv. Severe - Policy has not been approved within 60 days of annual approval timelines c. Rationale - There is a difference between approved policy and review of policies. The current approach repeats the violation in which 'not all policies have been approved within the required time period,' which creates confusion. By recognizing the difference in importance (approve vs. review) and framing review violations as less

severe, this provides a more relevant scale. (8.) R5 a. The R6 content applicable to R5, requiring the documenting of changes to delegations within 30 days, should be included within R5. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation in the violation of a single requirement. b. What is meant by the words 'specific actions'? We suggest striking the words 'specific actions' as it is too subjective to audit. (9.) R6 - Propose removal once recommended changes to R3 and R5 are enacted. This requirement simply identifies time constraints to document changes to R3 and R5 requirements. Any violation of this requirement would also result in the violation of R3 or R5 and introduces 'double jeopardy' concerns. (10.) Remove 'egress' from Guidelines 1.4

Individual

Kirit Shah

Ameren

No

Yes

(1)We appreciate the effort and detail that the SDT went through to develop this draft revision 5 to standard CIP-002. However, we believe the SDT has not provided clarity to the language of the proposed requirements, and has combined Facilities, Cyber Systems, and associated Cyber Assets such that it is confusing. We proposed that SDT start by developing a flowchart of the identification process, and the requirements, they should be pulled from the flowchart. Please notice that on page 33 of the Application Guideline there is a process flow chart, but also note that it does not start with a Facility and we feel this needs to be revised to add clarity and details. We feel that this flow chart should be part of the standard. Further, R1 and its sub-requirements should strictly address the identification of Facilities that impact the reliability of the BES. R2 and its sub-requirements should address the identification of BES Cyber Assets, and R3 and its sub-requirements should address the identification of BES Cyber Systems. The existing R2 approval of the facility identification should then become R4. (2)We recommend that Facilities are the first place to begin with when identifying cyber assets, because that is where Impact to the BES originates, even though there are questions about how we define various facilities; RTU's and substations. Then it will be clear that we are addressing BES Cyber Systems which are used in High, Medium or Low Impact Facilities. Attachment 1 should be retitled Facility Rating Criteria. Item 1, High Impact Rating (H) should be changed to High Impact Facilities (H) as it applies to BES Facilities and not to BES Cyber Systems. Item 2, Medium Impact Rating (M) should be changed to Medium Impact Facilities (M) BES Facilities and not to BES Cyber Systems. Item 3, Low Impact Rating (L) should be changed to Low Impact Facilities (L). If requirements are developed for Low Impact Facilities, they should be included as a separate standard. (3) No definition for "Adverse Impact of the reliable operations of the BES" is included in the standard or the application guidelines. In this regard, we suggest SDT to provide the definition of "Adverse Impact of the reliable operations of the BES" included on page 8 in the section on Real Time Operations, and also clarify is it the Impact on the BES or Impact on a Facility. Also note that definition of BES Cyber Asset (in the definition document) does not include the word "adverse" related to reliable operation of the BES. Suggest consistency or using NERC Glossary term "Adverse Reliability Impact" (pg 4 of the NERC glossary) definition to define/replace "Adverse Impact of the reliable operations of the BES". Definition of Adverse Reliability Impact is "The impact of an event that results in Bulk Electric System instability or Cascading." (4) The "15 minute time frame" included in the definition of BES Cyber Assets is problematic to provide evidence during the compliance audit. We suggest adding some guidance to the CIP-002-5 standard to help understand what type of evidence would suffice or identify some examples of BES Cyber Assets that would create an Adverse Reliability Impact within 15 minutes. (5) We ask that the SDT clarify their intention on page 8 under “Reliable Operation of the BES. The second sentence states “BES Cyber System perform or support any BES reliability function according to those reliability tasks identified for Functional entities in the NERC Function Model.” Even with the guidelines attached to CIP-002-5, we read this statement to mean all BES reliability function must be cross referenced against the system they use, and any system that may impact one of these functions in any way, must have security protections. (6) R1.3 states “low impact does not require discrete identification,” and Attachment 1 shows a list of Low assets requiring protection. These statements are all contradictory with R1.4 that states entities must track changes in the impact categorization from a lower to higher impact category to update the BES Cyber Asset list. The current wording is such that it will require discrete identification of low Impact Cyber Assets to adequately demonstrate compliance and this is a conflicting message that would impede approval. We

would propose to the SDT removing BES Cyber Systems used within Low Impact Facilities from the current draft 2 standards. If the drafting team must keep the Low Impact Facilities in scope, an entity should only be required to keep a list of facilities and not the cyber asset list. (7) The format of the draft standard is completely different from the other NERC reliability standards; for example, the background section in CIP-002-5 is included prior to the requirements and then application guidelines follow at the end. If the background and application guidelines are to be retained, we suggest both to be included at the end of the standard.
No
No
No
No
No
No
(1) R1 – Proposed word change for the requirement - “Each Responsible Entity for its high impact and medium impact BES Cyber Systems,” should be changed to “Each Responsible Entity for its BES Cyber Systems used in High Impact and Medium Impact Facilities.” This will clarify the Facility first approach. (2) R2 – Proposed word change for the requirement – "For BES Cyber Systems used in Facilities not identified as High Impact or Medium Impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics". The shift of impact ratings to Facilities supports that it is the Facilities which determines the impact. (3) R2 VSL - The VSL should be shifted to the left to use Lower/Moderate VSLs. Also note that the Table of Compliance Elements references a Medium VRF whereas the requirement identifies a Low VRF. (4) R3 – Need to add applicable content from R6 to R3 requirement, language should be added requiring the documenting of changes to the Senior Manager within 30 days, within R3. This will eliminate ‘double jeopardy’ concerns where failure to adequately document changes will only result in the violation of a single requirement. (5) R4 – Need to remove the words "and R2" from the requirement. This will eliminate the security policies for Low Impact BES Cyber Systems having to be signed by the Senior Manger each calendar year. We would suggest that these r policies for Lower Impact can be signed by a delegate instead of the Senior Manager. (6) R4 – We suggest the following changes for the R4 VSLs: Rationale – There is a difference between approving the policies and review of policies as written this repeats the violation in which ‘not all policies have been approved within the required time period,’ which creates confusion. (a) Lower – Policies have not been reviewed within 30 days of annual review time periods. (b) Medium – Policies have not been reviewed within 60 days of annual review time periods. (c) High – Policy has not been approved within 30 days of annual approval timelines. (7) R5 – Need to add applicable content from R6 to R5 requirement, requiring the documenting of changes to delegations within 30 days, should be included within R5. This will eliminate ‘double jeopardy’ concerns where failure to adequately document changes will only result in the violation of a single requirement. Also define and clarify the phrase “where allowed by the CIP Standards”. (8) R6 – We recommend that SDT remove this requirement, it simply identifies time constraints to document changes to R3 and R5 requirements as stated in our comment for R3 and R5 above. Not removing this requirement introduces ‘double jeopardy’ concerns. If requirement R6 must stay need to replace the word "delegator" with "Senior Manger" to help clarify this requirement.
Group
Salt River Project
Sara McCoy
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Individual
Michael Lombardi
Northeast Utilities
Yes
Yes
Attachment 1, Section 2.5 - We agree with the Drafting Team that the use of “aggregate weighted values” provides an objective approach for determining the potential impact level used for categorizing BES Cyber Assets. However, we also believe that due to variations between electrical systems that “one size does not fit all” and a mechanism should be in place to allow the asset owners to refine the impact level using studies and risk base analysis. Attachment 1, Section 2.6 - refers to facilities “that are identified by its Reliability Coordinator, Planning Coordinator or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.” Please clarify under which reliability requirement the Reliability Coordinator (RC), Planning Coordinator (PC) and Transmission Planner (TP) is required to inform each of the “Responsible Entities” associated with CIP-002-5. Without a notification requirement for the RC, PC and TP, the Responsible Entities are at risk of not complying with this standard. Attachment 1, Section 2.11 - Control Center is not a NERC defined term. Please clarify that Control Center used in this context refers to Regional (RTO/ISO) and Local (LCC) control centers and not the main control room of generating stations/units. Consider organizing the “Guidelines and Technical Basis” by subject (e.g., Transmission, Generation, etc.)
Yes
Yes
Yes
Yes
Yes
Yes
R1 and R2 - Recommend that a cross reference associated with each of the listed topics is provided. For example, revise 1.1 Personnel Security to read 1.1 Personnel Security (CIP-004) R5 - the first sentence of the rationale for R5 states: “The intent of the requirement is to ensure clear accountability within an organization for certain security matters.” It is not clear what is meant by “certain security matters.” Recommend that clarification be provided regarding what the limitations are concerning the delegation of authority by the CIP Manager.
Group
Florida Municipal Power Agency
Frank Gaffney
No
No
FMPA has comments for both Question 1 and Question 2. However, those questions no longer have a comments box in which to insert them. After speaking with Steven Noess at NERC, I was told that I could insert them here. (1) Question 1: First, FMPA wishes to thank the SDT for all of their hard work and a significantly better product than earlier versions. However, there are a few issues that cause us to vote negative as described in these comments. Requirement R1 is silent on what relationship to an asset or cyber system causes an entity to be responsible for that asset or cyber system which creates many opportunities for double jeopardy. For instance, is the owner or operator responsible? Is the outsourcer or outsource responsible? As written, if the GO and GOP, or TO and TOP are different entities, it would seem that both are responsible for the same thing creating conflict and double jeopardy, and in some ways decreasing security due to this ambiguity of authority. Due to the many types of different business arrangements that exist and the fact that we shouldn’t care who is responsible as long as one registered entity takes responsibility, FMPA suggests adding a statement something like: “If an asset or cyber system is used by more than one entity, the entities may decide amongst themselves which entity will take full responsibility for the standards for that asset or cyber system”. The sub-bullets of R1 use the term “Systems” which is defined in the NERC Glossary as including distribution, i.e., “A combination of generation, transmission, and distribution components”.

Distribution is specifically excluded from the standards through the Federal Power Act, Section 215, at (a)(1) and (i)(1). FMPA believes the SDT intends this phrase to only apply to UFLS and UVLS. As such, the term “Systems” should be eliminated since the term “equipment” is sufficient. Although we are appreciative of the efforts to minimize impacts on microprocessor based UFLS and UVLS relays, we are still very concerned of the broad reaching consequences of application of the standards to every microprocessor based relay whether or not that relay has connectivity via routable protocol. In the last round of comments, FMPA proposed the addition of a De Minimus Impact category, which the SDT interpreted narrowly as meaning only impact without a risk adjustment. While we understand that the impact of a relay is the same whether connected via routable protocol or not, we also recognize that the risk of malicious activity is significantly higher for relays connected via routable protocol. Hence, we amend our recommendation to create a De Minimus Risk category for which the standards would not be applicable for BES Cyber Assets that would fall within the Low Impact category but are not connected by routable protocol. Such a step would significantly reduce the administrative burden of the standards at little to no risk to reliability. (2) Question 2 comments: R2 has become redundant as a result of R1 bullet 1.4. The only purpose of an annual review is for change management, which is now covered by R1 bullet 1.4. Having a senior manager approve is simply an internal control not worthy of a requirement. FMPA proposes deleting R2, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report (FFTR).
Yes
No
No
No
No
No
FMPA has comments for both Question 4 through Question 9. However, those questions no longer have a comments box in which to insert them. After speaking with Steven Noess at NERC, I was told that I could insert them here. (1) Question 5: The word “implement” is problematic for Low Impact assets. The definitions of “implement” is “carry out, accomplish; especially: to give practical effect to and ensure of actual fulfillment by concrete measures”. Using such a definition means that for Low Impact assets, detailed end result measures of implementation would be needed to prove compliance with the requirement, including system by system information regarding access controls, granting access, denying access, etc., (otherwise, how would an entity prove that a electronic access policy was implemented?) which does not meet the intent of the SDT to remain at a “programmatic” level for Low Impact system. FMPA suggest using the phrase “in force”, e.g., “For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall have one or more documented cyber security policies in force that address the following topics.” Rewording the requirement in this way would mean that the only evidence needed is the policy itself, and not additional proof that the policy was implemented. (2) Question 6: R3 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement. (3) Question 7: R4 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement. (4) Question 8: R5 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement. (5) Question 9: R6 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the requirement.
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. 1. R1.4. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program as is appropriate for that entity. Thus, NextEra disagrees with the implementation of an arbitrary deadline, and, therefore, that

R1.4 be revised to read as follows: “Review, keep current and update, at a timeframe that the Responsible Entity deems necessary, the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. “ 2. R2. As a preferred alternative to that suggested by EEI, NextEra does not agree that a CIP Senior Manager is necessary to implement a robust, current and updated CIP compliance program. Thus, NextEra requests that the concept of a CIP Senior Manager be deleted from all CIP Reliability Standards. For support, NextEra notes that there is no evidence that without a CIP Senior Manager there is any additional risk to the BES. Further, the unnecessary focus on title of an employee and the duties of an employee is not only micromanaging a Responsibility Entity, but also takes away essential flexibility from an entity to design a CIP compliance program that best promotes cyber security. NextEra further believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2 be revised to read as follows: “ The Responsible Entity shall approve the identifications required by Requirement R1 as the Entity deems necessary.” 3. As a preferred alternative to that suggested by EEI, with respect to CIP-002-5 Attachment 1, Section 2 (Medium Impact Rating), NextEra is concerned that the draft language in Section 2.1 (and elsewhere) does not appropriately take into consideration the significant operational differences between wind and solar generation (intermittent resources) as compared to fossil generation. Wind and solar units, because of their intermittent nature, do not pose the same cyber security threat to the grid as traditional fossil units. NextEra therefore requests that drafting team adopt rating criteria for Attachment 1 that differentiates between intermittent resources and fossil resources and does not automatically result in a Medium Impact Rating for wind and solar units unless a Transmission Operator, Reliability Coordinator, Planning Coordinator, or Transmission Planner has in writing specifically identified the wind or solar unit as critical to reliability. In other words, NextEra requests that the Low Impact Rating be adopted as the default category for wind and solar units that are part of the Bulk Electric System. 4. As a preferred alternative to that suggested by EEI, NextEra also supports Mid-American's proposals on CIP-002-5 and in particular adding language as follows: Each Responsible Entity shall implement R1; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws in the application of the criteria set forth in R1.1 through R1.5 do not constitute per se violations of R1 NextEra also prefers the following language that provides for 15 months be used for the annual review processes in CIP-00-5: “The Responsible Entity shall update these lists as necessary, and review the list(s) at least once each calendar year or not to exceed 15 months between reviews.”
No
No
No
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. R3-R6. As a preferred alternative to that suggested by EEI, NextEra does not agree that a CIP Senior Manager is necessary to implement a robust, current and updated CIP compliance program. Thus, as noted above, NextEra requests that the concept of a CIP Senior Manager be deleted from all CIP Reliability Standards. The unnecessary focus on title of an employee and the duties of an employee is not only micromanaging responsible entities, but also takes away essential flexibility from an entity to design a CIP compliance program that best promotes cyber security. Therefore, NextEra requests the deletion of R3, R5, and R6. NextEra further believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R4 be revised to read as follows: “Each Responsible Entity shall review and update cyber security policies identified in Requirements R1 and R2, at a timeframe that the Entity deems necessary.”
Group
Madison Gas and Electric Company
Joseph DePoorter

No
Yes
Please see the MRO NSRF Comments. MGE has the following addition comments concerning CIP-002-5: For Criteria 2.11; A BA or TOP may only provide a very small number of individual functions as described within the Functional Model (and within the Application Guidelines) based on the CFR or JRO that they have filed at NERC. Every BA and TOP does not have the same impact on the BES as a larger BA or TOP. As written, 2.11 will require every BA and TOP that is registered as such as being in the "medium" category. This one size fits all approach does capture the entities that have an impact on the BES. The SDT uses a threshold of "300 MW or more of BES generation" based on a 300 MW limit of UFLS and UVLS within the Application Guide. Within a UFLS or UVLS system, the control is "instantaneous" where a BA that is responsible for 300 MW or more of BES generation can only "control" the generation. Recommend the words "controllable in real time" be added. This will take into consideration the ownership of joint generation units that BA's may share. Recommend the second sentence of 2.11 to read; "… of the preceding 12 calendar equal to or exceeding the controllable in real time amount of 300 MW or more BES generation". This slight change will support FERC Order 706, paragraph 253, FERC clearly speaks of being flexible "However, we are persuaded by commenter's that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity." The SDT may wish to maintain what is presently approved that BA's be viewed as in Attachment 1, CIP-002-4 brightline criteria 1.17 concerning a BA control center "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". This is presently FERC approved where the 300 MW threshold is only based on UFLS or UVLS thresholds (and has no firm basis). The 1500 MW comment is based on criteria 2.1 of version 5. Where the generation threshold of 1500 MW is used to assure that generation is captured as a medium impact. This provides a consistent approach that a generator within a BA area with the 1500 MW threshold and the BA are assigned the same level of impact to the BES. Another concern with criteria 2.11 is that a TOP registered as a TOP does not "control" any "real power".
Yes
No
Yes
Yes
Yes
Yes
Please see the MRO NSRF Comments.
Group
Pepco Holdings Inc & Affiliates
David Thorne
Yes
Yes
1)2.7 of Attachment 1 Does not take into consideration Facilities not identified as "Transmission" i.e. Sub-Transmission or Distribution facilities that are essential to meeting NPIR's. This requirement is presumptive to being high voltage BES components only. 2)Shouldn't a facility be considered essential if it is required by a Nuclear Plant License/NRC regardless of the voltage of the service. 3)Section 3.3 of Att. 1, What is the point to identify "Low Impact Cyber Systems" but have no discrete identification requirements of the resource. Could this result in a null list? 4) Does R2 this supersede an entities definition of Annual?
Yes
No
Yes
Yes
Yes
Yes
1) O5 - R2--If discrete identification is not required then enforcement becomes ambiguous. 2) O4--R4

--Yes, but does this supersede an entities definition of annual if so then it must be made clear 15 months is an absolute value from the prior review. Also if an additional 3 mo. is granted can the review be made 3 mo. prior to its due date and be considered valid? If so the review should be performed each calendar year on the anniversary + or – 3 months.
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying “that are part of a Load shedding program” implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW “program” and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. NRECA recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. Under the inclusion threshold for DP, 4.2.2, third bullet, states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” NRECA recommends that the following language be added to the end of that bullet; “, and where the Protection System is connected to a supervisory control system providing remote operation capability.” This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. Attachment 1 2.10 – see comment above 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for NRECA. It will be difficult to support CIP-002-5 without this revision.
No
R2 – NRECA is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, NRECA requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance.
Individual
Christina Conway
Oncor Electric Delivery Company LLC
No
Yes
GENERAL CIP-002-5 COMMENTS: (1) The Background section or Application Guidelines of CIP-002-5 should provide more discussion and detailed examples of the “BES Cyber System” concept. Multiple examples should be provided to address typical varying Responsible Entity configurations. This will aide in explaining the new “BES Cyber System” concept to the Responsible Entities. If there is a better understanding of the concept and how it applies to various facilities/assets, then Responsible Entities will be more likely to support the standards. (2) A high level summary of the CIP version 5 standards that shows the interaction between each standard, applicability type, and definition should be provided with the next draft. This will help resolve any remaining inconsistencies and overlaps between standards prior to the next draft. (3) Oncor supports the comments submitted by EEI in response to this question. ATTACHMENT 1 AND R1 REQUIREMENT COMMENTS: Oncor supports the proposed solution developed by the Midwest Reliability Organization NERC Standard Review Forum to clarify the flow for identifying BES Cyber Systems. Draft 2 of CIP-002-5 Requirement 1 appropriately reflects an attempt to provide ‘protection’ from forcing Registered Entities to discretely identify BES Cyber Systems used at Low Impact Facilities. Unfortunately, the language in this requirement is inconsistent with CIP-003-5 Requirement 2, which requires a Registered Entity to implement one or more documented cyber security policies for “BES Cyber Systems not identified as high impact or medium impact.” To demonstrate that it has implemented the required cyber security policies for “BES Cyber Systems not identified as high impact or medium impact,” a Registered Entity would likely

be forced to develop a list of low impact BES Cyber Systems. This is a significant point of concern given the resources, processes, time, and documentation that would be required to ensure the ability to demonstrate compliance for low impact BES Cyber Systems.
Yes
No
No
Yes
No
No
R2 REQUIREMENT COMMENTS: Oncor supports the proposed solution developed by the Midwest Reliability Organization NERC Standard Review Forum to clarify the flow for identifying BES Cyber Systems. Draft 2 of CIP-002-5 Requirement 1 appropriately reflects an attempt to provide 'protection' from forcing Registered Entities to discretely identify BES Cyber Systems used at Low Impact Facilities. Unfortunately, the language in this requirement is inconsistent with CIP-003-5 Requirement 2, which requires a Registered Entity to implement one or more documented cyber security policies for "BES Cyber Systems not identified as high impact or medium impact." To demonstrate that it has implemented the required cyber security policies for "BES Cyber Systems not identified as high impact or medium impact," a Registered Entity would likely be forced to develop a list of low impact BES Cyber Systems. This is a significant point of concern given the resources, processes, time, and documentation that would be required to ensure the ability to demonstrate compliance for low impact BES Cyber Systems. R3 REQUIREMENT COMMENTS: The CIP-003-5 R6 content that is applicable to CIP-003-5 R3, which requires the documentation of changes to the Senior Manager within 30 days, should be included within CIP-003-5 R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes could result in the violation of two requirements. R5 REQUIREMENT COMMENTS: The CIP-003-5 R6 content that is applicable to CIP-003-5 R5, which requires the documentation of changes to delegations within 30 days, should be included within CIP-003-5 R5. This will eliminate 'double jeopardy' concerns where failure to adequately document changes could result in the violation of two requirements. R6 REQUIREMENT COMMENTS: CIP-003-5 R6 should be removed after the recommended changes to CIP-003-5 R3 and CIP-003-5 R5 suggested above are adopted. This requirement simply identifies time constraints to document personnel changes in positions described in CIP-003-5 R3 and CIP-003-5 R5. Any violation of this requirement could also result in the violation of CIP-003-5 R3 or CIP-003-5 R5 and introduces 'double jeopardy' concerns. GENERAL COMMENT: Oncor supports the comments submitted by EEI in response to this question.
Individual
Gregory J. LeGrave
Wisconsin Public Service Corporation and Upper Pennisula Power Company
No
No
WPS and UPPCO support the comments submitted by EEI and the MRO NSRF. In addition WPS and UPPCO make the following comments: • The requirements on Low Impact Assets are too vague to assure consistent implementation and enforcement. Since the assets are self-described as having a low impact on the BES these requirements should be deleted. Barring deletion, the drafting team should better describe the requirements • The re-definition of annual is arbitrary and capricious and does not improve the safety, security, or reliability of the BES. • The definitions continue to be too complex and unclear. The drafting team needs to simplify and clarify the terms to assure consistent implementation and enforcement
No
No
No
No
No
No
WPS and UPPCO support the comments submitted by EEI and the MRO NSRF. In addition WPS and UPPCO make the following comments: • The requirements on Low Impact Assets are too vague to

assure consistent implementation and enforcement. Since the assets are self-described as having a low impact on the BES these requirements should be deleted. Barring deletion, the drafting team should better describe the requirements • The re-definition of annual is arbitrary and capricious and does not improve the safety, security, or reliability of the BES. • The definitions continue to be too complex and unclear. The drafting team needs to simplify and clarify the terms to assure consistent implementation and enforcement
Individual
Don Jones
Texas Reliability Entity
No
No
•Blackstart Units should not be discounted from the audit program. Blackstart Units should be rated at least at medium if not always high. •Items designated as low need to be documented. This covers the aspect of a whole, complete, and accurate evaluation. •The standard as drafted may dramatically affect the applicability of the CIP standards for a majority of GOPs which is not in the best interest of reliability. This is accomplished by the criteria included in Attachment 1 which requires a generation threshold of 1500 MW and the criteria language included in 2.3, 2.6 and 2.9. Was there any analysis or data on the effect that this would have on the applicability of CIPs for GOP CIP programs? The language appears to be worst case scenario from a planning perspective and seems to place an unreasonable high bar for the CIPs applicability to GOPs. In addition, what is the process or mechanism used to notify a GOP of such a designation from its PC or TP? •The VSLs for R1 include language stating, “For a Responsible Entities with more than a total of 40 facilities….” What is the significance of the quantity of 40 facilities and if a Responsible Entity has less than 40 facilities how would that impact the VSL analysis? Also, R1 includes Systems or equipment yet the VSLs make no mention. Is there a reason for the exclusions?
Yes
Yes
No
Yes
Yes
Yes
•The designated Senior Manager documentation should include title and documented responsibilities. •If R2 does not require an inventory list or discrete identification of the BES Cyber Systems (that have not been identified as high or medium impact) how would a CEA assess compliance with this requirement?
Individual
Don Schmit
Nebraska Public Power District
No
Yes
[1] The proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. The impact rating should align with the facility (BES Site) instead of the cyber asset. [R1 Proposed Flow] 1.1-Based on the definition for a BES Site, each entity should create a list of BES Sites. This step will determine for the entity, which sites have zero BES impact vs. which sites have an impact and will be later divided into high, medium, and low. The criteria for BES Site can also be considered the positive definition or threshold for Low Sites. These are sites that, based on the definition, will have some impact and require, at a minimum, programmatic protection at the Site level. There will be no need to identify the cyber assets associated with sites that have zero impact or those that remain in the Low category. All Sites will have the protections afforded the Low sites, but for those meeting the Medium and High criteria, additional protections are required, as well as the enumeration and classification of the cyber assets critical to providing the BES functionality of the location. After identifying the BES Sites, the Medium and High criteria must be considered for each Site. The following is a proposed flow for which the order can be modified while maintaining efficacy. 1.2- Based on the candidate list for sites with BES

impact created from the execution of the first step, identify the High impact sites using the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the High Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (A) or without (B) External Routable Connectivity, those cyber assets used for Electronic (C) or Physical Access (D) Control or Monitoring, and those cyber assets connected within the same ESP (E) as the cyber assets necessary for the performance of the reliability function. 1.3 – Based on the sites that remain on the candidate list and are not High impact, determine the medium sites based on the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the Medium Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (F) or without (G) External Routable Connectivity, those cyber assets used for Electronic (H) or Physical Access (I) Control or Monitoring, and those cyber assets connected within the same ESP (J) as the cyber assets necessary for the performance of the reliability function. Note: There are 10 types of cyber assets positively identified through this process, each with varying levels of risk to the BES if compromised or rendered unavailable. This, potentially, creates more than 10 levels of protection to be enumerated throughout the rest of CIP-003 through CIP-011. For administrative ease, the MRO NSRF recommends grouping these types of cyber assets based on their actual level of risk in each scenario involving a potential incident that is either cyber or physical in nature and based on the External Routable Connectivity. The rest of the Standards should be written to address each type or grouping of asset. Silence on any one type or grouping will lead to confusion regarding the necessary protective measures and commensurate improvement to security posture. 1.4 – Everything that made the initial candidate list requires protection of some sort, so if it didn't get picked for High or Medium, it gets assessed at Low, because it met the threshold criteria in the BES Site definition. Verbiage in the definitions and the requirements should support this process flow, which will allow the enumeration of High Sites, Medium Sites, and Lows Sites (since we all know a list is required to demonstrate even programmatic elements of CIP compliance). The lists of Cyber Assets will only be required at Medium and High Sites. If possible and feasible, the criteria for dividing the sites into those categories should be progressive in nature, allowing clear demarcation and rationale for the criteria chosen. Additionally, the rest of the Standards should address the requirements progressively for the asset types based on risk. The shift from the current draft to one with obvious progression throughout the CIP-002 methodology and again throughout the rest of the Standards will allow for ease of application at each entity. The current draft does not provide the entities with clear understanding of the order and rationale for identifying the scope of applicability for the CIP Standards, and the NPPD feels that the entities can't be successful with the current format. [2] Change the CIP-002 VSLS to reflect "BES Sites" instead of "Facilities" as those would be the enumerated list. In its current state, it conflicts with the statement that low and zero impact sites do not require enumeration. [3] All VSLs should change the impact designation from cyber asset based to site-based. "High," "Medium," or "Low" designations should precede the word "Site" not "BES Cyber Asset" or "BES Cyber System."
Yes
No
Yes
Yes
Yes
Yes
(1) [Proposed Verbiage] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is. (2) [Proposed Verbiage] CIP-003 R2. For BES Sites identified as low impact, each Responsible Entity shall provide guidance with one or more documented cyber security policies that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] The programmatic elements identified in the sub-requirements may remain, as is. Remove the statement eliminating the need to enumerate low facilities, as it is in conflict with the rest of the verbiage and definitions in the CIP-002-5 and CIP-003-5. (3) VSLs should reflect the actual risk to the BES when one or more elements are missing. The absence of a program should be high or severe, but the lack of discrete components should start at Low.

Group
Luminant
Rick Terrill
No
Yes
Luminant thanks the SDT for their work and the changes made in response to previous comments. In particular Luminant agrees with moving Blackstart Resources to Low Impact for improved BES reliability, and we support the consolidation of Low Impact requirements into one standard. For all responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
Individual
Stephanie Monzon
PJM Interconnection
Yes
Yes
Yes
No
Yes
No
No
No
R3 - We agree with the requirement but have issues with the definition of a CIP Senior Manager in that the definition should include the operation and maintenance of the requirements (ongoing compliance). Looking at the definition of a CIP Senior Manager it appears that after the requirements are implemented, according to the implementation plan, that there is no longer a need for a “CIP Senior Manager”. This appears to contradict what is required in CIP-003 R4 & R5 – Change the verbiage from “dated signature” to “dated approval”. The current verbiage does not take into account electronic workflow approvals. M6 Please update this verbiage so that it is clearer and more easily understood
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Yes
No
No
Yes
No
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Group
Southern California Edison Company
Nathan Smith
Yes

Yes
SCE comments to CIP-002-5: -Introduction A. 3. Purpose: Please clarify the term “misuse”. “Misuse” does not have to be malicious. Perhaps the section should be revised to say “…impact that loss, compromise, or intended malicious misuse of those BES Cyber…” -Facilities 4.1.6: Revise “Load-Serving Entity that owns Facilities” to “Load-Serving Entity that operates owns Facilities” to be consistent with the PRC standards.
Yes
Yes
Yes
Yes
Yes
Yes
SCE Comments to CIP-003-5 -R5: Please list the areas that do allow delegations.
Individual
Kathleen Goodman
ISO New England
No
No
Request clarification on the Applicability of Distribution Providers (DP) and Load Serving Entities (LSE). 1. Does 4.1.2 mean that any DPs owning assets in 4.2.2 need to comply with these CIP Standards? 2. Does 4.1.6 mean that LSEs owning assets in 4.2.1 need to comply with these CIP Standards? 3. Does 4.2.2 mean that only these DP assets are covered by these CIP Standards? 4. Does 4.2.1 mean that only these LSE assets are covered by these CIP Standards? 5. Does the DP’s third bullet in 4.2.2 apply to only protection systems, not UFLS or UVLS since those load shedding systems are covered by the DP’s first bullet? Note the NERC definition of “protection systems” includes load shedding systems, which generates this last question. 6. Section 4.2 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded. Request clarification on High Impact 1.3 and 1.4’s use of “associated data centers”. Are these the “computer rooms” that service a Control Center? Request clarification on the Standard Drafting Team (SDT) expectations on Medium Impact 2.1. Does the SDT expect that the “aggregate highest rate net Real Power capability of the preceding 12 months” will not flip flop on this threshold? In other words, does the SDT expect these asset to remain on one side or the other of this threshold? Recommend a change to R1’s VSLs since Lower and Severe use 100 or more High and Medium BES Cyber Systems while moderate and High uses BES Cyber Assets. Request clarification and consistency. Recommend BES Cyber Assets so that ISOs can easily hit their thresholds. Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: “Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; “ Suggested rewording: Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; Requirement 1.3 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads: “Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;” Suggested rewording: Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;
Yes
Yes
Yes
Yes
No

No
Recommend changing M5 from “signed” to “approved” since some companies use other approval processes. Also these Measures criteria need to be aligned with the Requirements. Measure M5 includes “to approve or authorize specifically identified items” while R5 states “and approved by the CIP Senior Manager”. Request a re-written M6 since it appears to add a new Requirement--“that within 30 days of discharging the delegated authority”. Recommend updating CIP-003 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures show R2 as “low”.
Group
SMUD & BANC
Joe Tarantino
No
No
ISSUE: The summation of actual peak-load seasonal MVA ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities where three or more connections to other Transmission stations or substations. Assessment utilizing the MVA threshold better aligns with other NERC Reliability Standards’ criteria for system impact and is a better measure to determine Medium Impact Rating of Transmission facilities. The reason for including peak load season is so that entities are not required by an auditor to use the higher winter continuous ratings for a system that is summer peaking . We offer the following language for consideration. SUGGESTION: The summation of actual MVA peak-load seasonal ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities at a single station or substation that are operating between 200 kV and 499 kV, are connected to three or more other Transmission stations or substations, and which exceeding 3,000 MVA. The MVA for a Transmission Facility is determined by summing the peak load season continuous ratings in MVA for each incoming or outgoing BES Transmission Line that is connected to another Transmission station or substation.
Individual
Scott Harris
Kansas City Power & Light
Yes
No
The “Low” category in Attachment 1 includes all BES Facilities not included in the High and Medium categories. Many BES Facilities serve customer load that have no impact on the operating reliability of the bulk electric system. Low designations should focus on those facilities that have an impact on the reliability of the bulk electric system not included in the High and Medium category. Recommend modifying the “Low” category to the following: Each BES Cyber System associated with: 3.1. BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M) and having an direct impact on supporting the reliability of the BES. 3.2. Blackstart Resources. 3.3. Elements in the Cranking Path and initial switching requirements.
No
No
No
No
Yes
No
R1 & R2: Recommend striking “and evidence of processes, procedures, or plans that demonstrate the implementation of required topics” from the Measure. Requiring the additional evidence beyond the policy expands the scope of the requirement that is unattainable because Entities won’t know what is sufficient to prove compliance. R3: Recommended wording addition: “Senior Manager by name or Title.” R6: Recommend striking this requirement and moving the change to Senior Manager to R3 and the change to delegates to R5.
Individual

Nick Lauriat
Network & Security Technologies, Inc.
No
Yes
N&ST has observed that with each revision more and more assets are the in the “Low Impact” category, and that owners of “Low Impact” BES Cyber Systems are basically obligated to do nothing. Increasing the size of the low impact category decreases the cyber security of the Bulk Electric System. N&ST strongly cautions against increasing the size of the low impact category (especially for generation assets), and urges the drafting team to attempt to make “medium impact” the default category, rather than “low impact.” N&ST is especially troubled that with the removal of black start, it is basically safe to assume that by the time these standards go in to effect that almost no generation assets in North America will meet the “medium impact” designation. Like others, N&ST expects that this set of cyber security standards should be built to stand the test of time. It's difficult to imagine a different, later drafting team doing a better job creating reliability standards for cyber security. As such, the drafting team should carefully consider whether these standards are challenging enough, or allow entities to (permanently) place assets in the "Low Impact" category simply by making a few network changes.
Yes
No
No
Yes
Yes
Yes
In CIP-003 Requirement R2, N&ST observed that one of the specific requirements is that “For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies (for)...Incident response to a BES Cyber Security Incident.” Despite this, CIP-008-5 does not apply to low impact BES Cyber Systems. N&ST believes that CIP-008-5 should be very “achievable” even for an entity with only low impact BES Cyber Systems. Why not make CIP-008-5 the yardstick that entities with only low impact BES Cyber Systems are measured against? N&ST also observed the same problem regarding CIP-003-5 and CIP-004 “awareness.” If entities are really, truly free to define their own programs for low impact BES Cyber Systems outside of any standards / requirements, perhaps the drafting team should specifically state that? In CIP-003 Requirement R3, N&ST believes the text stating 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 R3 requirement statement, not just the accompanying “Rationale” statement.
Group
Progress Energy
Jim Eckelkamp
No
No
:Progress Energy agrees with EEI and additionally Progress Energy recommends that if any further changes are made to Attachment 1, they be based on alignment with the other Reliability Standards, e.g., TPL, EOP, etc. Progress Energy supports the Standards Drafting Team’s efforts to seek the input of the Operations Committee with regards to the Blackstart issue.
No
No
No
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below R1= Original: Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall

implement one or more documented cyber security policies that address the following topics. Proposed: Each Responsible Entity for its BES Cyber Systems used in high impact and medium impact facilities shall implement one or more documented security policies that address the following topics. Rationale: references to Low/Medium/High Impact should be applied to facilities and not BES Cyber Systems. R2= Original: For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: Proposed: For Facilities identified as not having high impact or medium impact BES Cyber Systems, each Responsible Entity shall document security policies and implement an awareness program that addresses the following topics: 2.1 Cyber security awareness; 2.2 Physical access control; 2.3 Electronic access control; and 2.4 Incident response to a BES Cyber Security Incident. An inventory, list, or discrete identification of BES Cyber Systems is not required. Measure: Evidence must include one or more documented cyber security policies and evidence of processes or procedures. Rationale: If concern from the industry regarding CIP-003-5 R2 is focused on 1) wanting to keep low impact at the site level verses the asset level, and 2) concern around using the word "implementation" (both of which bring into question what evidence would be needed to prove compliance), we feel the following language will meet the intent and address the concerns: R3= Comment: The R6 content applicable to R3, requiring the documenting of changes to the Senior Manager within 30 days, should be included within R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation of a single requirement. R4= VSL's: a. Propose framing review violations as lower/medium VSLs as follows: i. Lower – Policies have not been reviewed within 30 days of annual review time periods ii. Medium – Policies have not been reviewed within 60 days of annual review time periods b. For Policy approval: i. High – Policy has not been approved within 30 days of annual approval timelines ii. Severe – Policy has not been approved within 60 days of annual approval timelines Rationale – There is a difference between approved policy and review of policies. The current approach repeats the violation in which 'not all policies have been approved within the required time period,' which creates confusion. By recognizing the difference in importance (approve vs. review) and framing review violations as less severe, this provides a more relevant scale. R5= Comment: The R6 content applicable to R3, requiring the documenting of changes to the Senior Manager within 30 days, should be included within R3. This will eliminate 'double jeopardy' concerns where failure to adequately document changes will now result in the violation of a single requirement. R6= Should be removed and content included in R3 Additional Comments below a. Comments: The current wording reflects an attempt by the CIP SDT to provide 'protection' from discrete identification of low impact BES cyber systems, yet the requirements are (still) framed in a way that would require discrete identification to adequately demonstrate compliance. This provides conflicting messages that would impede approval of protection controls for BES Cyber Systems used within High and Medium Impact facilities. b. Remove "egress" from Guidelines 1.4

Individual

John Allen

City Utilities of Springfield, MO

No

Yes

City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. But, we do not agree with the current draft of CIP-002-5 that forces all small Control Centers into the Medium Impact classification, subjecting them to the onerous compliance obligations of CIP-003 through CIP-011. Today there are many small entities with Control Centers that are not identified as Critical Assets, because studies show that the loss or compromise of their whole system would not cause a significant impact to the BES. However, it is our understanding that the impact of these small systems to the BES is not the purpose for this classification. Instead the reason for identifying all Control Centers is to address FERC's concern regarding "connectivity" to High Impact Control Centers. We believe that this concern is valid and can be addressed without the enormous compliance burden placed on small entities and the ERO by the proposed draft of CIP-002-5. It is timely that NERC is actively looking for ways to reduce the compliance monitoring burden on the Regional Entities. Significant work is being performed by the BES Definition SDT to properly identify Facilities that are important to the BES. There is also NERC's Risk Based Compliance initiative that is working to develop metrics that will classify an entity based on its risk to the BES. The goal is to reduce the amount of ERO resources needed to monitor the low

risk entities. However, it appears that CIP-002-5 is not consistent with these efforts. Therefore, NERC and the SDT should consider the huge impact of the proposed criteria in CIP-002-5 on compliance monitoring resources that are already overloaded. NERC and the drafting team should also consider the unintended consequence of diverting large amounts of industry resources to address requirements that could (emphasis added) impact the reliable operation of the BES, when at the same time NERC and the industry is diligently working to focus resources on the ones we know (emphasis added) impact reliability. It is important to note that with the recent approval of Version 4 “bright-line criteria”, the “High Impact” Control Centers will be secured, not only from vulnerabilities to outside attacks, but also from “connectivity” to other Control Centers. Each entity must be responsible for securing its own electronic security perimeter(s) and there is no possible way to remove all vulnerabilities and secure all of the “weakest links” that CIP-002-5 is attempting to address. Besides, how do you plan to secure all of the other networks that are "connected" to the High Impact Control Centers that are outside of FERC/NERC jurisdiction? However, we believe it is reasonable to support a set of standards that apply programmatic requirements to small Control Centers for such things as: 1. Control and monitoring of electronic access 2. Control and monitoring of physical access 3. Personnel risk assessments 4. Training 5. Incident response 6. Recovery plans Therefore, we propose the following options for the SDT to consider: 1. Create a size limit for “Medium Impact” Control Centers. For example, raise the threshold for “High Impact” Control Centers to 3000 MW and move the 1500 MW threshold to “Medium Impact”. Then classify all other Control Centers as “Low Impact” and add programmatic requirements to CIP-002 through CIP-009. 2. Remove the proposed requirements in CIP-003 through CIP-009 for “Medium Impact” Control Centers and replace with programmatic requirements. 3. Move criteria 2.11 into the “Low Impact” category and add programmatic requirements to CIP-002 through CIP-009. If there is concern that an entity with a “Low Impact” Control Center would not have enough incentive for security, then you could add a requirement that would change the compliance obligations based on a security incident due to negligence. For example, the entity could do an analysis to determine if the event was related to an issue of non-compliance with one of its programs. If so, then the Regional Entity could increase compliance monitoring of the entity’s programs for a period of time until the entity demonstrates that it has things under control. The changes we propose would decrease the financial impact on small entities by reducing the amount of compliance documentation required, while still ensuring a base-line of protection for those cyber systems that are connected to “High Impact” Control Centers via ICCP or other applications. It would also bring the CIP Standards into line with the Risk-Based Compliance initiative at NERC by matching an entity’s compliance obligations according to its risk to the BES. This would ensure that the ERO has adequate resources in the future to monitor the cyber systems that are critical to the reliable operation of the BES.
Yes
Yes
Yes
Yes
Yes
Yes
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We support the comments submitted by SPP and APPA.
Group
NCEMC
Scott Brame
No
Yes
(1) 4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying “that are part of a Load shedding program” implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW “program” and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. NCEMC recommends that the SDT provide guidance with very

clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. (2) Under the inclusion threshold for DP, 4.2.2, third bullet, states: "A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard." NCEMC recommends that the following language be added to the end of that bullet; ", and where the Protection System is connected to a supervisory control system providing remote operation capability." This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. (3) Attachment 1 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for NCEMC. It will be difficult to support CIP-002-5 without this revision. (4) We disagree with including LSE as an applicable entity. Per the NERC function model, LSE's do not own or operate UFLS or UVLS relays. Page 26 of the Reliability Functional Model Technical Document makes this clear with the statement, "Unlike the Distribution Provider, the Load-Serving Entity does not have Bulk Electric System assets ("wires") but does take title to energy." The only role that is given to the LSE in the Reliability Functional Model is to "participate in under-frequency load shedding systems and under-voltage load shedding systems through identification of critical customer loads that are to be excluded from load shedding systems". They are given no role to own, install or maintain UFLS or UVLS. They simply assist in the identification of critical loads to help ensure they are not inadvertently included in the UFLS or UVLS program. Because the standard only envisions inclusion of LSES due to UVLS and UFLS, their complete removal from the standard is warranted. (5) Use of Systems is not consistent with the NERC Glossary definition throughout many sections of the standard and application guidelines. The NERC Glossary defines System as: "A combination of generation, transmission, and distribution components." In section 4.2.2, how can a Distribution Provider have a System when two (generation and transmission) of three required elements to meet the definition are not included? Use of "System" in the first bullet under section 4.2.2 clearly does not intend the NERC Glossary definition but rather a computer or control system. It appears that a wholesale find and replace was performed on "system" between versions which may have contributed to this problem. There are many other instances in the Application Guidelines requiring the use of System that is questionable as well. (6) It is not clear why "Bulk Power" is capitalized in the second paragraph of the Rationale box for R1. (7) We recommend that Measurement M1 be clarified that the "list of changes to the BES" per Part 1.4 may be an acknowledgement that there were no changes. (8) What is the justification for the values used for the VSLs in Requirement R1? For example, how were 40 Facilities and 100 Cyber Systems arrived at for the Lower VSL? A justification needs to be provided? Why not use 80 Facilities and 200 Cyber Systems? (9) 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. This needs to be further clarified. (10) It would be helpful if the application guidelines clarify how the Reliability Coordinator, Transmission Planner or Planning Coordinator will notify the Generator Owner, Generator Operator, Transmission Owner and Transmission Operator that their equipment meets criteria 2.3 and 2.6. (11) Criterion 2.8 needs supporting explanation in the Application Guidelines explaining how the Transmission Owner will determine that a generator it is does not own or operate meets the criteria in Part 2.3. Otherwise, it is not clear how the Transmission Owner will know that its interconnection equipment to the generator should be included in this Medium Impact Rating. (12) There is a statement in the first paragraph of the "Applicability to Distribution Providers and Load Serving Entities" section of the Application Guidelines that states the qualifications for inclusion of the Distribution Provider are based on requirements applicable to Distribution Providers in EOP-005 and registration. This statement could actually be contradictory to Applicability section 4.2.2 which includes more applicability than just restoration per EOP-005. The statement should either be deleted or further explained. (13) The Application Guidelines on page 30 state the highest MW rating for the preceding 12 months will be used for Attachment 1 criterion 2.10 regarding load shedding systems. Rating is not the right word. Rather, the highest hourly integrated load is more correct. Instantaneous load should not be

considered.
No
No
Yes
Yes
Yes
Yes
(1) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-003-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding Question 4 (CIP-003-5 R1): Part 1.4 needs to be clarified that the NERC Glossary definition of System does not apply. (3) Regarding Question 4 (CIP-003-5 R1): The application guidelines for interactive remote access regarding inclusion of language in contracts with vendors, consultants and contractors should be modified. The guidelines state that the language should require them to adhere to the responsible entity's Interactive Remote Access controls. While we agree, in general, that contracts should reflect this language, the guidelines should be clear that this only applies to contracts executed after the enforcement date of this standard. Applying this standard to existing contracts could compel the responsible entity to renegotiate all contracts which puts the responsible entity at a significant disadvantage particularly with some contracts such those with EMS vendors. (4) Regarding Question 5 (CIP-003-5 R2): NCEMC is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, NCEMC requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance. (5) Regarding Question 5 (CIP-003-5 R2): 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. (6) Regarding Question 9 (CIP-003-5 R6): Four VSLs could and should be written based on the number of days late that the change to CIP Senior Manager or delegates was documented. (7) Regarding the Application Guidelines: The paragraph under Requirement R3 should apply to what is now Requirement R4 as a result of re-ordering the requirements from the previous draft. In the previous draft R3 requires the review and approval of the cyber security policies by the CIP Senior Manager at least once each calendar year, not to exceed 15 calendar months… This is now Requirement R4.
Individual
Scott Miller
MEAG Power
Yes
Yes
The summation of actual MVA ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities where three or more connections to other Transmission stations or substations. Assessment utilizing the MVA threshold better aligns with other NERC Reliability Standards. In Attachment 1, please clarify 'Functional Obligations' (1.3) and 'Data Center' (1.4) CIP-002-5, 2.11 as it is dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria ("SCRC"), section III (d), address the Transmission Owner ("TO")/Transmission Operator ("TOP") uses the same criteria to define both TO and TOPs. However, the application of what entities registers or is required to register as a Transmission Owner and not as a TOP is not defined and is not consistent though regions or North America. Section 2.11 should be removed because there is no "reliability based" justification that registration as TOP justifies a Medium Impact Rating. If the

registration thresholds were removed from section 2.11 we would likely change its vote to affirmative.
Yes
No
Yes
Yes
Yes
Yes
CIP 003-5 R2 states that the Responsible Entity for BES Cyber Systems not identified as High Impact or Medium Impact (i.e., Interpreted as “Low Impact” BES Cyber Systems) “shall implement one of more documented cyber security policies that address the following topics: 2.1 Cyber security awareness; 2.2 Physically access control; 2.3 Electronic access control; and 3) Incident response to a BES Cyber Security Incident”. This proposed language in CIP 003-5 R2 is “loose” and allows for potential future interpretation – via new NERC CAN’s, new NERC RSAW’s, NERC Regional Entity interpretations during Functional Entity audits, etc. - Which industry may (or may not) agree with in the future. Recommendation: 1) Eliminate ALL CIP 003-5 R2 requirements associated with BES Cyber Systems that are not High or Medium Impact – as Low Impact systems are Non Impact systems that should not impact BES system operating conditions – such as BES instability, separation, or cascading OR 2) Have the CIP drafting team address specific “prescriptive” Low Impact BES Cyber System requirements within CIP 003-5 through CIP 011-5 (for cyber security awareness/training, physical access control, electronic access control, incident response, etc.) – similar to the way the prescriptive requirements have been written for Medium and High Impact BES Cyber Systems.
Individual
Nathan Mitchell
American Public Power Association
No
Yes
APPA agrees in part with the changes the SDT made to the applicability section for DPs and LSEs. The SDT has made it clear that not all DPs and LSEs need to comply with these standards, only those who own and operate specific BES Facilities are required to comply. This will help eliminate the exercise of proving that some small entities do not own cyber assets that impact the BES, therefore CIP Reliability Standards do not apply to them. However, there are still some questions on the criteria the SDT used as a threshold in the Applicability section 4.2 Facilities. Point 1: The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying “that are part of a Load shedding program” implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW “program” and will be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. APPA recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. There must be a clear designation of the applicability of this standard so small entity impact can be minimized. Point 2: The SDT should strike the wording in the Special Protection System bullet of 4.2.2: “is required by a NERC or Regional Reliability Standard” and replace that with a threshold such as “where the Special Protection System or Remedial Action Scheme controls xxxxMW or more of peak resources.” Or designate the BA or another entity to determine the critical SPS and RAS by adding; “where the SPS and RAS is designated by the BA as critical.” A clear threshold will prevent future non-CIP standards from dictating applicability with the current CIP standard without due process through standards development. There must be a clear designation of the applicability of this standard so small entity impact can be minimized. Point 3: Under the inclusion threshold for DP the SDT states: “A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard.” APPA recommends that the SDT remove the “Protection System” bullet since it causes way too much confusion and will allow future non-CIP standards to dictate applicability with the current CIP standard without due process. At a minimum the SDT needs to clarify which “Protection Systems” they are referring to in this bullet. If the SDT did not intend on bringing in all other UFLS and UVLS relays not designated in the first bullet, there must be a clarifying exclusions such as: “Protection Systems (excluding UFLS and UVLS relays not covered above)…” If these

suggestions are not accepted by the SDT, there must at least be clear guidance on what specific Protection Systems are referred to in this bullet. APPA would even suggest that current standards that apply to this bullet be listed in the guidance. There must be a clear designation of the applicability of this standard so small entity impact can be minimized. Point 4: APPA agrees with the changes the SDT made to Attachment 1. We would like to commend the SDT for their insight in changing the designation of Blackstart Resources and Cranking Paths from Medium to Low Impact. This change will help avoid the reliability impact to the BES of Blackstart Resources being removed from the Transmission Operators Restoration Plan if those units become uneconomic due to compliance costs. This truly prioritizes reliability of the BES and mitigates the negative impacts of a compliance requirement. The following are further changes needed in Attachment 1: As stated in comments on the Definition of Control Center: APPA Recommendation: Clarify in guidance what "control" within the Control Center definition means. If the SDT uses the CIP Version 1 FAQ response as the guidance: "monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction" APPA recommends that control centers which use only manual or voice instruction as the control be designated as Low Impact facilities in CIP-002-5 Attachment 1. This designation will help reduce the burden of compliance for small entities that chose to use this cyber risk mitigation method. Criteria 2.10 in Attachment 1 is still unclear and should be changed. Similar to APPA's statement in Point 1 above, 2.10 "Each System or group of Elements that performs automatic Load shedding…" implies that an entity could have only 50 MW of load that will be shed as part of a System or group of Elements in a larger 300 MW "program" and be required to identify their UFLS system as a Medium Impact facility and comply with all CIP requirements. Another scenario where a DP with a 250 MW load shedding program not associated with any other group would not come into CIP applicability at all. APPA recommends that entities with UFLS and UVLS systems below 300 MW be classified as Low Impact facilities. APPA believes that Criteria 2.11 in Attachment 1 should at a minimum designate all control centers with control of less than 300 MW of resources as Low Impact. This will clearly define a lower threshold as requested for in 2.10 above and reduce the burden of compliance for small entities.
Yes
Yes
No
No
No
No
APPA agrees with the STD proposal to include all of the programmatic requirements for BES Cyber Systems not identified as High Impact or Medium Impact in one requirement. This will help the industry focus their compliance efforts on documenting the development and implementation of policies for the four sub requirements. However, APPA is concerned about the audit process that is implied in the Measures section. M2 states: "evidence of processes, procedures, or plans that demonstrate the implementation of the required topics." It has been stated at various STD meetings that auditors will need to measure "implementation" by sampling physical or electronic access controls at specific facilities or equipment. In order for sampling to be random and in accordance with auditing practice, there needs to be a data set to sample. This is contrary to the note in Requirement R2 that states: "An inventory, list, or discrete identification of BES Cyber Systems is not required." APPA recommends that the SDT work with NERC enforcement staff in crafting an RSAW that will include evaluation of the documented processes, procedures and/or plans as the auditor's first measure of implementation. APPA recommends removal of CIP-003-5 R3, and R5 since CIP-002-5 Requirement R2 implies that all of the documentation is done to designate the CIP Senior Manager and requiring further documentation does not improve BES reliability. The review process of CIP-003-5 Requirement R3 should be included in R1 and R2. This will eliminate unnecessary documentation requirements from the standards and may help reduce the paperwork burden of the small responsible entities.
Group
SPP and specific Member companies
Lesley Bingham
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
1. In CIP-003-5 Measure 4, the measure says “Evidence may include but is not limited to” and then lists two numbered items connected by the word “and”. If evidence “may include”, then the items below are suggestions, not requirements. As they read now, they are both required and not strictly examples of appropriate evidence. These should be bulleted (i.e. example items which are not the only methods for compliance) and either one, if presented, should be appropriate evidence. Specifically, if a document management system captures and tracks approvals, that should be sufficient evidence for this requirements. A hard copy with a wet ink signature should not also be required for compliance. 2. CIP-003-5 R5 states that the CIP Senior Manager may delegate authority “where allowed by the CIP Standards”. It would be helpful to have the standards where it is not allowed listed in this requirement. While the goal of having clear standards that do not point to other standards is laudable, citing the specific items that cannot be delegated would provide much-appreciated clarity. 3. CIP-003-5 R6 needs additional clarification. Certainly, changes to the CIP Senior Manager should be reflected in timely updates to the authorization document. A new delegation should also be similarly captured. However, what is not clear is what smaller changes should be reflected. Specifically, the sentence “Delegation changes do not need to be reinstated with a change to the delegator” is confusing. Does this mean that if the CIP Senior Manager changes, the downstream delegations do not change and only the documentation pertaining to the CIP Senior Manager needs to be approved by the “high level official” who designates the CIP Senior Manager? Or does this indicate that if delegations are specified by title and the person carrying the title changes, no update of documentation is needed as long as the new title holder can also carry the delegated approval (i.e. Director of Physical Security approves—by delegation—physical access requests, specific person leaves, replacement Director retains approval rights)? It would be more clear to state “Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegated authority, whether by name or by title, within thirty calendar days of the change.”
Individual
Jennifer White
Alliant Energy
No
Yes
[1] The proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. The impact rating should align with the facility (BES Site) instead of the cyber asset. [R1 Proposed Flow] 1.1-Based on the definition for a BES Site, each entity should create a list of BES Sites. This step will determine for the entity, which sites have zero BES impact vs.which sites have an impact and will be later divided into high, medium, and low. This also creates positive definition or threshold for Low Sites. These Low sites, based on the criteria, will have some impact and require, at a minimum, programmatic protection at the Site level. There will be no need to identify the cyber assets associated with sites that have zero impact or those that remain in the Low category. All Low, Medium, and High Sites will have the protections afforded the Low sites, but for those meeting the Medium and High criteria, additional protections are required, as well as the enumeration and classification of the cyber assets critical to providing the BES functionality of the location. After identifying the Low BES Sites, the Medium and High criteria must be considered for each Site. The following is a proposed flow for which the order can be modified while maintaining efficacy. Also, the proposed flow may require an adjustment of the criteria, if any of the High criteria are dependent on Medium criteria output. The order should, when applied, be progressive in nature and not require jumping from one criteria list to another. 1.2 – Based on the sites that remain on the candidate list, determine the medium sites based on the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the Medium Sites. The cyber assets that are critical to the

performance of the reliability function will then be divided into those with (F) or without (G)External Routable Connectivity, those cyber assets used for Electronic (H) or Physical Access (I) Control or Monitoring, and those cyber assets connected within the same ESP (J) as the cyber assets necessary for the performance of the reliability function. 1.3- Based on the candidate list for sites with BES impact created from the execution of the first step and second step, identify the High impact sites using the criteria in the attachment. A candidate list for cyber assets required in order for the BES Site to perform its reliability function(s) will be created for the High Sites. The cyber assets that are critical to the performance of the reliability function will then be divided into those with (A) or without (B)External Routable Connectivity, those cyber assets used for Electronic (C) or Physical Access (D) Control or Monitoring, and those cyber assets connected within the same ESP (E) as the cyber assets necessary for the performance of the reliability function. Note: There are 10 types of cyber assets positively identified through this process, each with varying levels of risk to the BES if compromised or rendered unavailable. This, potentially, creates more than 10 levels of protection to be enumerated throughout the rest of CIP-003 through CIP-011. For administrative ease, Alliant Energy recommends grouping these types of cyber assets based on their actual level of risk in each scenario involving a potential incident that is either cyber or physical in nature and based on the External Routable Connectivity. The rest of the Standards should be written to address each type or grouping of asset. Silence on any one type or grouping will lead to confusion regarding the necessary protective measures and commensurate improvement to security posture. 1.4 – Everything that made the initial candidate list requires protection of some sort, so if it didn't get picked for High or Medium, it gets assessed at Low, because it met the threshold criteria in the BES Site definition. Verbiage in the definitions and the requirements should support this process flow, which will allow the enumeration of High Sites, Medium Sites, and Lows Sites (since we all know a list is required to demonstrate even programmatic elements of CIP compliance). The lists of Cyber Assets will only be required at Medium and High Sites. If possible and feasible, the criteria for dividing the sites into those categories should be progressive in nature, allowing clear demarcation and rationale for the criteria chosen. Additionally, the rest of the Standards should address the requirements progressively for the asset types based on risk. The shift from the current draft to one with obvious progression throughout the CIP-002 methodology and again throughout the rest of the Standards will allow for ease of application at each entity. The current draft does not provide the entities with clear understanding of the order and rationale for identifying the scope of applicability for the CIP Standards, and the MRO NSRF feels that the entities can't be successful with the current format. [2] Change the CIP-002 VSLS to reflect "BES Sites" instead of "Facilities" as those would be the enumerated list. In its current state, it conflicts with the statement that low and zero impact sites do not require enumeration. [3] All VSLs should change the impact designation from cyber asset based to site-based. "High," "Medium," or "Low" designations should precede the word "Site" not "BES Cyber Asset" or "BES Cyber System." [Proposed Draft CIP-002-5] This is one of several proposed drafts for CIP-002-5. Others are being offered through independent contacts with the SDT. Recommend considering the following, in whole or in part, as an alternative to the currently drafted CIP-002-5. Requirements R1. BES Site Identification – Each Responsible Entity shall identify BES Sites as determined through an annual application of the criteria contained in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 3.1 – 3.5. The Responsible Entity shall use this candidate list to further identify the BES Sites as Low, Medium, or High Impact BES Sites using the following applications: [Violation Risk Factor: High] R1.1. Using the list of BES Sites identified in R1, identify Medium Impact BES Sites as determined through an annual application of the criteria contained in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 2.1 – 2.11. R1.2 Using the list of BES Sites identified in R1 and R1.1, identify High Impact BES Sites as determined through an annual application of the criteria contained in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 1.1 – 1.4. R1.3 BES Sites failing to be identified in R1.1 and R2.2 while meeting the minimum criteria for CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 3.1 – 3.5 shall be identified as Low Impact BES Sites. Low Impact BES Sites are not subject to CIP-002-5 R2. R1.4 Review (and update as needed) the identification in Requirement R1, Parts 1.1, 1.2, and 1.3 within 60 calendar days of when a change to a BES Site is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the identification or categorization of the BES Site from a lower to a higher impact category. M1. Acceptable evidence may include, but is not limited to, dated electronic or physical lists required by Requirement R1, Parts 1.1, 1.2 and 1.3, and a list of changes to the BES (with a date for each change) that cause a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category. R2. BES Cyber System Identification – Using the lists of High and Medium

Impact BES Sites pursuant to Requirement R1.1 and R1.2, the Responsible Entity shall develop risk category lists of BES Cyber Systems essential to the performance of reliability functions at each BES Site. In order to apply protective measures based on security and BES functionality risk, the Responsible Entity shall identify: [Violation Risk Factor: High] R2.1.BES Cyber Systems with External Routable Connectivity R2.2 BES Cyber Systems without External Routable Connectivity R2.3 Physical Access Control and Monitoring Systems R2.4 Electronic Access Control and Monitoring Systems R2.5 Associated Protected Cyber Assets within the ESP of a BES Cyber System with External Routable Connectivity R2.6 Review (and update as needed) the lists identified in Requirements R2.1 – R2.5, Parts 1.1, 1.2, and 1.3 within 30 calendar days of when a change to a BES Cyber System is placed into operation, which is planned to be in service for more than six calendar months and causes a change in the categorization of the BES Cyber System or BES Cyber Asset(s). M2. Acceptable evidence may include, but is not limited to, dated electronic or physical lists required by Requirement R2, Parts 2.1- 2.5, and a list of changes to the BES Cyber System (with a date for each change) that cause a change in the categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher risk category. R3. Annual Approval – The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 and R2 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3. [Violation Risk Factor: Lower] M2. Acceptable evidence may include, but is not limited to, electronic or physical dated and signed records, even if the lists are null, to demonstrate that the Responsible Entity has had its CIP Senior Manager or delegate review and update, where applicable, the identification and categorization of BES Sites, BES Cyber Systems, and their associated risk categorizations for any associated cyber assets, at least once each calendar year, not to exceed 15 calendar months between occurrences. Alliant Energy agrees with the MRO NSRF comments related to the criteria in attachment 1.
Yes
No
Yes
Yes
Yes
Yes
(1) [Proposed Verbiage] CIP-003 R1 Each Responsible Entity for the identified BES Cyber Systems critical to the operation of high impact and medium impact BES Sites shall implement one or more documented cyber security policies that address the following topics: Keep 1.1 – 1.10 as is. (2) [Proposed Verbiage] CIP-003 R2. For BES Sites identified as low impact, each Responsible Entity shall provide guidance with one or more documented cyber security policies that address the following topics: [Violation Risk Factor: Low] [Time Horizon: Operations Planning] The programmatic elements identified in the sub-requirements may remain, as is. (3) VSLs should reflect the actual risk to the BES when one or more elements are missing. The absence of a program should be high or severe, but the lack of discrete components should start at Low. Please note that the above changes apply to structure and not content of what the SDT is intending to accomplish.
Group
Dairyland Power Cooperative
Tommy Drea
No
Yes
Please see MRO NSRF comments.
Yes
No
Yes
Yes
Yes
Yes
Please see MRO NSRF comments.
Individual

Tracy Richardson
Springfield Utility Board
No
Yes
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. 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.
Yes
Yes
Yes
Yes
Yes
Yes
SUB has no additional comments since the last comment period.
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
Yes
CIP-002-5, Attachment 1, 2.3 and 2.6: The language in these requirements provide for entities other than the registered entity to designate assets for treatment as Medium level assets. As written, the process is a unilateral decision when it should be a more collaborative determination process with a mutual understanding of the decision. Further, 2.6 enables RCs, PCs or TPs to identify assets for inclusion, but does not require that they inform the assets owners/operators of the identification as the language should and does in 2.3. These are serious concerns. Sections 2.3 and 2.6 should include language to challenge the inclusion of assets by other entities perhaps in conjunction with the BES exception process or an alternate mechanism to challenge. CIP-002-5, Attachment 1, 2.10: We accept the 300 MW threshold; however, the number lacks a technical justification and basis in reliability. The history of the 300 MW as a trigger for OE-417 reporting is not relevant to reliability nor is it sufficient justification for standard requirements. The language around the threshold is critical to

the threshold as to the appropriate applicability of the requirements. So while we accept the language in 2.10, the context of the threshold should remain part of the standard development record to avoid future expansion of requirements at the 300 MW threshold. CIP-002-5, Attachment 1, 2.11: Similar to 2.10, there is little basis for the 300MW threshold. We recognize that determining an appropriate, reliability-based threshold is a challenge. At least the 1500 MW threshold has a more relevant to reliability as an average of contingency reserves. CIP-002-5, Attachment 1, 3.: While we suspect that 3.2 and 3.3 are specifically identified in the attachment because they were previously identified elsewhere in the language in earlier drafts, because they are no longer listed in sections 1 or 2, they should automatically be classified as Low. It is not necessary to include 3.2 or 3.3. Consider updating the section 3 language to more simply read: 3. Low Impact Rating (L) - Each BES Cyber System associated with BES Facilities not categorized in Section 1 as having a High Impact Rating (H) or Section 2 as having a Medium Impact Rating (M). BES Cyber Systems that are not identified as high impact or medium impact shall default to the category of low impact and do not require discrete identification.
Yes
No
Yes
Yes
No
Yes
CIP-003-5, R2: In R2, the language restates that the requirement applies to BES Cyber Systems not identified as high or medium impact rather than specifically saying low. We understand that this wording is intentional to avoid suggesting that "identifying" systems as low impact requires a list to demonstrate compliance. While the language is somewhat awkward, we support this approach. Maintaining a complete list of low impact assets to demonstrate 100% compliance presents significant compliance risk, while missing the value of policies addressing the cited topics of concern. The implementation of cyber security policies and practices applicable to low impact systems is more relevant to reliability than a list identifying low impact systems. Leaving a system covered by the policies and practices off a list is irrelevant to reliability. To further clarify the R2 language, please consider adding discussion of the reasoning behind the specific language in the guideline section. CIP-003-5, R5: R5 is acceptable; however, for consistency, M5 should read like M6. Please revise the first line to read: "Evidence may include, but is not limited to, dated documentation, …"
Group
Western Electricity Coordinating Council
Steve Rueckert
No
Yes
Identification of BES Facilities, systems and elements: WECC objects to the proposed the Impact Rating Criteria (“Criteria”) changes in “Attachment 1, 1. High Impact Rating.” The proposed changes exclude a number of BA and TOP Control Centers, Backup Control Centers, and Data Centers. Further, the proposed changes are inconsistent with the mandates of FERC Order 706 . FERC does not distinguish Transmission Operator control centers as posing “less of a risk.” FERC Order 706 at 280 states that “it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a Critical Assets.” FERC Order 761 goes further addressing CIP Version 5 stating: we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with requirement of Order No. 706.” WECC recommends that all Control Centers, backup Control Centers, and associated data centers used to perform function obligations of the RC, BA and TOP should be categorized as “High Impact” facilities. WECC objects to the categorization of “Blackstart Resources” and “Elements in a Cranking Path and initial switch requirements” as “Low Impact.” FERC explicitly rejected the rationale underpinning this categorization. FERC Order 761 at 47 states: “We [the Commission] disagree with MISO that designating a “must run” unit as a Critical Asset may create an incentive for generator owners and generator operators to remove units from service prior to their designation as Critical Assets.” WECC Enforcement recommends that “Blackstart Resources” and “Elements in a Cranking Path and Initial Switch Requirements” be categorized as “High Impact” or, at

least as “Medium Impact.” WECC objects to proposed changes in Criteria 2.6 and Criteria 2.9, that eliminate consideration of facilities critical to derivations of SOLs and contingencies for transmission paths listed in the most current table titled “Major WECC Transfer Paths in the BES.” WECC does not rely on derivation of IROLS. Consideration of Major WECC Transfer Paths must be considered to ensure reliability in the Western Interconnection. In the event that WECC may monitor their system for IROL’s the language in the standard should stipulate “continuous IROL’s.” R1.1. WECC recommends that R1.1 use consistent terms. R1.1 requires the identification of certain facilities, and “systems,” or equipment”. The VSL for R1.1, however, only references the number of facilities and does not reference “systems” or “equipment.” The terms “systems” and “equipment” are undefined and create ambiguity. To be consistent, the VSL for R1.1 should include “systems” and “equipment” and the terms “systems” or “equipment” should either be defined or revised to “BES systems and BES equipment.” Enforcement also recommends that R1.1 explicitly require entities to “identify and list” facilities as either “high” impact facilities, or as “medium” impact facilities.” This would be consistent with R1.2 and R1.3 requires separate identification of High impact BES Cyber Systems and Medium BES Cyber Systems. R1.2 WECC recommends that R1.2 require entities to identify each High impact BES Cyber System and Cyber Assets comprising that BES Cyber System. Further, Enforcement proposes that additional clarification be provided for the term “used for.” R1.3 WECC proposes that references to “systems or equipment” be stricken or defined for reasons stated above. Enforcement recommends that R1.3 require entities to identify and document each High impact BES Cyber System and Cyber Asset comprising that BES Cyber System. Further, Enforcement proposes that additional clarification be provided for the term “used for” R1.4 WECC objects to R1.4 in its entirety. The change to any BES Element or Facility should, automatically trigger a review. Further, the addition of facilities or any BES Element should also be considered in any review under R1.4. Limiting a review to facilities “planned to be in service for more than six calendar months” is unenforceable. The term “planned” is ambiguous. What would constitute evidence of “planning?” What if the duration of the change is “planned” for 6 months, but exceeds the 6 month period. Is the change still exempt because at the time of implementation, the change was “planned” not to exceed 6 months? Further, R1.4 review is triggered only after determining there is a “change in the identification or categorization of BES Cyber Systems.” It is impossible to identify this change, however, without first conducting a review. Enforcement recommends rewriting the proposed requirement to first require a review of any change to BES facilities or systems, regardless of their duration. Secondly, based on this review, Enforcement recommends that entities then identify BES Cyber Assets or BES Cyber Systems that should be categorized from a loser to higher impact category.
Yes
Yes
Yes
Individual
Scott Berry
Indiana Municipal Power Agency
No
No
IMPA does not agree with the wording in Attachment 1, Section 2, Subsection 2.11, to be used for determining if each BES Cyber Systems associated with Control Centers and associated data centers that are not designated as having a High Impact Rating (H) should have a Medium Impact Rating. More specifically in Subsection 2.11 part (2): “control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation.” This is an overly broad definition that will cause smaller Control Centers that control several smaller generation Facilities over multiple Balancing Authority Areas to have a Medium Impact Rating because the aggregate real power capability they control is equal to or exceeds 300 MW. IMPA would propose that the wording be modified to include only those Control Centers and associated data centers that control an aggregate real power capability equal to or exceeding 300 MW in a single Balancing Authority Area. GOPs already have a relationship with their respective BA(s) and this would be a natural extension of the Functional Model that is already in place. In addition, as currently written the inclusion of “Control Center” and “monitor and control” will cause non-operating entities (entities that don’t directly control generation and may only have a hand in the scheduling for startup

of the generation prior to the actual real time operation/control of the unit by operating personnel) to have a Medium Impact Rating for a Control Center that clearly should be Low Impact.
Individual
Gregory Campoli
NYISO
No
Yes
The references to NIST and Risk Methodology seem puzzling. In utilizing FISMA and as a result NIST, impact is assigned by classification of levels of confidentiality, integrity and availability of data and by using Risk Assessments to apply additional appropriate and commensurate security controls. In contrast, the application of CIP security controls have no dependency on Risk Assessment or from the impact to an organization through compromise of data confidentially and integrity. Additionally, CIP specifically uses only vulnerability assessments without regard to threats and probability calculations in the “Risk” equation. - CIP standards are applied without regard of compromise to confidentiality and integrity of data and only on merits regarding impact in support of the Bulk Electric System. In addition, FIPS 199 supports data impact assessment as a component of a cyber system(s) as well as data in other forms. One parallel exists between the two frameworks only by using availability of a BES Cyber System and therefore the availability of its data to support the BES; as cyber systems are a means of supplying data one could use the definition of BES Cyber System to mean data AND function. CIP High, Medium or Low impact level is determined as a function or mission of cyber assets in support of the BES. Other factors affect impact such as proximity to other critical cyber assets along with other supporting monitoring and authentication processes. It isn’t until CIP 011 that the standards specifically address information protection and effects of data compromise as leading to potential instability of the BES. - FISMA calls for FIPS 199 to assess impact by determining the confidentiality, integrity and availability of data either alone or part of a larger system or systems. FISMA additionally requires application of baseline security controls from NIST 800-53 commensurate to the assigned impact level. Additional security controls are implemented as a result of Risk Assessments within the cyber system lifecycle. CIP has no application of Cyber System Lifecycles within the context of ongoing evaluation security controls. - FISMA allows the application of technical, operational and managerial controls of equal proportion without an compulsory dependence on technical controls. CIP utilizes, in lieu of technical controls, Technical Feasibility Exceptions as compensating measures.
Yes
Yes
Yes
No
Yes
Yes
CIP-003 R4 M4 item 2 change the words “dated signature” to “dated approval” for better alignment with the requirement. CIP-003-5 R5 M5 change the word “signed” to “approved” for better alignment with the requirement.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
Yes
FEUS agrees with the comments submitted by APPA. The second criteria for Attachment 1.4 – “control of one or more of the generation assets that meet criteria 2.3, 2.6 and 2.9,” should the and be an or?
Yes
Yes
Yes
Yes

Yes
Yes
FEUS agrees with the comments submitted by APPA
Individual
Scott Kinney
Avista
see comments provided by EEI
See comments provided by EEI
Group
CenterPoint Energy
John Brockhan
No
Yes
CenterPoint Energy appreciates the evident consideration of previous comments; however, the Company disagrees with the overall changes made to CIP-002-5 since the last formal comment period. Specific suggestions and/or proposals for alternative language are as follows: R1.1 – CenterPoint Energy recommends that the sentence end after “Attachment 1” as the additional description of the Impact Rating Criteria does not enhance the requirement. R1.4 – CenterPoint Energy requests examples of changes to be covered under this requirement. Attachment 1 - CenterPoint Energy proposes that the introductory paragraphs under each of the Impact Rating Criteria be deleted as it may create uncertainty in what is being identified through the application of Attachment 1 (ex. Facilities and equipment versus BES Cyber Systems). CenterPoint Energy understands that Attachment 1 is now focused on Facilities; therefore, the phrase “used by and located at” is no longer needed. CenterPoint Energy also has significant concerns with criteria 2.5. As currently defined, the values force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. CenterPoint Energy recommends the values be revised as follows: Voltage Value of a Line 200 kV – 399 kV – Weight Value per Line - 800; Voltage Value of a line 400kV to 499 kV – Weight Value per Line – 1300. CenterPoint Energy shares the auditability and documentation concerns discussed in industry groups and committees such as Edison Electric Institute (EEI) and Texas Reliability Entity NERC Standards Review Subcommittee (NSRS) regarding the low impact criteria, “BES Cyber Systems which are not included in high impact or medium impact shall default to the category of low impact and do not require discrete identification.” Given the removal of the blanket connectivity exclusion in CIP-002, CenterPoint Energy recommends that significant consideration be given to each requirement to be applied in Medium Impact Facilities that do not have External Routable Connectivity. CenterPoint Energy supports the efforts to enhance security and minimize recently identified vulnerabilities (ex. Stuxnet). Several changes made since the last formal comment period have addressed some concerns; however, there are a few requirements for which applicability should still be addressed. CenterPoint Energy has made specific subsequent comments per Standard.
Yes
Yes
Yes
Yes
Yes
Yes
CenterPoint Energy recommends that the phrase, “in sufficient detail” be removed from the Guidelines and Technical Basis as it is subjective. CenterPoint Energy also notes that Account Management under Personnel Security appears to be out of place and recommends that the topic be moved under System Security. Under Electronic Security Perimeters, the topic, “Organization stance on use of wireless networks” is not in the Standards/Requirements. CenterPoint Energy proposes that this topic be removed to better align with the Standards/Requirements. Under Remote Access, the topic “Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access” is also not in the Standards/ Requirements. CenterPoint Energy recommends that the topic be removed. The phrase, “For vendors, contractors, or consultants: include language in

contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls" is not in Standards/Requirements and should also be removed. Under Provisions for CIP Exceptional Circumstances, "Processes to allow for exceptions to policy that do not violate CIP requirements" is Contradictory to the CIP Exceptional Circumstance definition. CenterPoint Energy also prefers removal or an alternative to the word, "violate", be used.
Individual
James TUcker
Deseret Power
Yes
Yes
4.2.1 and 4.2.2, and Attachment 1, 2.10 – The threshold for 300 MW of UFLS or UVLS load shedding is clear, but saying "that are part of a Load shedding program" implies that an entity could have only 50 MW of load that will be shed as part of a larger 300 MW "program" and be drawn into the applicability and required to comply with the Medium Impact facility requirements. Another scenario is where a DP with a 250 MW load shedding program not associated with any other group would not come into applicability at all. DESERET POWER recommends that the SDT provide guidance with very clear examples of scenarios that would include or exclude DP or LSE entities from required compliance with CIP Version 5 standards. Under the inclusion threshold for DP, 4.2.2, third bullet, states: "A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard." DESERET POWER recommends that the following language be added to the end of that bullet; ", and where the Protection System is connected to a supervisory control system providing remote operation capability." This language will help to further appropriately clarify the scope of applicable Protection Systems in the CIP standards. Attachment 1 2.10 – see comment above 2.11 – The 300 MW value should be revised to 1500 MW to properly align it with 2.1 in the Medium Category. The 300 MW value has not been adequately technically justified and the resulting potential compliance obligation actions and costs that could be required will likely far outweigh the reliability benefit of keeping the 300 MW value in this section. If the change to 1500 MW is made, then all other Control Centers, and associated data centers, not included in the High or Medium Category will be included in the Low Category. This is a major issue for DESERET POWER. It will be difficult to support CIP-002-5 without this revision.
Yes
No
Yes
Yes
Yes
Yes
R2 – DESERET POWER is concerned that even though it is stated that a list of Low Category assets is not required for compliance, we do not see how compliance could be proven/demonstrated without such a list. Given that the requirements for Low Category assets are intended to be programmatic in nature, and not asset specific, DESERET POWER requests that the SDT make changes necessary to not in effect require a list of Low Category assets to demonstrate compliance.
Individual
Warren Rust
Colorado Springs Utilities
Yes
Yes
Colorado Springs Utilities appreciates the energy the SDT has had to expend to this point as well as this opportunity to continue to comment on this evolving draft standard. CSU is also grateful for the thoughtful comments of others and agrees with comments submitted by SMUD, AECI & SNPD regarding CIP-002-5, Appendix 1; to wit: Criterion 2.5: The summation of actual MVA ratings for each circuit should be the measure to determine Medium Impact Rating (M) for Transmission facilities where three or more connections to other Transmission stations or substations. Assessment utilizing the MVA threshold better aligns with other NERC Reliability Standards' criteria for system impact and is a better measure to determine Medium Impact Rating of Transmission facilities. [original comment

SMUD] [SNPD] disagrees with the CIP-002-5, 2.11 as it dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria ("SCRC"), section III (d), address the Transmission Owner ("TO")/Transmission Operator ("TOP") uses the same criteria to define both TO and TOPs. However, the application of what entities registers or is required to register as a Transmission Owner and not as a TOP is not defined and is not consistent though regions or North America. SNPD supports removing section 2.11 as there is no "reliability based" justification that registration as TOP justifies a Medium Impact Rating. [or consider AECI's recommendation, below] [AECI] is ... proposing several changes to CIP-002-5, Appendix 1, pp 17 & 18, parts 1.2, 1.3, & 1.4, 2.10, and 2.11, in order to resolve technical discrepancies in MW impacts, and in particular deal with part 2.11's implication that any BA or TOP of any size is at least a Medium Impact, as well as the part 2.11 implication that any 300 MW has Medium Impact upon the BES, which is simply not the case. Therefore, AECI suggests revising the Bright-lines for High Impact from 1500 to 3000 MW and controlling two or more elements. The Bright-lines for Medium Impact would be 1500 MW and controlling one or more elements. This will provide a more well-defined difference between High and Medium. In addition, part 2.10 changes deal with the same 300 MW impact issue, in addressing centralized UVLS and UFLS system size and impact, necessarily differentiating the two. AECI recommends changing 2.10 as described below. All changes are summarized below. CIP-002-5, Appendix 1, p 17, part 1.2 Replace: 1500 MW With: 3000 MW Replace: "one or more" With: "two or more" Rationale: Assess High Impact to twice that of Medium Impact potential CIP-002-5, Appendix 1, p 17, part 1.3 Replace: "one or more" With: "two or more" Rationale: Assess High Impact to twice that of Medium Impact potential CIP-002-5, Appendix 1, p 17, part 1.4 Replace: 1500 MW With: 3000 MW Replace: "one or more" With: "two or more" Rationale: Assess High Impact to twice that of Medium Impact potential CIP-002-5, Appendix 1, p17, part 2.10 Replace: "of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) " With: "of 800 MW or more implementing Under Voltage Load Shedding (UVLS) or implementing Under Frequency Load Shedding (UFLS) within a single Interconnection in excess of thresholds in Table X (Derived once from 5%-droop for peak Interconnection load 2012, constrained to 5% error) Table X Interconnection UFLS Peak MW Threshold Eastern 1500 MW (cap on computed value of 4144 MW) Western 1400 MW (computed value was 1437 MW) ERCOT 750 MW (computed value was 772 MW) QUEBEC 300 MW (computed value was 310 MW)" Rationale: 1) Assess threshold for UVLS, no greater than a single large 800 MWnet coal-fired plant, because UVLS impacts are more localized and so a commiserate threshold is prudent in order to avoid cascading outages. 2) Assess UFLS Medium impact MW threshold level commiserate with Interconnection impacts, where no more than 5% of an Interconnection's droop-characteristic governor-responses from nominal frequency to first-step UFLS relays per PRC-006 is allowed be risked within a centralized UFLS. However, the corresponding guidelines should note that, should an Entity's centralized UFLS system fail, they could individually be assessed a Severe VSL for under-performance, and their RC be assessed greater than Low VSL for their aggregate failure to perform per current VSLs for Requirement 9 of PRC-006-1, page 13. (While this 5% margin agrees with PRC-006 Low Violation Severity Level for Interconnection Impacts, that Entity's business risk of violation due to their UFLS system's failure, could be enormous under NERC Standard PRC-006.) CIP-002-5, Appendix 1, p 17, part 2.11 Replace: "(1) perform the functional obligations of Balancing Authority or Transmission Operator, or (2) control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 300 MW or more of BES generation." With: "(1) perform the functional obligations of Balancing Authority or Generation Operator, and control an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW or more of BES generation, or (2) perform the functional obligations of the Transmission Operator, that includes control of one or more of the assets that meet criteria 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10. Rationale: Align Medium impact Medium impact 1500 MW or Asset amounts. (And see AECI recommendations for Parts 1.2..1.4 High impact ratings.)
Yes
Yes
Yes
Yes

Yes
Yes
Group
Tri-State G&T - Transmission
Tracy Sliman
No
Yes
Increase threshold for High Impact from 1500 to 3000 and increase threshold for Medium Impact from 300 to 1500.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Seattle City Light
Pawel Krupa
General Comments: SCL does not support the approach proposed in version 5 of the CIP Standards, either as to fundamentals or details. Fundamentally SCL believes the v5 approach is flawed and will introduce significant compliance burden without ensuring cyber security for the BES. Detailed concerns remain as provided previously (please refer to comments submitted by SCL on January 6, 2012). Although today's enforcable CIP Standards share many of the flaws of v5, SCL believes industry would be better served by developing maturity around the existing Standards while developing a new, different approach to cyber security that is based on the established practices and theory of the information technology industry.
Individual
Steve Alexanderson
Central Lincoln
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
Yes
Yes
Yes
Yes
1. Thank you for consolidating the low impact requirements. 2. We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Individual

Oscar Alvarez
Los Angeles Department of Water and Power
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Yes
Yes
Yes
Yes
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Individual
John Tolo
Tucson Electric Power
Yes
Yes
The wording in Appendix 1. Criteria 2.3, where commas were added before and after “as necessary”, is unusual and seems to add confusion. The commas weren’t there in Draft 1 or Version 4’s attachment. Suggest removing the commas surrounding as necessary. TEPC agrees with EEI’s comment to CIP-002 regarding wording of facilities and clarifying the approach “Facilities, Systems, and equipment”.
Yes
Yes
No
Yes
No
No
R3, R5, and R6: Agree with EEI comment: Move R6 content applicable to R3 and R5 and remove R6 requirement, which will eliminate ‘double jeopardy’ concerns. Suggested language for R3: Each Responsible Entity shall identify a CIP Senior Manager by name, and document any change within 30 days. Suggested language for R5: Add applicable section of R6 to this requirement – “Delegation changes do not need to be reinstated with a change to the delegator.” Remove R6.
Individual
Russell A. Noble
Cowlitz County PUD
No
Yes
Cowlitz agrees with comments submitted by APPA, and in addition adds emphasis regarding the applicability section 4.2.2, second and third bullets where the verbiage “is required by a NERC or Regional Reliability Standard” is used. This implies that a Reliability Standard may be written to require the installation of equipment. This violates the statutory limitations established in regard to Reliability Standard development which “…does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Rather, it appears the SDT intent was to point to standards which followed the statutory allowance to write requirements governing “the design of planned additions or modification to such facilities.” However, such a Standard applicability would be vague and difficult to track. Cowlitz strongly advises that section 4.2.2 be revised such that it stands on its own, and does not require a general search through all the Reliability Standards to establish applicability.
Yes
Yes

No
No
No
No
Please refer to the comments submitted by APPA.
Group
PacifiCorp
Sandra Shaffer
No
No
• PacifiCorp supports the EEI consensus comments in general for item no. 3, but specifically endorses the approach to CIP-002-5 set forth in the alternate draft CIP-002-5 presented byproposal of MEC and -Alliant. PacifiCorp has consistently advocated this kind of approach from the first distribution of the Version No. 5 draft standards. The SDT has made minor stepincremental changes in response to industry comments on the framework of CIP-002-5, but has not made the wholesale structural change to the framework of CIP-002-5 that needs to be made to render the vital process of identifying the assets to be regulated under the standards simple and straightforward. PacifiCorp shares the industry opinion that the suite of Version No. 5 standards cannot and should not be supported by the industry until the fundamental problems with CIP-002-5 are corrected. PacifiCorp strongly recommends that the alternate CIP-002-5 be adopted in lieu of the current SDT draft, and that SDT efforts be re-directed at refining and improving the alternate approach. Comments on MidAmerican-Alliant Version---- The Requirement/Measurement language presented in the MEC-Alliant version of CIP-002 is easy to interpret and eliminates . The straight forward criteria will eliminate confusion for auditing efforts. • PacifiCorp agrees with the industry consensus provided in EEI's comments that external connectivity needs to be taken into much greater consideration in the suite of standards. The problem with including a qualifier in every requirement where connectivity is an issue is that this approach does not create any clean, bright lines of applicability, and only increases the complexity of the standards (requiring separate tracking for every asset that requires different treatment under the standards). The solution is to establish a bright line (between Medium and High impact rating facilities/assets) at a higher structural level in the standards. While PacifiCorp still believes that an "external connectivity" requirement should be universally applied to all regulated cyber assets, PacifiCorp is much more persuaded that it is particularly important to protect cyber assets in a High impact rating facility, regardless of whether those assets have/use external connectivity or not. But this is not true for cyber assets associated with Medium or Low impact rating facilities. Implementation of this bright line could be fairly simply accomplished by adding the following two sentences to the end of the definition of BES Cyber Asset: o "Unless integrated into a BES Cyber System that qualifies as a "High Impact Rating" BES Cyber System, a Cyber Asset is not considered a BES Cyber Asset unless it [uses/enables] external connectivity functionality (via either routable or dialup connectivity). All Cyber Assets integrated into BES Cyber Systems which have been designated as "High Impact Rating" BES Cyber Systems are automatically deemed to be BES Cyber Assets, regardless of whether they [use/enable] external connectivity or not." Any areas that dictate an exception to this bright line rule could then be addressed as a true exceptions, rather than the current situation where external connectivity is addressed in every requirement and sub-requirement that has a direct impact on a regulated cyber asset. • Another important issue that needs to be addressed is the proliferation of zero defect standards that impose large administrative burdens with no commensurate protections to the bulk electric system. nclusion is the "…detect flaws expeditiously;.." clause. 100% compliance is an untenable position in many instances throughout the suite of draft standards (including CIP-002-5), and creates an unreasonable burden on both entities and auditing bodies with no clear improvement in reliability. Utilities Responsible entities must be afforded the ability to manage business concerns that do not materially impact reliability within normal operational practices. PacifiCorp supports the various EEI consensus comments and specific language suggested in the alternate CIP-002-5 proposal of MEC and -Alliant alternate CIP-002-5 that eliminates administrative violations where flaws have been detected and corrected expeditiously.
Response to #1 • The process flow is a significant improvement over the last version (generally moving from analysis of the general to the specific), but the draft published by the SDT still clings to the erroneous view that BES Cyber Assets/BES Cyber Systems can exist independent of Facilities.

PacifiCorp strongly supports the alternate version of CIP-002 put forth by MidAmerican Energy Company (“MEC”)/Alliant, as such version presents a much clearer approach to the identification of high and medium impact BES assets. PacifiCorp believes that the industry and the drafting effort will be much better served by adopting and refining the alternate version of CIP-002-5 proposed by MEC-Alliant. See comments below in response to #3. • Facilities need to be categorized first (High, Medium and Low), and then the associated BES Cyber Assets and BES Cyber Systems, as is done in the current version of the standard and the MEC-Alliant proposed alternate version of CIP-002-5. • While the process steps in the current version of CIP-002 appear to move from general to specific, the substance of the defined terms that are used in the process steps (trying to ferret out BES Cyber Assets/Systems independent of BES Facilities) has the registered entity bouncing back and forth between the general and the specific, rendering the initial fundamental process of identifying assets to be regulated convoluted and confusing. • The term “BES Elements” needs to be eliminated from R1.4. Since Low BES Cyber Systems (BES Elements) are not discretely identified (and rightly so because it would be a waste of resources to track things on such an insignificant level), changes to those BES Elements are not discretely tracked either (making R1.4 impossible both to comply with and to audit since most relevant changes will be from a Low to a Medium category). Changes to Facilities which would move the Facility from a Low to a Medium category can and should be tracked. It is much more relevant to talk about changes that result in a significant change to a Facility than to changes to the Elements of a Facility. The Elements (BES Cyber Assets/Systems) are automatically re-categorized by association with the Facility when a change is implemented at the Facility level. • The process flow is a significant improvement over the last version (generally moving from analysis of the general to the specific), but the draft published by the SDT still clings to the erroneous view that BES Cyber Assets/BES Cyber Systems can exist independent of Facilities. PacifiCorp strongly supports the alternate version of CIP-002 put forth by MidAmerican Energy Company (“MEC”)/Alliant, as such version presents a much clearer approach to the identification of high and medium impact BES assets. PacifiCorp believes that the industry and the drafting effort will be much better served by adopting and refining the alternate version of CIP-002-5 proposed by MEC-Alliant. See comments below in response to #3. • Facilities need to be categorized first (High, Medium and Low), and then the associated BES Cyber Assets and BES Cyber Systems, as is done in the current version of the standard and the MEC-Alliant proposed alternate version of CIP-002-5. • While the process steps in the current version of CIP-002 appear to move from general to specific, the substance of the defined terms that are used in the process steps (trying to ferret out BES Cyber Assets/Systems independent of BES Facilities) has the registered entity bouncing back and forth between the general and the specific, rendering the initial fundamental process of identifying assets to be regulated convoluted and confusing. • The term “BES Elements” needs to be eliminated from R1.4. Since Low BES Cyber Systems (BES Elements) are not discretely identified (and rightly so because it would be a waste of resources to track things on such an insignificant level), changes to those BES Elements are not discretely tracked either (making R1.4 impossible both to comply with and to audit since most relevant changes will be from a Low to a Medium category). Changes to Facilities which would move the Facility from a Low to a Medium category can and should be tracked. It is much more relevant to talk about changes that result in a significant change to a Facility than to changes to the Elements of a Facility. The Elements (BES Cyber Assets/Systems) are automatically re-categorized by association with the Facility when a change is implemented at the Facility level. Response to #2 An annual period for this requirement is sufficient and adding the “not to exceed 15 calendar months” requirement is not warranted. There are many very good reasons that the timing of an entity’s annual review and assessment of its assets needs to be shifted or scheduled outside of a 15- month window from the last review. This requirement adds a layer of administrative compliance that is not supported by a reciprocal improvement to the reliability of the Bulk electric System.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
No

No
No
No
Yes
Yes
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Group
Puget Sound Energy, Inc.
Tom Flynn
Yes
Yes
None
Yes
Yes
Yes
Yes
Yes
Yes
Group
PNM Resources
Michael Mertz
No
Yes
See comment submission from EEI.
No
Yes
Yes
Yes
Yes
Yes
See comment submission from EEI.
Individual
Darcy O'Connell
California ISO
Yes
Yes
Yes
No
No
No
No
CIP-003 R3 we agree with the requirement but have issues with the definition of a CIP Senior Manager in that the definition should include the operation and maintenance of the requirements (ongoing compliance). Looking at the definition of a CIP Senior Manager it appears that the after the requirements are implemented, according to the implementation plan, that there is no longer a need

for a “CIP Senior Manager”. This appears to contradict what is required in CIP-003. CIP-003 R4 M4 item 2 change the words “dated signature” to “dated approval” for better alignment with the requirement. CIP-003-5 R5 M5 change the word “signed” to “approved” for better alignment with the requirement. CIP-003 R6 M6 needs to be reworded and clarified.
Individual
Martin Bauer
US Bureau of Reclamation
No
Yes
1. Add another categorization level of “Minimal Impact” BES Cyber Systems which are not included in high impact, medium impact, or low impact shall default to the category of minimal impact, which includes small control centers that control an aggregate highest rated net Real Power capability of the preceding 12 calendar months ranging from 300 to 700 MW of BES generation and Blackstart resources and generators rated below 75 MVA. Minimal impact facilities do not require further consideration. 2. Section “Categorization Criteria” Change third sentence to read “All BES Cyber Systems or Facilities not included in Attachment 1 – Impact Rating Criteria, Parts 1.1 to 1.4 and Parts 2.1 to 2.11 defaults to be low impact and do not require discrete identification; or minimal impact and do not require further consideration.” Change Section 3.2 to read Blackstart Resources rated at 75 MVA or greater. 3.3 Elements in the cranking path of black start resources rated 75 MVA or greater and initial switching requirements. (Rationale: If the BES impact rating is “minimal” then no further consideration should be required, including any associated access protection system requirements. Small control centers that control and Blackstart resources/generators rated below 75 MVA would be included in the “minimal impact” category, thus reducing costs/resource burdens for smaller facilities, and the likelihood of entities removing Blackstart resources from restoration plans.
Yes
Yes
Yes
Yes
Yes
Yes
Group
Hydro One
Sasa Maljukan
No
Yes
Yes
Yes
Yes
Yes
No
Yes
Recommend changing R5 from “sign” to “approval” since some companies use other approval processes. Also these Measures criteria to align with Requirement. This Measure includes “to approve or authorize specifically identified items” while the Requirement states “and approved by the CIP Senior Manager” Request a re-written M6 since it appears to add a new Requirement – “that within 30 days of discharging the delegated authority” Recommend updating CIP-003 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R2 as “low”