Individual or group. (99 Responses)

Name (68 Responses)

Organization (68 Responses)

Group Name (31 Responses)

Lead Contact (31 Responses)

Question 1 (76 Responses)

Question 1 Comments (83 Responses)

Question 2 (71 Responses)

Question 2 Comments (83 Responses)

Question 3 (70 Responses)

Question 3 Comments (83 Responses)

Question 4 (68 Responses)

Question 4 Comments (83 Responses)

Question 5 (72 Responses)

Question 5 Comments (83 Responses)

Question 6 (72 Responses)

Question 6 Comments (83 Responses)

Question 7 (42 Responses)

Question 7 Comments (83 Responses)

Question 8 (73 Responses)

Question 8 Comments (83 Responses)

Individual
mike albosta
Phillips 66
No
No problem with 2.1, 2.2, 2.3 2.4 - Requiring the user to give a "reason" for accessing does nothing to increase security and would require a rewrite of the system. 2.5 - We just wrote an Incident Response Plan for EOP-004-2 that would cover cyber incidents. This is redundant and more work. 2.6 - ditto. And quarterly is ridiculous. And you don't define "practices" or what "reinforce" means.
Group
FirstEnergy
Cindy Stewart
Yes
FirstEnergy supports the revisions to the CIP standard in general. Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does have concerns around the RSAWs and support EEIs comments in regards to the RSAWs.
Yes
FirstEnergy supports the revisions to the CIP standard in general. However in the Guidelines and Technical Basis, FirstEnergy requests the addition of a clarification that entities are not expected to enforce CIP-006 on third party components that are out of the entity’s control. FirstEnergy also has concerns around the RSAWs and support EEIs comments in regards to the RSAWs.
No

FirstEnergy does not agree with this approach. Suggest the requirements for Transient Cyber Assets & Removable Media Protection be an additional requirement under CIP-007 as these devices require similar protection (i.e. malicious code prevention, security patching) as those applicable systems in CIP-007. As currently placed, Transient Cyber Assets & Removable Media have little in common with Configuration Change Management and Vulnerability Assessments creating confusion in internal programs, SMEs and RSAWs.
Yes
Yes
Yes
No
None known
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does have concerns around the RSAWs and support EEIs comments in regards to the RSAWs.
Individual
Greg Froehling
Rayburn Country Electrical Cooperative
No
The proposed version provides adequate specificity relative to the strategies required. E.g. “restrict physical access”. The concern I pose, comes with the subjective nature of the enforcement review. Does the standard sufficiently cover the appropriate levels and tactics expected to be used to be compliant. (is locking the door enough?) However this COULD be addressed with a sufficiently detailed technical guidance document much like the style of the PRC-005 Technical Guidance Document. Next Section 2.5 needs some language clarification; two intervals are mentioned, quarterly and 15 calendar months. However there is some ambiguity surrounding what is to be done on those intervals. A suggested wording / format revision to clarify. Implement a security awareness program that: •Reinforces good cyber security practices at least quarterly. In addition. •Specifically cover Parts 2.2, 2.3, and 2.4 above, once every 15 calendar months.
No Comment
No Comment
Yes
The timeline for CIP-003-6 R2 should be sufficient. But I point out that the implementation plan does not address newly identified "Low" BES Cyber Assets. The situation could occur for some distribution assets that were not applicable at the time this standard was approved, at a later date rising to the applicability levels and as such needing to implement the "Low" requirements.
Yes
Items for the FAQ document produced by the drafting team. •Suggested approaches for compliance that address the topics in CIP-003-6, Requirement R2, and Parts 2.2 – 2.5. (See PRC-005 Technical guidance document for level of specificity.) •What levels of restrictions for physical access are expected to be performed? (Switchyard/ Substations, Generation facilities and areas within those facilities…) •Explore issues around “2.3.3 Authentication when establishing Dial-up Connectivity, per Cyber Asset capability. The documentation of the capability and or suggested approaches to establishing authentication. •Address implementation period for newly identified LOW BES Cyber Assets, currently there is NONE! •Discuss “Guilt by association” example: a substation classified by entity A as “Medium” has Protection Systems (BES Cyber System) that rely on Entity B’s substation Protection Systems, does this potential Reliability Operating Service provided by Entity B make the Entity B’s station a Medium or not? •Also explore the situation above where Entity B’s substation is a

non BES station. Does this scenario extend to those connected to "Low" substations? For CIP-003 R2, I propose the original 2 years from regulatory approval as it was originally with version 5 since it has taken longer than 3 months from V5 FERC Approval till now. More time is needed due to: •The objective criteria and the specific nature of the processes or program required for these proposed revisions that did not exist prior to now. •Entities are not only required to “develop them”. •Entities must demonstrate they have “implemented them” Please address implementation period for newly identified LOW BES cyber assets. Currently this is a situation that can arise, and without an implementation period being identified it can pose some difficult situations.
Individual
Debra Horvath
Portland General Electric
Yes
Yes
Yes
Yes
No
PGE is concerned about the removal of the ‘identify, assess, and correct’ language from the CIP Version 5 standards. The inclusion of this language in the CIP Version 5 standards was a large part of the reason that the industry voted to pass the standards in the first place. The intention of the IAC language was to address the standards being ‘zero defect’, an intention which FERC supported in order 791. ‘Zero defect’ standards cause undue burden and harm on the industry without supplying a meaningful reliability or security benefit. Rather than remove the IAC language entirely, it would be worthwhile to modify the language to add a qualitative aspect that would be responsive to FERC’s concern that the language is too vague. PGE understands that the Reliability Assurance Initiative may be used to address “zero defect” but its effectiveness remains to be seen. It is preferable to include language within the CIP Version 5 standards to address “zero defect”.
Yes
Yes
Yes
Group
CenterPoint Energy
John Brockhan
No
R2/M2 - Although CenterPoint Energy generally agrees with the approach to meeting the CIP-003 directive, one requirement for low impact assets with objective criteria, the Company questions the deletion of the link back to CIP-002-5, Requirement R1, Part R1.3. The Company recommends the following wording: “Each Responsible Entity for its assets identified in CIP-002-5 Requirement R1, Part 1.3 shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets.”. (The phrase “containing low impact BES Cyber Systems” is not needed as it should be understood after asset identification in CIP-002-5.) CenterPoint Energy also recommends that M2 be revised to reflect the pattern of the other measures in CIP-003. For example, the following wording would be appropriate: “Examples of evidence may include, but are not limited to, applicable documented policies and processes that collectively include each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets and additional evidence to demonstrate implementation as describe in the Measures column of the table.” Alternatively, the SDT may consider the pattern found in other Standards (ex. CIP-007-5/6) and remove the word “any” from the draft measure.

Part 2.4.3 - CenterPoint Energy also requests that the SDT review and consider the use of the term “authentication” versus “access control” in Part 2.4.3 and the supporting Guidelines and Technical Basis. Does the SDT intend for entities to have authentication or access control when establishing Dial-up Connectivity? Although this requirement is to be implemented “per Cyber Asset capability”, CenterPoint Energy proposes that access control is more appropriate and commonly feasible. Part 2.6 - The level of detail in Part 2.6 is above what is required even for High and Medium Impact BES Cyber Systems. CenterPoint Energy recommends that Part 2.6 be revised as follows: “Implement a security awareness program that reinforces cyber security practices (which may include associated physical security practices) at least quarterly.”. Delete the sentence “Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.”.
Yes
No
CenterPoint Energy acknowledges the risks associated with transient devices; however, the Company is concerned with management and documentation to be associated with the requirements for transient devices. CenterPoint Energy considers sustained compliance with the requirements exceptionally challenging or unattainable. CenterPoint Energy also recommends that the examples statement be removed from the Guidelines and Technical Basis on Page 41 – Requirement R4 as it is redundant to the definitions of Transient Cyber Assets and Removable Media.
Yes
Yes
CenterPoint Energy supports this revision approach for IAC. As proposed by NERC, the Company looks forward to the concepts of IAC being implemented within the final framework of the Reliability Assurance Initiative (RAI).
No
The timeframe for CIP-010-2, Requirement R4 is not appropriate. Efforts will be focused on the implementation of CIP Version 5 (High and Medium Impact Assets) through April 1, 2016. After that date, entities will have 1 year to document and implement requirements for Low Impact Assets. Although comprehensive efforts toward CIP Version 5 and the potential of CIP Version 6 compliance are occurring to date, CenterPoint Energy recommends that Registered Entities not be required to comply with Reliability Standard CIP-010-2, Requirement R4 until at least 1 year after the effective date of Reliability Standard CIP-010-2 as it, along with CIP-003-2, is the most complex of the CIP Version 5 revisions.
Group
Arizona Public Service Co
Janet Smith
Yes
Yes
Yes
Yes
Yes
Yes
This is not applicable to AZPS as an entity

No
Group
Northeast Power Coordinating Council
Guy Zito
No
We recommend common control objectives. Language inconsistencies create confusion and compliance risks. Here are some examples: Example 1 – Request a definition (CIP-003-6 Rationale R2 and Part 2.4) of “external routable protocol paths” so that Entities and Auditors clearly understand the differences with External Routable Connectivity. We recommend avoiding the earlier CIP-001 confusion between Facilities and facilities. We believe “external routable protocol paths” creates a similar interpretation risk. Example 2 – security awareness (Part 2.6) is more stringent than the High / Medium in CIP-004-6 R1 Example 3 - the Low Incident Response Plan in Part 2.5 is inconsistent with High / Medium Incident Response Plan in CIP-008-5 R2 Example 4 – policy requirements for Low Impact creates different set of Requirements for Entities with Low, Medium or High. There are inconsistencies in the language of this requirement, which causes confusion to entities. Why is LOW impact rating requirements addressed in this standard versus in the applicable standards such as for High & Medium impact ratings? Example: the security awareness should be addressed in CIP 004 as it is for High & Medium. Whether the all-in-one requirement approach or the spreading out into all the standards approach is taken, the most important thing is that there is consistency between the standards and requirements and maintaining the tiering of activities to the risk.
Yes
Request CIP-007 R1 Part 1.2 Rationale be added to the Guidelines and Technical Basis section. Suggest illustrative examples be included in the Measures and Technical Guidelines so that entities and auditors have the same interpretation.
Yes
Yes
Yes
How does NERC intend to address an internal controls program? What is the time line? Refer to the comment for Question 8.
No
Request a clear, concise table of all proposed Implementation Plan updates. Ensure that all new effective and mandatory dates are after their CIP V5 dates. The current format is confusing. Please provide a clear and consistent time line for implementation of these requirements.
No
Yes
More clarity and scenarios should be provided on how RAI and CIP will work together. The NERC Project 2014-02 CIP Version 5 Revisions Standard Drafting Team should be allowed to help clarify and provide guidance for industry issues and items discovered in the pilots. In particular the following should be addressed by NERC with the SDT representing industry: 1. Transfer Trip: CIP-002-5 R1, ‘transmission stations and substations’ for medium category assets, what some refer to as the “transfer trip” issue. 2. Clarify the term “programmable devices” which is an undefined term open to strongly differing viewpoints. 3. Clarify “effect within 15 minutes” issue and the burden of evidence for proving that something does not exist. Please clarify if diversity vs redundancy can be considered as part of the Entity’s impact assessment (i.e. separate system using a different technology). Recommend adding “or” to CIP-010 R4 Part 4.1.4 to make this Part consistent with CIP-010 R1 Part1.1.1.1. Part 1.1.1 requires a baseline of Operating system(s) (including version) OR firmware where no independent operating system exists; while Part 4.1.4 requires Authorization to include Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability). Part 4.1.4 requires Authorization of both Operating System AND

Firmware for a transient device while Part 1.1.1 requires baseline of Operating System OR firmware. We suggest the proper approach is to retain the OR. When applying R4 to a laptop we normally record the OS and version and not look to the firmware BIOS.
Group
ACES Memebers
Warren Cross
No
In regards to the requirement for physical security (R2.2), the requirement is partially focused on whether one or more processes is documented to restrict physical access. The requirement and measures should be focus on the effectiveness with specific physical access restriction criteria instead of a documented process. Would an entity have to document their processes for each asset if the means of restriction are different? If so, this effort to document each process for each location for each asset would be burdensome and ineffective in restricting physical access.
Yes
Yes
Yes
We are supportive of the approach as long as the Reliability Assurance Initiative is fully implemented by the effective date of these standards.
Yes
We are supportive of the approach as long as the Reliability Assurance Initiative is fully implemented by the effective date of these standards.
Yes
No
No
Group
Pacific Gas and Electric
John Hagen
No
The Requirements proposed in 2.1, 2.2 and 2.3 are sound and apportion appropriate controls for Low Impact Cyber Systems. However, the “external routable protocol paths” language in Requirement 2.4 requires entities Low Impact Cyber Systems to provide and comply with “some form of electronic security perimeter,” regardless of risk to the Bulk Power System/Bulk Electric System. In addition, the language in the context of a CIP program is confusing. On one hand, entities would be required to identify, maintain and comply with “some form of electronic security perimeter” (ESP) for Low Impact rated BES Cyber Systems, yet on the other, CIP Version 5 (or the proposed Revisions) states that “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” This is contradictive at best and should be clarified. And while it is understood that one consideration for this language is a scenario where a Low Impact Cyber System could potentially be compromised and/or utilized to compromise or misuse Medium or High rated Cyber Systems; this should be alleviated considering that Low, Medium and High BES Cyber Systems are inherently designed, deployed and operated with existing physical and electronic controls to deter this. Recommend language changes to address only Low Impact Systems which have direct access to “untrusted” networks (e.g. networks not owned and operated by the entity). Recommend adding language to address Low Impact BES Cyber Systems with “external routable protocol paths” and depending on the path and number of paths, determine the controls such as monitor and control communications, implementation of subnets, and manage external connections using boundary protection devices. Recommend the performance of an annual sampling assessment of such classified systems to determine the state of their security controls.

This sampling could be based on the NERC sampling guidelines or other generally accepted audit principles for security controls with established levels of materiality to provide a threshold or cut-off point.
Yes
Implementing physically secured cabling and alarms to components outside of PSP is an appropriate approach. Also, Part 1.10 mandates an alarm or alert to personnel with 15 minutes of detection. However Part 1.10 does not define timeframe that alert or alarm must be respond to or be investigated by personnel to determine if/how/where breach was attempted. Also recommend that periodic review of the integrity of the implemented physical protection measures and alarm processes remain intact as design and approved as part of CIP Senior Manager sign-off.
No
CIP-010-6 R4.1.4 requires the Entity to “identify and document the Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).” And in 4.6, the Entity is required to “Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4.” For entities that depend on vendors and contract support personnel to maintain the Reliability of the Bulk Electric System, this becomes a great administrative challenge. This requirement becomes dependent upon the number of Transient Devices, the number of vendors, contractors or support personnel, and the type and variance of Transient Cyber Assets and tools used to perform their job duties. The challenge in requiring a baseline of firmware alone far exceeds the vulnerably and risk to the BES Cyber Asset. Recommend changing the language in requirements R4.1.4 and R4.6 to address Entity owned-maintained Transient Devices separately from Vendor or Contracted Support owned-maintained Transient Devices. This allows entities to reasonably develop and implement Administrative and Technical Security Controls for Transient Devices based on risk, yet monitored from a compliance standpoint. Recommend language changes to require “the implementation of a Transient Device Security Baseline for Entity and Vendor/Contracted Support Transient Devices.” This allows Entities to implement controls yet maintain the flexibility to address multiple device types and functions. This also allows Entities and their vendors or contracted support personnel to implement Administrative and Technical controls of Transient Devices based on risk. Recommend language changes to require sampling of Transient Devices Security Baseline. This allows Entities a mechanism for monitoring both Entity and Vendor/Contracted Support personnel owned-maintained Transient Devices. Recommend language changes to require a security policy for Transient Devices which includes a requirement for Transient Devices with direct access to BES Cyber Systems. This allows Entities to establish and implement Administrative Controls for Transient Devices as well as recommend Technical Security Controls in the form of Transient Device Access Portals. Recommend consider a standardized implementation of a Transient Device Security Access Portal which allows vendors to perform their work without directly accessing systems. This would allow Entities Vendors, Contractors and support personnel to use a standardized and document attestation of security baseline for Transient Cyber Assets. Recommend leveraging the NERC Guidance for Secure Interactive Remote Access jump hosts concept for transient devices with remote access capabilities.
Yes
The new definition for Transient Cyber Assets and Removable Media is an appropriate revised definition. However, there may be an issue with scope of applicability related to the 15 minute parameter classification of High BES Cyber Asset and Protected Cyber Assets. The new R4 approach should be required across all components contained within the ESP regardless of classification. Also, it is stated under Requirement "4.1 Authorization shall include 4.1.1 Users, individually or by group/role:". Recommend that authorization should always note individual user and removing "by group/role".
No
The intent to removing the specific 17 requirements related to the "Identify, Assess, and Correct (IAC)" language was to shift focus from addressing specific types of incidents to implementing better practices in identifying risks. This shift may present responsible entity with overly-vague, unclear or not detailed enough scope or definition, compliance obligations, timeframes and requirements resulting in hard to develop and implement auditable processes. Recommend defining clearer requirements, scope definitions and obligations in the NERC Compliance Monitoring and Enforcement Program.

Yes
The existing effective dates for the mentioned standards appear reasonable and appropriate.
No
Yes
In the past references have been made regarding a need to protect High BES Cyber Systems from Electro Magnetic Pulse (EMP) related to solar or intentional anomalies. This has been an ongoing topic of discussion and concern however no direction, requirements, obligation or risk considerations have been made. Recommend providing guidance on whether EMP anomalies should be considered in risk assessments or policies and procedures.
Individual
Joe O'Brien on behalf of Jerry Freese
NIPSCO
No
Although we agree with EEI and the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. 4. Applicability The scope of dispersed generation in the CIP-003-6 Applicability section should be limited and similar to PRC-005. Suggested Revision: Under the Introduction section, 4 Applicability, 4.2 Facilities, add the following statement after 4.2.2 All BES Facilities: “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back the reference to CIP-002-5 Requirement R1.3 in CIP-003-6 R2. 6. Background With the addition of the table to Requirement R2, the Background Section should include a paragraph referencing the tables and the “Applicable Systems” Column to be consistent with the Background section of the other CIP standards with similar tables. Suggested Revision: Add the following paragraph after the first sentence of the CIP-003-6 Background Section 6: “Requirement R2 opens with, ‘Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets.’ The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.” Also, add a paragraph similar to the “‘Applicable Systems’ Columns in Tables:” from other CIP standards into the Background Section 6 for CIP-003-6 for Requirement R2. Requirement R2 Add back the reference to “for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3” to properly set the scope. Also, change the table reference to “CIP-003-6 Policies, Processes, Plans and Programs.” to match the proposed revision to the table title. Suggested Revision: Change R2 to: “Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.” Table Title for Requirement R2 The Table title for Requirement R2 “CIP-003-6 Table R2 – Low Impact Assets” does not match the format of the tables used in the other CIP standards, which focus on the requirements not the applicable systems. Suggested Revision: Change the R2 table title to: “CIP-003-6 Table R2 – Low Impact Asset Policies, Processes, Plans, and Programs” Requirement R2, Part 2.1 An entity may not have a low impact BES Cyber System at a Control Center (R2.3) and therefore R2, Part 2.3 is not applicable. Suggested Revision: Edit text to read “that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 -2.6.” Requirement R2, Subpart 2.4.1 Clarify that an external routable protocol path is “external” to the asset identified in CIP-002-5.1 R Requirement R1, Part 1.3 containing low impact BES Cyber Systems. Suggested Revision: Delete “external” and insert “to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems” such that 2.4.1 becomes: “All routable protocol paths to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems, if any, must be through one or more identified access point(s).” Requirement R2, Subpart 2.4.2 Remove “by default” as it implies

the use of a firewall, which limits access control options. For example, an entity could use access control lists on a router or switch to provide security for traffic control. However, routers and switches do not do this by default. This will allow entities more options on how to accomplish traffic control. Also, include a statement to allow documentation of access permissions individually or by group. Reasons for granting access are included in CIP-005-5 Requirement R1, Part 1.3 for high and medium impact BES Cyber Systems. Documentation for low impact assets individually or by group is consistent with the measure, but as in CIP-005-5 Requirement R1, Part 1.3 should be added to the standard. Suggested Revision: Remove “by default” and add “and document access permission reasons individually or by group” such that 2.4.2 becomes: “For each identified access point, if any, require inbound and outbound access permissions, deny all other access, and document access permission reasons individually or by group.” Requirement R2, Part 2.6 The specificity of what must be covered and having to track two time periods is more prescriptive than the requirements for medium and high impact BES Cyber Systems. The proposed revision uses language from the medium/high impact requirement (CIP-004-R1.1) with the time period adjusted to once every 15 calendar months to differentiate for the lower risk. Cyber security awareness can be addressed during annual training for employees and contractors in addition to other ongoing cyber security awareness communications. Suggested Revision: Remove the references to the subpart requirements as they may not apply to all entities and remove the quarterly requirement such that Part 2.6 becomes: “Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months.” Guidelines and Technical Basis Align the drawings and wording in the guidelines and technical basis with the requirement language.

Yes

(EEI Comments) Guidelines and Technical Basis Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity’s control.

No

We agree with the following EEI comments: Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. Requirement R4, Part 4.1 EEI members are concerned with unnecessary administrative burdens created by Part 4.1. For example, Authorization generally applies to users. A user of a Transient Cyber Asset should be authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. Suggested Revision: EEI does not have a specific revision to suggest to address these concerns; however, we recommend a careful review of the specific concerns and suggestions raised by Registered Entities to help reduce the administrative burden of this part. Requirement R4, Part 4.7 The requirement should be tied together better such that it clearly allows mitigation instead of patching, when justified. Suggested Revision: Condense the language into one sentence to help clarify the requirement. For example: “Evaluate Transient Cyber Assets, within 35 calendar days prior to use, for applicable security patches and take one of the following actions: • Apply the applicable patches, or • Create a dated mitigation plan, or • Revise an existing mitigation plan.” Guidelines and Technical Basis The Part 4.1 guidance conflicts with the “Applicable Systems”. The guidance says the requirement (R4) “applies to any transient devices”, yet the “applicable systems” in the requirements tables are not the transient devices. Suggested Revision: Edit the language under Requirement R4 to: “This Requirement applies to Transient Cyber Assets and Removable Media that will be connected temporarily to an applicable system. Examples of these hardware/software devices include, but are not limited to: • Diagnostic test equipment • Packet sniffers • Devices used for BES Cyber System maintenance • Devices uses for BES Cyber System configuration • Devices used to perform vulnerability assessments” The guidance for Requirement Part 4.1, says “Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets.” Requirement R4, Part 4.1 says “Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances.” (emphasis added) The guidance language

should be edited to be consistent with the standard’s requirement. Bullet 2, under Requirement Part 4.1, says “It may be reasonable to have separate Transient Cyber Assets for each impact level.” Requirement R4, Part 4.1 is focused on High and Medium Impact BES Cyber Systems, not all BES Cyber Systems. The language in bullet 2 includes “low impact,” which is not an applicable system for this requirement. Therefore the guidance goes beyond the scope of the standard. This guidance should also be edited to be consistent with the language of the standard’s requirement.
No
We agree with the following EEI comments: BES Cyber Asset – CIP-002.5.1 Guidelines and Technical Basis The definition of BES Cyber Asset combined with the guidance creates opportunities for misinterpretation. The scope of the reliability standards under Section 215 of the Federal Power Act is limited to “(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability.” (emphasis added) The BES Cyber Asset definition says “if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which , if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.” (emphasis added) The Guidelines and Technical Basis section of CIP-002-5.1 (guidance) goes to some length discussing the concept of BES Reliability Operating Services (ROS) as a tool to identify the BES Cyber Systems that would be in scope. What “affect” means is made unclear by this guidance. If we arbitrarily assume that “affect” means “unable to perform one or more BES ROS” then the loss of a programmable device which provides status and magnitude of breakers, current flows, etc. for “Monitoring and Control” and “Situational Awareness”, would be considered to be affecting the BES, and it would begin to do so immediately upon such loss. However, these devices are not necessary to operate “an interconnected electric energy transmission network” or “to maintain transmission system reliability.” Therefore, we do not think this is what the Standard Drafting Team intended, however clarification in the guidance, which aligns with the scope of a reliability standard is needed. Removable Media There is a consistency issue. The definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to; however, the definition for Removable Media is not. It can be implied that the definition refers to connection to applicable systems, but it is not clear. It would also be clearer to switch the order of the Removable Media and Cyber Assets in the last sentence. Suggested Revision: Change the definition of Removable Media to: “Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
Yes
We agree with the following EEI comments: EEI supports the removal of the identify, assess, and correct language due to the expectation that NERC will refine its compliance and enforcement process under the Reliability Assurance Initiative (RAI) to move away from a zero tolerance approach to compliance. We expect the new RAI to be finalized prior to final ballot to address the zero tolerance concerns that the identify, assess, and correct language intended to address.
Yes
No
not applicable
Yes
We agree with the following EEI comments: CIP-002-5.1, CIP-005-5 and CIP-008-5 were not opened for revisions, comments or ballot. These standards contain one or more items that need to be updated to maintain consistency with the CIP standards which were opened. There are also items which need to be addressed to provide clarity for implementation and auditability. We respectfully request that the Revisions Standard Drafting Team make these “conforming changes” and other changes to the three standards regardless of whether they are opened for any other revisions. Examples include: • CIP-002-5.1, CIP-005-5 and CIP-008-5 all, in section 5, reference effective dates. These all need to be updated to be consistent with the effective date of the standards which

were opened for revision. • CIP-005-5 and CIP-008-5, in section 6, reference CIP-003-5, CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5 and CIP-010-1 and CIP-011-1. These references need to be updated to reflect -6 and -2 as appropriate
Individual
Leonard Kula
Independent Electricity System Operator
Yes
The IESO agrees in general with the requirement approach. We do not believe this will affect the IESO as our assets will be considered High Impact.
Yes
The IESO agrees with the requirement approach.
Yes
The IESO agrees with the requirement approach.
Yes
The IESO agrees with the revised definitions.
Yes
The SWG agrees with the requirement approach.
Yes
The SWG agrees with the requirement approach.
No
The IESO is not aware of any provincial or other regulatory requirements that need to be considered at this time.
No
Individual
James Gower
Entergy
No
CIP-003 R2 Part 2.3.2 requires entities to implement one or more processes that include “For Control Centers with external routable protocol paths, monitoring physical access point(s)” for Low Impact BES Cyber Systems. Executing this requirement would require entities to identify physical access points to Low Impact BES Cyber Systems which, in essence, would require the identification of a Physical Security Perimeter. This was not required under CIP-006-5 for Low Impact BES Cyber Systems. The risk reduction this requirement would bring is low due to the impact designation of Control Centers, where entities would protect all of the BES cyber systems located at and associated with the operation of those Control Centers designated as either High or Medium impact.
Yes
These changes are in line with the “ORDER REMANDING PROPOSED INTERPRETATION OF RELIABILITY STANDARD CIP-006-4” issued by FERC 3/21/2013.
Yes
Yes
Yes
No
With multiple effective dates for different requirements and sub-requirements, confusion may arise and result in an increased risk of potential violations. Making all requirements effective on the same date, or grouping compliance date by High, Medium, and Low designations would make for a more consistent transition to CIP Version 5.
No

Yes
: The naming convention for the standards should be standardized to prevent confusion. There are “CIP Version 5” standards that contain requirements suffixed -5 and -1. If the proposed revisions are approved, there will be standards suffixed -2,-5,-6, and -1 if CIP-014 is included. This is contrary to the precedent set by previous versions of the standards. Version 4 only contained changes to CIP-002, but all requirements in that Version were updated to -4, even though they did not change. Now the suffix is being incremented only when requirements have changes made to them, resulting in multiple suffixes. Requirements should all be suffixed with the same number to easily identify the current set of enforceable requirements as a package.
Individual
Erica Esche
Southern Indiana Gas and Electric Company d/b/a Vectren Energy Delivery of Indiana
Individual
Silvia Parada Mitchell
NextEra Energy
No
Looking at this from a risk perspective, the probability that someone will enter into a NERC CIP facility with access control devices, cameras, on-site personnel, etc. and then try to tap into the wiring, as opposed to just entering into the PSP and utilizing the BES Cyber System is not logical. Thus, NextEra recommends the following changes to the CIP-006, Requirement R1, Part 1.10 and its measure: By adding a paragraph to the Requirements Section which states: To restrict physical access to such cabling and components, the Responsible Entity shall document and implement one or more of the following: - Secured with conduit; or - Secured with cable trays; or - Implement alternative physical security control measures that utilize a defense in depth strategy that may include, but are not limited to: o multiple physical access control layers within a non-public, controlled space; o 24 x 7 security or operational personnel; o camera/video coverage; o other alarm systems; o multi-factor authentication devices; o other related security devices; Then under the Measures Section, modify the verbiage slightly to read: An example of evidence may include, but is not limited to, records of the Responsible Entity’s implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays or alternative physical security control measures) encryption, monitoring, or equally effective logical protections.
Group
MRO NERC Standards Review Forum
Joe DePoorter
Yes
Yes
Yes
The NSRF recommends that CIP-002-5.1 be updated (containing red lined and final versions) with the new and revised definitions.
Yes

: The NSRF supports the removal of IAC language from this fleet of Standards. We do not want any type of internal control or management practice to be an auditable instrument. Every entity needs to determine how they assess if they are compliant with EVERY applicable Requirement that they are registered for.
Yes
Unknown
No
Individual
Dan Roethemeyer
Dynegy
No
The Low BES Cyber Systems in the Applicable Systems column of the Tables would seemingly require a detail inventory similar to that required by Highs and Mediums to determine what are BES Cyber Systems. This should not be required per the Standard. If this is not what is intende then please provide guidance in the Standard as to how to determine Low Impact BES Cyber Systems without the using the detail inventory process.
Yes
Yes
On June 19, 2014, NERC gave a webinar on V5 and their was good Q&A at the end of the call. I thought their were many good questions but also many good answers that seemed to make sense from NERC. I couldn't write fast enough to get them down and repeat here but I suggest you get the recording (if available) and weave those answers into the Standards for guidance.
Individual
Kathryn Zancanella
South Feather Power Project
Yes
Yes
Yes
Yes
Yes
Part 2.6 of CIP-003-6 requires a quarterly "security awareness" component for entities with low impact cyber assets. For a small entity with few assets to begin with, instituting a quarterly "security awareness" communication could result in the opposite effect of what is desired. Rather than highlighting security awareness, such as is done during annual training that is already required by

FERC for hydropower licensees, a quarterly communication will take on the nature of routineness. I recommend changing Part 2.6 to require annual secuirty awareness communications.
Group
Arkansas Electric Cooperative Corporation
Philip Huff
No
We appreciate the approach to provide more specificity by using existing language from the other CIP Cyber Security Standards, and we support the language for all but the physical security Requirement Part 2.2. The requirement to restrict physical access does not provide sufficient criteria for entities to know they have satisfied the obligation. We suggest keeping the language of the requirement part and adding guidance to restrict physical access for BES Cyber Systems at a generation Facility and BES Cyber Systems at a substation. In particular, the guidance should confirm an approach whereby BES Cyber System components in a control house or control room can have greater physical protection applied than components distributed throughout the facility.
Yes
Yes
Yes
Yes
No
Overall, we feel the proposed timeframes are reasonable. However, we would like to submit a possible oversight in the timeframes for newly identified assets. There is currently no additional time given for newly identified assets with low impact BES Cyber Systems. It is possible for unplanned changes to result in an asset becoming part of the Bulk Electric System. In CIP-003-5, this was less of an issue because CIP-003-5 R2 was more programmatic and entities could address new assets as part of their overall program. The proposed CIP-003-6 R2 now has specific criteria, which necessitates consideration in the implementation plan for unplanned changes resulting in low impact categorization. We suggest a 12 month period for compliance implementation in this scenario. Also, we wish to express our support for the SDT completing all four Order 761 directive areas. It is important to have industry-developed objective criteria for the low-impact BES Cyber Systems when the requirements goes into effect on April 1, 2017. The industry begins its 7th year in which these Standards have been in development. It is difficult to grow and mature security programs with so much change in the compliance rules. We hope the industry, NERC and FERC can come to an agreement in the coming months and provide finality to these Reliability Standards for a time.
No
No
Individual
Michael Haff
Seminole Electric Cooperative, Inc.
Individual
Jo-Anne Ross
Manitoba Hydro
Yes
In Section C: Compliance Section 1.3, the meaning of “Complaints Text” is unclear
Yes
Yes

Yes
Yes
Yes
No
Yes
1) Given that the CIP standards become effective after governmental authority approval for most Canadian utilities, the CIP-002-5.1 and CIP-005-5 effective dates will be lagging behind the rest of revised standards by virtue of keeping CIP-002-5.1 and CIP-005-5 effective dates unchanged. We suggest changing the CIP-002-5.1 and CIP-005-5 effective dates to match the new implementation plan accordingly. 2) Under Section C 1.1 Compliance Monitoring, the CEA definition from a Manitoba Hydro perspective is incorrect as the Public Utility Board (PUB) is Manitoba Hydro's CEA. We suggest revising the definition to take Canadian utilities situation into account
Group
Colorado Springs Utilities
Shannon Fair
No
The Requirements proposed in 2.1, 2.2 and 2.3 are sound and apportion appropriate controls for Low Impact Cyber Systems. However, the "external routable protocol paths" language in Requirement 2.4 requires entities Low Impact Cyber Systems to provide and comply with "some form of electronic security perimeter," regardless of risk to the Bulk Power System/Bulk Electric System. Compliance to this requirement would be excessive given the risk associated with Low Impact rated BES Cyber Systems, and would require entities to maintain a list of Low Impact Cyber Systems, even though specifically not required by the standard.
Yes
Yes
Yes
Yes
No
Recommend changing the Implementation Plan time schedule to fall after the CIP Version 5 standards implementation dates. Entities are currently in transition from CIP version 3 to Version 5, implementing physical security controls, developing and enhancing policies, procedures, and security controls, preparing for audits, as well as performing the day-to-day operations of the systems.
No
CSU is not aware of any additional Canadian regulatory requirements that need to be considered during this project.
No
Individual
Patrick Farrell
Southern California Edison Company
Yes
Yes

SCE encourages the SDT to clearly provide entities with the choice between the physical access restrictions and the alternative means of protection, such as encryption of data, monitoring of the status of the communication link, and other logical protections. As we have a large and varied system, we will need the clear flexibility to select the best method of the system and environment. The proposed draft seems to suggest that physical protection is the first and preferred method, which could force entities to establish criteria for determining when to default to the alternative methods, thus complicating compliance.
Yes
SCE believes that the SDT's approach is sound, but believes that the final implementation plan for the entirely new Requirement 4 should reflect the additional procedural and record-keeping burden associated with it.
Yes
Yes
We accept the SDT's decision to remove the Identify, Assess, and Correct language from the 17 requirements in which it appeared, but believe that NERC must work expeditiously to complete the Reliability Assurance Initiative project and secure FERC approval of the project. The high frequency security obligations included in the CIP Version 5 Reliability Standards require that NERC and the Regional Entities exercise the enforcement discretion called for in RAI aggressively.
Yes
Group
Tennessee Valley Authority
Brian Millard
No
The Registered Entity suggests the SDT use the existing applicability tables throughout the standards to apply controls to Low Impact assets rather than consolidating in CIP-003 R2. The SDT has stated that they ‘pulled language and concepts from CIP-004, CIP-005, CIP-006 and CIP-008 to add objective criteria to each of the previous policy topic areas in CIP-003, Requirement R2’. The language and concepts that have been pulled into CIP-003-6 R2 do not belong in the CIP-003 standard. The Registered Entity suggests the drafting team maintain consistency with the applicability tables found throughout the CIP version 5 standards and keep similar concepts grouped by standard. The Registered Entity strongly encourages the SDT to add protections to Low Assets in the appropriate CIP standard using the applicability table that already exists within the standards. CIP-003-6 R2.1 should stay in CIP-003. CIP-003-6 R2.2 and R2.3 should be moved to CIP-006. CIP 003-6 R2.4 should be located in CIP-005. CIP-003-6 R2.5 should be located in CIP-008. CIP-003-6 R2.6 should be located in CIP-004. Regarding R2.4: The terms ‘external routable protocol paths’ and ‘identified access points’ are ambiguous and may lead to inconsistent application and auditor interpretation without clarification. The Registered Entity suggests glossary terms be created to provide consistent application of requirements. Regarding R2.5: Can one incident response plan encompass multiple facilities/BES Cyber Systems? Does testing of the plan mean that testing must occur for each facility?
No
A. Need clarification regarding minimum acceptable data encryption standard. B. Need clarification regarding maximum acceptable opening size for conduit to be considered ‘secure’. C. For cable enclosed in conduit that spans a locked room between PSPs, what physical access controls should be applied to the room?
No
Regarding R4.5, need clarification regarding timeliness of signature / pattern files. How frequently does this update need to occur? Regarding R4.7, need clarification regarding minimum acceptable patching / mitigation prior to use. As written, creation of a dated mitigation plan appears to satisfy this requirement. There is no stipulation that mitigation must be completed prior to use of the asset.

No
Need clarification on what is meant by ‘directly connected’. Does it include specific media types (e.g. RS232, routable protocols, USBs, etc.)?
No
The removal of IAC from the standards requires that the RAI process be clarified regarding reporting timeframe and definition of ‘minimal risk’.
No
Effective dates should be reset to start with the approval date of CIP version 6. For large registered entities the level of effort to implement the standards on ‘Low Impact’ systems may now be greater than the burden of transitioning from version 3 to version 5 ‘High Impact’ and ‘Medium Impact’ systems.
<none>
No
Need clarification for what defines the lower threshold of the ‘Low Impact’ categorization. Does the BES definition serve to establish the lower boundary of the scope of the CIP standards?
Individual
Mikhail Falkovich
PSEG
No
The requirement for the ‘Low Impact’ security awareness goes above and beyond the equivalent requirement for High and Medium assets. We recommend removing the extra language in table R2 part 2.6 “Once every 15 calendar months, the program shall reinforce Parts 2.2., 2.3,2.4, and 2.5 above”. This will bring the language more in line with the equivalent requirement in CIP-004 R1.1. Additionally, we urge the SDT to reconsider the ‘quarterly’ periodicity of the security awareness reinforcement for Low Impact assets. While higher impact assets have a need for higher frequency of security awareness, the appropriate periodicity of reinforcement for Low Impact assets should be longer (annual periodicity is adequate).
Yes
Yes
Yes
No
While PSEG supports the approach of removing the IAC language and relying on the RAI function within NERC to manage the ‘zero defect’ issues, the RAI program has not yet been rolled out to the industry, and there is significant concern with the consistency of the RAI implementation. PSEG would like to have additional clarity and finalization of the RAI process prior to the implementation of the new standard language.
No
By the time this standard will be approved, the requirements impacting the low impact assets will change from the original CIPv5 requirements. Due to this fact, the industry should be allotted additional time to implement the necessary changes, as entities may have waited for finalization prior to initializing the low impact compliance/security projects. We request that the enforcement date for CIP-003-6 R2 be extended an additional 12 months to comply with CIPv6 low impact requirements.
No
No
Individual
Robert Ganley

Long Island Power Authority
Individual
Cliff Johnson
Consumers Energy Company
No
We agree with R2.1, R2.2, and R2.3. We do not agree with R2.4 as written. The Standard needs to clearly state that the access point can reside either at the substation OR at the remote end of an external routable protocol path. We do not agree with R2.5 as written. The language of the Standard needs to clarify that the Responsible Entity can create a holistic Incident Response plan utilizing physical security mechanisms that lead to Cyber Security Incident identification, classification, and response; and that logging and monitoring of Low Impact Cyber Systems is not required. We do not agree with R2.6 as written. The language of the Standard needs to clarify that the Responsibility Entity's security awareness program applies only to their employees, but could include non-employees, and that posters, emails, and topics at staff meetings are sufficient delivery method and that tracking of reception is not required. Overall comment, the Guidelines and Technical Basis contain the clarification language, but Responsible Entities are audited on the language of the Standard.
No
Comments: This has the potential to create significant undue burden on entities. The use of undefined terms such as "nonprogrammable" and "extended ESP" along with referencing between standards makes the requirement difficult to comply with. The sentence "In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP." From of the CIP-006-6 Guidelines and Technical Basis on page 37 leaves the requirement open to interpretation with no clear stopping point. The terms should be defined to limit the scope of the requirement and even though entities may utilize defense-in-depth controls beyond what is required, the requirement should be limited to the first termination point outside the PSP.
Yes
Yes
Yes
No
Not as written, but may be reasonable if adjusted according to entity feedback.
No
No
Individual
Candace Morakinyo
Wiscsonsin Electric Power Company (d/b/a We Energies)
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No

We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations.
No
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations. We Energies cannot vote to approve standards with "zero tolerance for exceptions".
No
We Energies is particularly concerned with Requirement R2.4 and its subrequirements, further explained in the Edison Electric Institute (EEI) response to question 1 on low impact requirements.
Not familiar with Canadian provincial or other regulatory requirements.
Yes
We Energies participated in the development of and supports the comments submitted by Edison Electric Institute (EEI), including suggested revisions and recommendations. Additionally, We Energies provides the following comments: * CIP-002-5.1 Attachment 1 Impact Rating Criteria 2.3 is not specific enough with respect to which BES Cyber Assets meet the criterion, or when they must be compliant. In general, it is understood that newly identified BES Cyber Assets must be compliant within one year of identification. However in this criterion, it is feasible that a generation Facility might be identified in a study looking out 5, 10 or more years with some level of uncertainty in study assumptions. Securing such a Facility is good business practice. Expending the effort to be auditably compliant years before the Facility actually becomes a limiting factor to BES reliability is wasteful of resources. Implementing compliance measures and incurring compliance risk is wasteful of resources if real world conditions change over time such that the Facility never becomes a limiting factor to BES reliability. * CIP-002-5.1, CIP-005-5 and CIP-008-5 all, in section 6, state that “An entity should include as much as it believes necessary in its documented process but it must address the applicable requirements.” It should also explicitly state that any entity-specific processes which go “above and beyond” the standard requirements will not incur regulatory compliance obligation. * CIP-003-6 Section 6 Background states that an entity should include as much as it believes necessary in its documented process but it must address the applicable requirements. It should also explicitly state that any entity-specific processes which go “above and beyond” the standard requirements will not incur regulatory compliance obligation.
Individual
Kayleigh Wilkerson
Lincoln Electric System
No
Although appreciative of the drafting team's efforts in developing the CIP Version 6 revisions, LES offers the following comments for the drafting team's consideration: CIP-003-6 R2.4.2 should be a sub bullet of 2.4.1. CIP-003-6 R2.5 – Requiring incident response on the Low Impact Assets seems unnecessary in consideration of the physical and electronic protections already required in the other draft CIP-003-6 requirements at the Low Impact Assets. Recommend the drafting team either remove R2.5 or else add an exclusion for ‘Low Impact assets without routable connectivity’ in recognition that a cyber-incident at a non-routable connected substation does not affect any other Low, Medium or High Impact BES Asset. CIP-003 R2.6 – Recommend the drafting team provide additional clarification regarding general awareness for Low Impact Assets. Is it the drafting team’s intent that awareness information be posted at every Low Impact Asset or is the posting of information in crew rooms and on intranet sites sufficient to meet this requirement? Additionally, do registered entities need to be concerned with contractors at their Low Impact Facilities and ensuring they get the quarterly awareness information too? In consideration that awareness training is already required of High and Medium Assets, LES recommends the drafting team consider, at a minimum, adding an exclusion to R2.6 for the ‘Low Impact assets without routable connectivity’ in recognition that a cyber-incident at a non-routable connected substation does not affect any other Low, Medium or High Impact BES Asset.

Individual
Michael Hill
Tacoma Public Utilities
No
Tacoma supports LPPC's comments on CIP-003 R2
Yes
One potentially unintended outcome of the wording of CIP-006 R1 [1.10] is a detailed cable map for each and every cable path relevant to an ESP in order to show protections for all of those that happen to fall within an ESP boundary, but not a PSP boundary. Detailed network diagrams may not be sufficient to prove whether or not a particular cable path falls inside, or outside a PSP.
No
Tacoma Power Supports LPPC's comments on CIP-010 R4 & CIP-004 R2. Additionally, Tacoma Power suggests CIP-010 R4 technical controls be moved to the like locations in CIP-007 (CIP-010 R4 [4.2-4.5] -> CIP-007 R3, CIP-010 R4 [4.7] -> CIP-007 R2). And move Authorization requirements to CIP-004 (CIP-010 R4 [4.1.1-4.1.2] -> CIP-004 R4) and Policy requirements to CIP-003 (CIP-010 R4 [4.1.3] -> CIP-003). Leaving CIP-010 R4 [4.1.4 & 4.6] in CIP-010, if they remain in the standard.
No
Offering a modification to the Removable Media definition below: "Removable Media: Media capable of removal without powering down the system, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media." This would remove the need to create a further definition of "Portable media." This definition would include hot-swop hard drives. Additionally, an argument can be made that all flash media contains a programmable microcontroller, and would therefore qualify as a Cyber Asset.
Yes
Tacoma Power Supports NERC's efforts to develop the Reliability Assurance Initiative (RAI) as a way to move away from a zero-tolerance enforcement approach.
Yes
No
No
Individual
David Rivera
New York Power Authority
No
NYPA recommends that the language added to CIP-003-6, table R2 (low Impact Assets) be moved to the specific tables in each of the Standards CIP-004-6 through CIP-011-2 where applicable. The inclusion of these control requirements with a unique table in CIP-003-6 result in Standards language inconsistencies that creates confusion and additional compliance risks. The following are some specific examples (not meant to be a complete list): A. A new definition is now needed (CIP-003-6 Rationale R2 and Part 2.4) for the phrase "external routable protocol paths" to ensure that entities and auditors clearly understand the differences between that phrase and the defined term External Routable Connectivity. This would avoid duplicating the confusion seen in earlier versions of the CIP Standards, such as the CIP-001 confusion between Facilities and facilities. The phrase "external routable protocol paths" may create a similar interpretation risk. B. With the new wording in CIP-003-6, table R2, security awareness (Part 2.6) is now more stringent for Low Cyber System than those that are High / Medium in CIP-004-6, R1 C. The Low Cyber System Incident Response Plan in Part 2.5, is very inconsistent with High / Medium Incident Response Plan required in CIP-008

R2 D. Policy requirements for Low Impact Cyber Systems would require a different set of policies to cover Low Cyber Systems for Entities with a combination of Low, Medium or High Cyber Systems. E. The shifting of the Low impact requirements to CIP-003-6, R2, breaks one of the prime objectives defined when CIP version 5 was being developed that each of the Standards (except CIP-002) be able to stand on its own. At entities with Low “and” either Medium or High Cyber systems, it would be necessary that CIP-003 “always” be referenced when any of the requirements in CIP-004-6 through CIP-011-2 are being designed and implemented, since dependencies are always possible between Cyber Systems part of any impact category. The end of result of having these Low Cyber System controls contained only in CIP-003-6, is that going forward, as the CIP requirements are refined and enhanced, the risk of new inconsistencies being created will always be a very higher. For example, if a slight change is made to a requirement in CIP-007-6, which somehow affects the set of Low Cyber Systems, then having to make a similar change to CIP-003-6, R2, in accounting for that change, may result in the change being missed or becoming inconsistent. These new set of CIP standards are already very complex, and any added confusion caused by this obvious structural problem will make it even more difficult (and costly) in meeting the Standards and likely negating the goal of improving overall reliability.
Yes
NYPA supports NPCC comments to this question.
Yes
Yes
Yes
No
NYPA Supports NPCC comments to this question.
No
Yes
NYPA Supports NPCC comments to this question.
Individual
Brenda Hampton
Luminant Energy Company, LLC
Yes
Luminant appreciates the work the drafting team has put into these standards. We agree with the general direction, but do have comments to provide clarification within the language. (1) For CIP-003, R2 the Rationale section states that “external routable protocol paths” is intended to focus only on paths to the low impact BES Cyber Systems rather that other networks such as Corporate. Can this be a defined term to explicitly state that rather than rely on the Rationale section? (2) CIP-003, R2.2 lists operational and procedural controls to restrict physical access. What is the difference between these two controls? Please provide examples. (3) The intent of CIP-003, R2.4.1 is dependent upon a definition of paths that can vary for each entity. The emphasis is needed on the controls that are implemented for clarity and measurable objective criteria. Please consider the following as a revision to R2.4.1: “Access points must be used to control routable communications to destinations and/or sources external to the BES asset where Low Impact BES Cyber Systems are located.” This revision places the emphasis on documenting the controls that accomplish the goal of restricting electronic access. (4) In Section C, part 1.3 the listed “Complaints Text” is confusing. Is the inclusion of the word “text” a typo? If not, please provide some context for this statement. (5) CIP-003 VSLs table can be challenging to follow. Consider removing redundant language wherever possible. Potential text edits include: (a) R2, item 1 “but failed to address one of the topics included in Requirement R2, Parts 2.2-2.6.” instead of referencing the text that references other texts (page 18 of 32). (b) R2 applies to low impact BES cyber systems. Is it necessary to repeat “with a low impact rating” or “for assets with a low impact rating” throughout the VSLs? (6) Suggested revision for CIP-003 “Guidelines and Technical Basis Section” Paragraph 2.2. This section includes a

statement of “operational or physical controls” however this language should match the requirement language which reads “operational or procedural controls”. (7) Suggested revision for CIP-003 “Guidelines and Technical Basis Section” Paragraph 2.3. (a) This section includes a statement of “external routable connectivity” however this language should match the requirement language which reads “external routable protocol paths”. (b) Since the primary purpose of monitoring is to watch for unauthorized access. Consider the revised language for the last two sentences: “Monitoring does not imply logging and maintaining logs, but monitoring that access has occurred at an access point (e.g., a door has been opened or traversed). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity’s controls.” (8) Suggested revision for CIP-003 “Guidelines and Technical Basis Section” Paragraph 2.4. (a) Within examples of sufficient access controls, the “public internet” seems to be a preferable listing rather than “world-wide-web” to include various external locations. (b) Within examples of sufficient access controls, details are provided for dialup modem connections. Is it the intent to not allow the modem to accept calls from authorized numbers? Should the wording be revised to clarify that calls from authorized numbers can be configured to autoanswer. Does the authorized phone number represent “some form of access control”? (c) Consider the following revisions to change the access technology to be more generic to not inadvertently restrict technology changes in the future. Consider revised language: “An asset has external routable connectivity due to a BES Cyber System within it having a wireless communications card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet on an unrestricted basis and from search engines such as Shodan.”

Yes

(1) The language in CIP-006, R1.10 seems to be in conflict with the Applicability section of CIP-007, R1.2. CIP-006, R1.10 includes only “nonprogrammable communication components outside a PSP” while CIP-007, R1.2 includes “nonprogrammable communication components located inside both a PSP and an ESP”. This conflict could be interpreted to imply that “entity owned and managed nonprogrammable network devices”, which are also “nonprogrammable communication components” are to be exempt from CIP-007 R1.2. Consider revising the Applicability section of CIP-007, R1.2 (which is not included in the current comment and ballot scope) to state the following: “Nonprogrammable communication components that are entity owned and/or managed and located inside an ESP.” (2) For the VRFs/VSLs for CIP-006-6, R1 and R2 please provide some understanding for removing all but Severe VSL. What would this mean if an entity has a process documented and implemented but fails follow it perfectly? For instance, what if an entity has a process to retaining logs for 90 days but unfortunately actually retain all the logs. Is this not a violation since it does not rise to the level of Severe?

No

(1) The wording for the Applicable Systems and the Requirements in CIP-010-2, R4 should be consistent to avoid potential confusion across the various parts of the requirement. Potential revision is to add “on applicable systems” to R4.1, R4.6, R4.7 and “prior to use on applicable systems” to R4.5 OR remove “on applicable systems” from R4.3. (2) CIP-010-2, R4.3 and R4.6 include the language “prior to use.” This language is problematic due to the ambiguity of “use” and leaves much to interpretation. There is language provided in the Guideline and Technical Basis, but enhanced language within the standard requirements would provide more clarity of the SDT intent to all industry segments. Additionally, it does not address Medium Impact BES Cyber Systems that are not required to be inside an ESP (or even a PSP) because they do not use routable protocols. Such devices are not subject to proposed requirement R4.6 but are subject to proposed requirement R4.3. (3) There appears to be a gap in CIP-010-2, R4.5. If an entity were to have a Transient Cyber Asset connected for 29 days, that Transient Cyber Asset should not necessarily have signature files that are 29 days old. Instead, if a Transient Cyber Asset is connected during a regularly scheduled signature update for non-transient devices, that Transient Cyber Asset should also be updated. The following language is suggested as an addition to the Requirement for R4.5 to remediate this gap: Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 when Transient Cyber Assets remain connected during regularly scheduled updates pursuant to CIP-007-Table R3 Part 3.3. (4) There appears to be a gap in the requirements if a PCA is used in any way other than it use as specified in R4.1.3. Consider the addition of CIP-010-2, R4.8 as follows to close this potential gap in the standards. If language is added, revisions are also needed in VRFs, VSLs and guidelines.

PART 4.8. APPLICABLE SYSTEMS: High Impact BES Cyber Systems and associated PCA, Medium Impact BES Cyber Systems at Control Centers and their associated PCA. REQUIREMENTS: Evaluate Transient Cyber Assets in accordance with 4.6 and 4.7 after any use not included in Part 4.1.3. When the evaluation results indicate the Transient Cyber Asset has been modified, take one of the following actions prior to use: -Remediate by returning the Transient Cyber Asset to the documented state in Part 4.1.4; or -Update the documented state in Part 4.1.4. MEASURES: An example of evidence may include but is not limited to, updated documentation with the date, evaluation results, and status of any remediation activities. (5) Guidelines and Technical Basis, Requirement 4. There is some good information included as a reference to support a clear understanding of the standards and requirements. The examples of transient devices that are provided could be strengthened with further specifying the intended meaning for Hardware/software diagnostic test and Hardware/software packet sniffers to clarify what the devices are used for. Possible revisions or additional language could include: ""Software diagnostic test equipment" is hardware equipment running such diagnostic software" and "Hardware/software packet sniffers" to "Hardware device running software packet sniffers. Which means an asset is categorized by a hardware component and specific associated applications or software they are running." Revisions to these bulleted items will improve the clarity and provide guidance to industry. (6) Guidelines and Technical Basis, Requirement 4, Parts 4.2, 4.3, 4.4 and 4.5. (a) The statement, "Pre-authorized Transient Cyber Assets may have the malicious code prevention maintained on the device and do not require specific actions for each use" is reasonable, but the actual requirements do not make this clear. Revisions are needed to the appropriate requirements statements to clarify the SDT intent. (b) The statement, "For Removable Media and Transient Cyber Assets authorized at the time of connection, the detection of malicious code must be addressed prior to use" has the same problem as Requirement 4.3: What is a "use" as intended for the standard? (c) A later paragraph states, "For Requirement R4, Part 4.4, if malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident." The second sentence seems ambiguous and could lead to different interpretations for entities and other stakeholders. How is an entity supposed to decide whether or not malware that is (1) detected and (2) removed before a transient device is connected qualifies as a Cyber Security Incident? It may or may not be easy to tell. Are entities expected to keep records of such occurrences? We suggest removal of the second sentence above and allow the entity to handle the malicious code detection within existing response requirements and avoid introducing this requirement here. (d) The next paragraph states, "Part 4.5 requires a process to update signatures or patterns, where applicable. This process is to be documented in the overarching program. As with CIP-007-6, Requirement R3, the process is to include testing and installing of updated signatures or patterns." The requirements in CIP-010 R4 do not require testing. This last sentence should be removed or revised to only include "process to document the installation of updated signatures or patterns." (7) Guidelines and Technical Basis, Requirement 4, Parts 4.6 and 4.7. The first paragraph states, "Requirement R4, Part 4.6 requires the entity to evaluate Transient Cyber Assets to ensure that no unauthorized modifications have been made to the operating system, firmware, or software. This is a review of the current state against what is currently documented pursuant to Part 4.1.4. If there are differences, the modified code may be removed or the documentation updated to align to the authorized or current state." The term "prior to use" can be interpreted different ways (e.g. the start of a new workday, start of work within an ESP after leaving another ESP across the hall, start of the work week due to Transient Cyber Asset not being in direct control of the employee over the weekend, etc.) The "prior to use" language needs to be amended to avoid forcing entities to perform R4.6's specified tasks in situations when it is not required or needed.
Yes
Yes
Yes
No

Individual
Venona Greaff
Occidental Chemical Corporation
No
Occidental appreciates the work the SDT has done in response to FERC's directive in Order 791 to "address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets". However, we do not agree that the SDT developed objective criteria. Instead of establishing reasonable limits on the extent of evidence required to validate that an entity is providing sufficient physical protection, electronic access controls, cyber-incident preparation planning, and awareness training, R2 leaves the discretion up to the CEA. In order to prevent uneven application of the requirement across Regions – or changing over time – Occidental makes the following recommendations: 1) Change the focus of each sub-requirement from "implementing one or more processes" to "develop and maintain one or more processes". The 36 month recurring validation of the incident response plan (R2.5.6) would serve as a proxy for evidence of implementation – perhaps with an additional statement indicating that at least one Cyber System's physical/electrical protections must be evaluated as part of the exercise. Thus, the sample itself is under the entity's control – but the requirement could provide the minimum scope of cyber controls that must be validated. 2) Change the language in the Measures from "Examples of evidence may include, but are not limited to:" to "Each bullet point below provides an example of evidence sufficient to satisfy this requirement". A catchall bullet point would be needed to state that the entity is free to provide other equally effective evidence that satisfies the requirement. Although Occidental respects the good work that NERC has done to move away from zero-tolerance compliance methodologies, non-binding assurances that a reasonable compliance assessment will always be applied are not enough. Subjective interpretations by Regional Entities are still a very real concern. In the fast moving world of cyber security, it is far too easy to apply 20-20 hindsight to determine that an entity "should have been better prepared" for a new cyber-attack vector that did not exist when the protective strategies were developed.
Abstain
Abstain
Yes
No
In Order 791, FERC articulated that they understood the intent of the IAC language, but did not agree with the strategy taken to implement it. The Commission shared the concern that the rapid evolution of cyber-attack methods required flexibility in the protective strategies Responsible Entities deployed to address them. Forcing the industry to take mitigating steps to address future cyber-security incidents based upon the cyber environment in 2014 could be problematic. The SDT's approach in removing the IAC language and providing assurances that CEAs will apply appropriate consideration (via RAI process) for unknowable changes in the cyber-environment is somewhat concerning. Although OCCIDENTAL is a proponent of RAI and agrees that the regulatory community has taken positive steps in the direction of risk-based compliance, we have concerns that reason may not prevail in the aftermath of a destructive cyber incident. As mentioned in our comments to Question 1, subjective interpretations by Regional Entities are still a very real concern. Question 4 in the Identify, Assess, and Correct and Reliability Assurance Initiative FAQ document and its response reinforces our concern. How has the SDT chosen to address the concerns of IAC? The SDT discussed the concerns and options within FERC Order 791 and revised the 17 requirements containing IAC by removing the language. The approach fulfils the Order 791 directive regarding the IAC language and leaves resolution of "zero defect" or "zero tolerance" to the RAI 'discretionary path to enforcement' implementation. We appreciate the difficult task the SDT faced in addressing this issue because we too are hard pressed to come up with an equally effective method of addressing FERC's directive. We also recognize that delaying addressing FERC's directives with regard to IAC until RAI is officially rolled-out is problematic. But, until industry as a whole understands, and experiences first hand, a successful RAI approach, the requirements leave too much open to regulatory interpretation. The ancillary documents provide some guidance but in the end only the requirements within the Standards are subject to compliance and are enforceable. Our proposed alternative would be to encode the IAC concept into separate sub-requirements under each of the 17 affected requirements.

An example binding method might take the following form: Requirement Header: Each Responsible Entity shall implement a <program, procedure, policy> in a manner that is consistent with its best understanding of the cyber threat and protective strategies available at that time. A list must be included in the <program, procedure, policy> that captures the Responsible Entity's assumptions. Sub-Requirement A: At least once every 3 years, or after experiencing a Reportable Cyber Incident, or upon receipt of a NERC Alert related to this requirement, the Responsible Entity will perform and document an assessment of the adequacy of their <program, procedure, policy> and the assumptions. Sub-Requirement B: The Responsible Entity will develop and execute a Corrective Action Plan within 30 days of an adequacy assessment performed in accordance with Sub-Requirement A which indicates a reliability gap has been detected.
Yes
Abstain
No
Group
Dominion
Connie Lowe
No
Dominion suggests the SDT revise the wording of Part 2.1 to indicate "Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.". Without the word "applicable", a registered entity would have to have a policy associated with "Low Impact BES Cyber Systems at Control Centers" even if the entity doesn't have any "Low Impact BES Cyber Systems at Control Centers". Part 2.4.1 uses the term "external routable protocol paths". Clarity is needed to understand what "external" is in reference to. Provided there are no defined ESPs associated with Low Impact BES Cyber Systems, there are no defined external routable paths. Additionally, private network connections can exist between relays at different "impact rated" substations and restrictions should not exclude or preclude vendors from improving communications between relays by converting from a teltone connection to a digital connection. The requirement of defined access points and access permissions could interfere with such progress. Dominion believes that this requirement should be clarified to apply solely to external interactive access. Dominion suggests Part 2.6 should be revised to state: "Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months." As written, the requirement is more prescriptive than requirements for medium and high impact BES Cyber Systems. The language of the requirement should reflect the low impact rating of the asset class. Dominion notes that certain requirements, such as 2.3, may not apply to an entity, therefore, the language of the Part should not be overly prescriptive such that the concept of 'applicability' is excluded.
No
In general, Dominion agrees with the approach, but has concerns regarding how the last bullet in CIP-006-6, Requirement 1, Part 1.10 will be measured. The language of the last bullet states "• an equally effective logical protection". In order for this language to be auditable, a determination would have to be made on the effectiveness of the logical protection when compared to the first two bullets which state "• encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or" If an equally effective logical protection is required to be documented, Dominion believes clarification is needed regarding 1) how the protection would be measured and 2) who would be responsible for making the determination of the effectiveness of the control.
No
Dominion suggests adding a sub-part under CIP-010-5 Part 4.1 that allows entities to authorize classes or groups of Transient Cyber Assets. The suggested language is "4.1.x. Transient Cyber Assets, individually or by class or group of like assets;" Change CIP-010-2 Part 4.1.4 to be

consistent with CIP-010-2 Part 1.1.1. Part 1.1.1 states “Operating system(s) (including version) or firmware where no independent operating system exists”. Part 4.1.4 states “Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).” Recommended language for CIP-010-2 Part 4.1.4 is as follows: Operating system(s) or firmware where no independent operating system exists, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability). Dominion also suggests that additional language be added to the Guidance and Technical Basis section of this Standard to clarify what “per Cyber Asset capability” means. For example, Dominion needs clarity in understanding the extent to which an entity should go to determine the Cyber Asset capability; if the device doesn’t have a direct method of providing internal diagnostic and baseline information about the device itself, does this qualify the Transient Cyber Asset as not having “the Cyber Asset capability” to provide this information? Part 4.1: CHANGE: Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances TO: Authorize the usage of Transient Cyber Assets individually or by group prior to initial use, except for CIP Exceptional Circumstances Part 4.2 -- Clarity is needed regarding the “(per Cyber Asset Capability)” clause. Additional language should be added to the Guidelines and Technical Basis to describe the purpose of this clause. In practice, Dominion believes the clause means that when method(s) to deter, detect, or prevent malicious code can’t be technically implemented on a Transient Cyber Asset, procedural and policy controls are adequate. Additionally, where technical controls could theoretically be applied to deter, detect, or prevent malicious code on the Transient Cyber Asset, but the technical controls aren’t a recommended or approved configuration from the manufacturer of the Transient Cyber Asset, procedural and policy controls are adequate to meet this Part. Dominion is concerned that the “theoretical ability to implement a technical control per Cyber Asset capability” will be misinterpreted as requiring entities to adopt any and all technical controls per Cyber Asset capability regardless of operational feasibility. Part 4.6 -- Clarity is needed regarding the linkage of this Part to Part 4.1.4. Is an entity expected to reauthorize the baseline list of “Operating system(s) or firmware where no independent operating system exists, and intentionally installed software” for a Transient Cyber Asset when it’s changed as a result of executing Part 4.6. Dominion suggests no re-authorization is required since Part 4.1 states the authorization is required prior to initial use.
No
Dominion suggests combining the last sentence from BCA and PCA definitions and add it to the end of the proposed definition for Transient Cyber Asset to read as; A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Transient Cyber Asset is not a BES Cyber Asset or a Protected Cyber Asset. Dominion can’t comment further until clarity is provided on the phrase “programmable electronic device” and it’s applicability to the Bulk Electric System. Dominion believes this phrase unintentionally includes assets that would divert focus from the true intention of the standards.
No
Dominion is in support of the removal of the language as long as the removal is in conjunction with the adoption of an industry-approved RAI approach to ensure there’s relief from the administrative burden imposed by zero-tolerance. An alternative approach to RAI would be to address FERC’s concerns by modifying the individual Parts of each of the CIP Requirements.
Yes
No
No
Group
Southwest Power Pool Regional Entity
Bob Reynolds
Yes

While the SPP RE agrees that the explicit directives in FERC Order No. 791 have been met, the SPP RE has two concerns. First, the SPP RE disagrees with the premise in the Guidelines and Technical Basis section of the Standard that compliance can be demonstrated purely through presentation of the documented processes at audit. There is an expectation that the documented processes will be implemented by the Responsible Entity. In fact, the VSLs for R2 specifically refer to implementation (or failure thereof) of the documented processes. The compliance auditor is expected to evaluate whether or not the documented processes have been implemented and it is best left to auditor discretion how to accomplish that review. Rather than asserting that there should not be an expectation of verifying process implementation, as can be inferred by the paragraph in question, the guidelines would better serve the Responsible Entity by advising them to consider how they would demonstrate implementation and compliance with their documented processes. The guidelines should inform the Responsible Entity and the auditor what is expected to comply with the requirements and not how the requirements should be audited. The comment that the SDT strongly believes sampling is not necessary is inappropriate and should be removed. Second, the protection expectation for Low impact BES Cyber System is a weak, periphery control at best. Two critical protective controls are missing, especially with respect to a control center environment, and those are security patching and anti-malware protections. The entity does not necessarily have to perform the extensive testing expected of higher impacting BES Cyber Systems, but it is well known that somewhere around 90 percent of all successful cyber compromises could have been prevented with up-to-date patches and up-to-date, active anti-virus solutions. Given the likelihood of trusted network interconnectivity between control centers with Low impact BES Cyber Systems and control centers with higher impacting BES Cyber Systems, this critical shortcoming could be the key to a successful, widespread cyber attack.
Yes
The SPP RE agrees with the approach in general, however the SPP RE believes that in the instance where monitoring is the alternative process implemented in lieu of physical access protections, the alert needs to include a follow-up response that investigates the cause of the alert, regardless of the duration of the outage or communication interruption. Ignoring a momentary interruption could result in not detecting a splice, tap, or in-line compromise (similar to a key logger placed between the keyboard and the PC). Obviously, long-haul circuit protection, especially when the communication path includes commercial carriers (such as AT&T) or third-party providers, is best provided through the use of encryption. Within a building or for short runs between PSPs as might be found at a generating plant, an investigation response is quite feasible.
No
CIP-010-2, Part 4.2 could be construed as mandating anti-malware on a transient device. If read in this manner, it would preclude the use of a hardened laptop where the laptop is booted from a read-only CD and the hard drive-based operating system has been removed. Installing and maintaining anti-malware in this instance would be an unnecessary burden. The SPP RE recommends including a discussion of alternatives to the use of anti-malware in the Guidelines and Technical Basis section at a minimum. CIP-010-2, Part 4.5 needs to be strengthened by requiring the signature files to be updated and current prior to each use of the transient device, where anti-malware solutions are used. As written, a process that calls for an annual update of the signature files, while unreasonable, would satisfy the strict language of the requirement. CIP-010-2, Part 4.7 should require the transient system to be fully patched and not permit an alternative mitigation plan. Transient devices are not operationally critical and thus there is no risk-based reason they cannot be regularly patched. As the transient device does not continuously reside within an ESP, it cannot be guaranteed of being afforded the risk-mitigating protections enabled by the ESP requirements. Introducing a transient device into an ESP effectively bypasses most, if not all, periphery (ESP) protections. That can only be mitigated by eliminating risk on the transient device itself to the maximum extent possible. The SPP RE strongly recommends that the discussion of Transient Cyber Assets in the Guidelines and Technical Basis for CIP-010-2 be updated to more clearly state the expectation with respect to “prior to use.” As written, the guidelines suggest the Transient Cyber Asset does not have to be evaluated or otherwise prepared "prior to use" as long as it does not change ESPs or PSPs. That could be construed to allow the Transient Cyber Asset to be used outside of the PSP/ESP and not have to be re-evaluated as long as it was connected back into the same PSP/ESP it was last used in. The SPP RE believes the intent, while not clearly stated, is for the Transient Cyber Asset to be evaluated or otherwise prepared for use within a defined ESP prior to use in the ESP after being used

elsewhere. The SPP RE also suggests that a Transient Cyber Asset could be used consecutively in multiple PSPs/ESPs as long as the Transient Cyber Asset is not used outside of a PSP/ESP in the interim. For example, consider the laptop used to perform maintenance on substation relays. As long as the laptop is connected only to substation relays within PSPs/ESPs, and never to anything else in the interim, the laptop could be moved and used in multiple substations without having to prepare it for first use for each substation being visited. Similarly, a laptop used for maintenance or vulnerability assessments could move between the primary and backup control centers as long as it was never connected to a non-ESP network in the interim. Once the Transient Cyber Asset has been connected to a Cyber Asset or network outside of a CIP ESP, the Transient Cyber Asset must be reevaluated and prepared for "first use" before using it again within an ESP. This provision, as suggested by the SPP RE, should be tempered by the concept found in the Guidelines of having a separate Transient Cyber Asset for each BES Cyber System impact level due to the differing degrees of protection afforded to BES Cyber Systems and Protected Cyber Assets of different impact levels. The discussion of Part 4.5 in the Guidelines and Technical Basis section of CIP-010-2 states that process to update the signature or pattern includes testing the signatures or patterns in the same manner as CIP-007-7, requirement R3. The requirement to test is not included in Part 4.5.
No
The definitions of BES Cyber Asset and Protected Cyber Assets explicitly exclude a Transient Cyber Assets, which is problematic if the definition of Transient Cyber Asset is too permissive. The definition of Transient Cyber Asset is broad enough that a Responsible Entity could, theoretically, treat BES Cyber Assets or Protected Cyber Assets as transient devices by temporarily disconnecting them from the network every 30 days. The definition should be revised to state "A Cyber Asset directly connected to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset, expressly for a pre-approved, temporary purpose and disconnected immediately upon conclusion of the temporary need. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." Similar treatment should be given to Removable Media. In this instance, the expectation should be applied to removable media used for a temporary purpose, such as data transfer, and immediately removed upon completion of the temporary need. Portable media, such as an external hard drive, "permanently" connected to a Cyber Asset should not be considered Removable Media. To complete the distinction, the SPP RE suggests clarifying the term by referring throughout the definitions and standards to "Transient Removable Media."
No
The goal of the IAC language was to remove the expectation of 100% compliance within the standards. While the RAI program can address the handling of an issue of non-compliance through a number of enforcement options, the RAI program does not eliminate the now-restored 100% compliance expectation of the standard itself. There are a number of requirements where a less-than-100% performance expectation can be explicitly defined. For example, the change control and configuration management program is intended to prevent unauthorized changes from being implemented. A performance metric could be developed that allowed for an infrequent (frequency to be defined) occurrence as long as the entity’s detective controls detected the unauthorized implementation activity within a to-be defined detection period (perhaps 24 hours) and the unauthorized change was promptly investigated. Other requirements, such as CIP-007-6, Requirement R4 (Security Event Monitoring that includes a logging component), could include a performance expectation stated in terms of percent availability over a defined period (e.g., 99.99% over a rolling 12-month period, which equates to a maximum allowable outage of approximately 53 minutes over the 12-month period). Adding performance metrics to the requirements themselves provides defined, measurable, and achievable goals and expectations and would eliminate, in many cases, the need to even refer the issue to enforcement for handling. RAI could continue to address the enforcement handling of any issues exceeding the allowable performance expectations.
No
The compliance date for CIP-006-6, Requirement R1, Part 1.10 refers exclusively to BES Cyber Systems. Under CIP Version 3, all Cyber Assets within an Electronic Security Perimeter had to reside within the PSP and were subject to the provisions now found in Part 1.10. The implementation plan for Part 1.10 should be consistent with the actual Version 3 expectation. In other words, the extended compliance period should only apply to new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not previously subject to CIP-006-3,

requirement R1.1 by virtue of being contained within a CIP Version 3 Electronic Security Perimeter. The incremental changes introduced in CIP-007-6, Requirement R1, Part 1.2 are sufficiently straightforward that an additional six months to comply is not warranted. The requirement only applies to controls centers, which greatly limits the scope and potential impact of the change. With the exception of perhaps CIP-010-2, Requirement R4, Parts 4.1 and 4.6 that require an inventory of operating systems, firmware, and intentionally installed software, there is no reason the provisions of CIP-010-2, Requirement R4 cannot be in place upon the overall effective date of CIP-010-2. The expectations of Parts 4.2, 4.3, 4.4, 4.5, and 4.7 are basic security practices that are good utility practices that should already be performed. This risk of introducing malware into the Electronic Security Perimeter is too high to grant nine additional months to comply with these basis security controls.
Yes
The implementation plan for CIP-004-6 allows for the later of April 1, 2016 or first day of the first calendar quarter that is six calendar months after the date that the standard is approved by an applicable governmental authority. However, only three months is allowed if approval by a governmental authority is not required. This appears to be an inadvertent inconsistency in the implementation plan. Additionally, there have been a couple of errata changes to the Guidelines and Technical Basis section of CIP-002-5.1 that have been submitted to NERC by the SPP RE. Specifically; (1) the guidance for Criterion 2.13 should have stated: "Criterion 2.13 categorizes as medium impact *those BES Cyber Systems used by and at* BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1." and (2) the discussion of Criterion 2.8 should state "Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) *or* 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon)." These changes should be incorporated into CIP-002-5.1.
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
Group
SPP RTO
Lesley Bingham
Yes
No comments
Yes
There is a concern about the last bullet in CIP-006-6 R1.10. We do appreciate the flexibility the last bullet provides and how it allows for technological solutions which may not exist today. A Responsible Entity may believe that they have implemented an “equally effective” control, but if the Compliance Enforcement Authority disagrees, then that leads to a contentious audit and possible violations and fines for the Responsible Entity. Additional examples may help to guide the Compliance Enforcement Authority and help them seek reasonable solutions when auditing.
Yes
The section of CIP-004 which was amended was Requirement R2, not R1. An additional comment would be to remove the word “with” in the addition in Part 2.1.9.
Yes
We do appreciate the clarity that removing the IAC language will provide. There is a concern that we are being asked to approve standards based on a program that is currently under development. By the time that a Responsible Entity will see how RAI is applied in audit situations, these standards, with the IAC language removed, will long have been voted upon.
Yes

Consistency of effective dates is very important in a compliance situation. Although the extra time for these standards is appreciated, having 4 dates to manage (April 1, 2016; October 1 2016 for CIP-007-6 R1 Part 1.2; January 1, 2017 for CIP-006-6 R1 Part 1.10, CIP-010-2 R4, and April 1, 2017 for CIP-003-6 R2) is a concern. We would recommend that the six month window for CIP-007-6 R1 Part 1.2 be extended to a nine month window, reducing the number of dates and outlying requirements.
N/A
Yes
We would appreciate clarification on CIP-003-6 R2 Part 2.6. That requirement could be read to mandate two training sessions: a quarterly security awareness program and an additional training once every 15 calendar months to reinforce Parts 2.2, 2.3, 2.4, and 2.5 of CIP-003-6 Requirement 2.
Individual
Daniel Duff
Liberty Electric Power LLC
No
2.4.2, as written, would require the reason for granting access be part of the electronic access process. Suggest elilinating the phrase "including the reason for granting access", and adding 2.4.4 "maintain a record of the reason for granting access".
Yes
No
As writtine 010 R4 assumes the registered entity owns and operates the transient devices and removable media. In many cases contractors do so. The requirement should not force RE's to maintain contractor devices by patching them, nor should it force RE's to keep logs of contractor equipment. The requirement should only focus on scanning such devices prior to use.
Yes
No
The IAC language was needed to gain consensus on the V5 standards. The SDT approach was to simply remove this language without creating an alternitive to a zero tolerance standard. At a minimum, the VSLs and measures should be rewritten to allow for minor instances of errors. For example, instead of a single instance of failing to revoke access for a transfer, rewrite the requirement to requre a process that assures the access is revoked, with a low violation if the process fails to keep instances under 5% annually, or less than 2 in cases where there are small numbers of transfers each year.
Yes
Individual
Amy Casuscelli
Xcel Energy
No
Xcel Energy has several concerns as detailed below. The FERC directive requested objective criteria to be able to evaluate the efficiency of the protections of Low Impact facilities while the rationale and the inventory statements of the proposed Standard state “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” The breakout of Control Centers in R2.3 seems contradictory to both the direction of FERC and the language in the proposed Standard. FERC directed objective criteria, not the identification of specific Low Impact BES Cyber Systems or a tiered level of approach of differing Low Impact BES Cyber Systems. It is recommended that R2.3 be removed entirely or combine R2.3.1 and R2.3.2 under R2.2. We would like to see additional clarity that requirements related to Low Impact systems can

be satisfied at the same time as those for Medium/High. For example, the organization can have a single incident response plan, which does not need to be tested separately for a Low system if a test covered a Medium/High as per CIP-008. These compliance requirements better align with the subject matter of their Medium/High counterparts (CIP-004, -005, -006, -008) and should be moved there, rather than stay in a CIP program governance Standard where they may be overlooked. R2.4.1 and R2.4.2 state that “all external routable protocol paths, if any, must be through one or more identified access point(s)” and “For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.” Xcel Energy feels that by stating that an access point is required for network connected low impact assets, the actual scope of CIP controls significantly increases for these sites. A utility cannot arbitrarily install an access point without performing additional CIP program controls that typically support an effective access point. This would include performing a complete inventory of all assets and their connectivity, developing and establishing ESP diagrams, and performing a vulnerability assessment to verify any potential needs for additional access points. Additionally, it would require periodic controls to validate the access point including equipment inventory, configuration and ESP verifications, as well as the performance of periodic vulnerability assessments to ensure the access point is effective. By stating that an access point is required, this in effect forces entities to implement the full program of CIP controls at assets identified as having a zero to minimal impact to the BES. As worded, the scope of this requirement would be an additional 150 substations for Xcel Energy, dispersed across multiple states. In order to meet the access point requirement, full CIP controls would need to be implemented with no additional protection to the BES. This would result in a 245% increase to the number of substations where controls would need to be implemented; the cost and time of implementation does not seem commensurate with the protection added. R2.4.3 requires “Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.” Xcel Energy is concerned with the scope expansion resulting from this requirement, specifically for assets that have little to no impact to the BES (Low Impact). Xcel Energy anticipates approximately 60 to 70 substations to be classified as medium impact substations under current CIP version 5 requirements. The proposed authentication requirement for dial-up connected low-impact assets would bring approximately 400 additional substations into scope. Identifying, implementing and maintaining configuration management and capabilities to ensure authentication functionality is maintained at an additional 400 substations across multiple states would be an immense effort that would have adverse impacts to utilities such as Xcel Energy. It may also deter operational capabilities as an entity could decide disconnecting dial-up communication would be a better business decision when compared to the expense and level of effort necessary to meet this requirement for low impact assets. R2.6 is much more prescriptive regarding content for the awareness program than CIP-004 R1.1 requirements for Med/High. It should be written more generally to not require specific topics. Additionally, the training and awareness frequency requirements for Low Control level assets are excessive. For example, the quarterly awareness training interval is the same as that required for Medium/High assets. This undermines the meaning of risk level and only serves to promote complacency or a tendency to ignore quarterly missives, rather than promote awareness appropriate to risk level. Because low category assets indeed have a low risk of grid disruption if compromised or lost, the training interval should be less than that of Medium or High Control level assets, to be commensurate with that risk. Xcel Energy fully appreciates that cyber threats are continuously evolving. However, we have incident alert and event management systems to provide notice and awareness of evolving threats to low level asset holders. The incident management process serves to provide awareness of emerging threats, if needed. This quarterly training interval exceeds that of many other very important grid management activities, such as node balancing, Emergency Operations Management, non CIP control center operations, etc. If these very important grid reliability activities do not require quarterly awareness reinforcement, yet have shown through operational history to operate reliably, why should CIP training be more frequent? R2.6 should be revised as follows: “Implement a security awareness program that reinforces cyber security practices at least annually. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4 and 2.5 above.”

No

Both the Standard and the RSAW use the wording “or an equally effective logical protection: but do not offer criteria on who or what would determine what constitutes “effective.” While we appreciate the attempt for flexibility, part of the FERC directive was to reduce ambiguity and provide concise direction for both the Registered Entity and the CEA; this vague definition does not seem to afford

that direction. We recommend either clarifying the words “logical protection” by replacing them with a level of encryption, use or armored wire, or by removing the third bullet entirely.
Yes
There is a huge dependency on RAI accomplishing the intent to remove “zero tolerance” elements of the standards.
Yes
No
No
Group
Edison Electric Institute
Melanie Seader
No
Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. ***4. Applicability*** The scope of dispersed generation in the CIP-003-6 Applicability section should be limited and similar to PRC-005. {Suggested Revision} Under the Introduction section, 4 Applicability, 4.2 Facilities, add the following statement after 4.2.2 All BES Facilities: “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back the reference to CIP-002-5 Requirement R1.3 in CIP-003-6 R2. ***6. Background*** With the addition of the table to Requirement R2, the Background Section should include a paragraph referencing the tables and the “Applicable Systems” Column to be consistent with the Background section of the other CIP standards with similar tables. {Suggested Revision} Add the following paragraph after the first sentence of the CIP-003-6 Background Section 6: “Requirement R2 opens with, ‘Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets.’ The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.” Also, add a paragraph similar to the “‘Applicable Systems’ Columns in Tables:” from other CIP standards into the Background Section 6 for CIP-003-6 for Requirement R2. ***Requirement R2*** Add back the reference to “for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3” to properly set the scope. Also, change the table reference to “CIP-003-6 Policies, Processes, Plans and Programs.” to match the proposed revision to the table title. {Suggested Revision} Change R2 to: “Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.” ***Table Title for Requirement R2*** The Table title for Requirement R2 “CIP-003-6 Table R2 – Low Impact Assets” does not match the format of the tables used in the other CIP standards, which focus on the requirements not the applicable systems. {Suggested Revision} Change the R2 table title to: “CIP-003-6 Table R2 – Low Impact Asset Policies, Processes, Plans, and Programs” ***Requirement R2, Part 2.1*** An entity may not have a low impact BES Cyber System at a Control Center (R2.3) and therefore R2, Part 2.3 is not applicable. {Suggested Revision} Edit text to read “that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 -2.6.” ***Requirement R2, Subpart 2.4.1*** Clarify that an external routable protocol path is “external” to the asset identified in CIP-002-5.1 R Requirement R1, Part 1.3 containing low impact BES Cyber Systems. {Suggested

Revision} Insert “ bi-directional” prior to " external “ and insert “to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems” such that 2.4.1 becomes: “All bi-directional external routable protocol paths to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems, if any, must be through one or more identified access point(s).” ***Requirement R2, Subpart 2.4.2*** Remove “by default” as it implies the use of a firewall, which limits access control options. For example, an entity could use access control lists on a router or switch to provide security for traffic control. However, routers and switches do not do this by default. This will allow entities more options on how to accomplish traffic control. Also, include a statement to allow documentation of access permissions individually or by group to provide more contrast to CIP-005-5 Requirement R1, Part 1.3 for high and medium impact BES Cyber Systems. Documentation for low impact assets individually or by group is consistent with the measure, but should be added to the requirement. {Suggested Revision} Remove “by default” and add “and document access permission reasons individually or by group” such that 2.4.2 becomes: “For each identified access point, if any, require inbound and outbound access permissions, deny all other access, and document access permission reasons individually or by group.” ***Requirement R2, Part 2.6*** The specificity of what must be covered and having to track two time periods is more prescriptive than the requirements for medium and high impact BES Cyber Systems. The proposed revision uses language from the medium/high impact requirement (CIP-004-R1.1) with the time period adjusted to once every 15 calendar months to differentiate for the lower risk. Cyber security awareness can be addressed during annual training for employees and contractors in addition to other ongoing cyber security awareness communications. {Suggested Revision} Remove the references to the subpart requirements as they may not apply to all entities and remove the quarterly requirement such that Part 2.6 becomes: “Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months.” ***Guidelines and Technical Basis*** Align the drawings and wording in the guidelines and technical basis with the requirement language.
Yes
Guidelines and Technical Basis Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity’s control.
No
Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. ***Requirement R4, Part 4.1*** EEI members are concerned with unnecessary administrative burdens created by Part 4.1. For example, Authorization generally applies to users. A user of a Transient Cyber Asset should be authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. {Suggested Revision} EEI does not have a specific revision to suggest to address these concerns; however, we recommend a careful review of the specific concerns and suggestions raised by Registered Entities to help reduce the administrative burden of this part. ***Requirement R4, Part 4.7*** The requirement should be tied together better such that it clearly allows mitigation instead of patching, when justified. {Suggested Revision} Condense the language into one sentence to help clarify the requirement. For example: “Evaluate Transient Cyber Assets, within 35 calendar days prior to use, for applicable security patches and take one of the following actions: (1) apply the applicable patches, or (2)create a dated mitigation plan, or (3) Revise an existing mitigation plan.” ***Guidelines and Technical Basis *** The Part 4.1 guidance conflicts with the “Applicable Systems”. The guidance says the requirement (R4) “applies to any transient devices”, yet the “applicable systems” in the requirements tables are not the transient devices. {Suggested Revision} Edit the language under Requirement R4 to: “This Requirement applies to Transient Cyber Assets and Removable Media that will be connected temporarily to an applicable system. Examples of these hardware/software devices include, but are not limited to: - Diagnostic test equipment - Packet sniffers - Devices used for BES Cyber System

maintenance - Devices uses for BES Cyber System configuration - Devices used to perform vulnerability assessments” The guidance for Requirement Part 4.1, says “Requirement Part 4.1 requires the entity to document and implement its process to authorize the use of Transient Cyber Assets.” Requirement R4, Part 4.1 says “Authorize the usage of Transient Cyber Assets ***prior to initial use***, except for CIP Exceptional Circumstances.” (emphasis added) The guidance language should be edited to be consistent with the standard’s requirement. Bullet 2, under Requirement Part 4.1, says “It may be reasonable to have separate Transient Cyber Assets for each impact level.” Requirement R4, Part 4.1 is focused on High and Medium Impact BES Cyber Systems, not all BES Cyber Systems. The language in bullet 2 includes “low impact,” which is not an applicable system for this requirement. Therefore the guidance goes beyond the scope of the standard. This guidance should also be edited to be consistent with the language of the standard’s requirement.
No
Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described below. ***BES Cyber Asset – CIP-002.5.1 Guidelines and Technical Basis*** The definition of BES Cyber Asset is inaccurately quoted on p.17 of the Guidelines and Technical Basis section of CIP-002-5.1 (guidance), which creates opportunities for confusion and misinterpretation. A BES Cyber Asset is a “Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which , if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.” By contrast, p.17 of the guidance inaccurately quotes the final phrase of the BES Cyber Asset definition as follows: “…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact [sic] the reliable operation of the BES.” This mistake in the guidance introduces an unfortunate source of potential confusion about this important definition. This error should be corrected. {Suggested Revision} In guidelines, p.17, under heading “CIP-002-5.1,” replace second sentence with the following: “The Glossary defines a BES Cyber System as ‘[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.’ The term BES Cyber Asset is defined as follows: “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.” Generally speaking, the definition of BES Cyber Asset encompasses those programmable electronic devices that could relatively quickly (within 15 minutes) have an adverse impact on BES Facilities, systems, or equipment (without regard for redundancy) which would, in turn, affect the reliable operation of the BES.” ***Removable Media*** There is a consistency issue. The definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to; however, the definition for Removable Media is not. It can be implied that the definition refers to connection to applicable systems, but it is not clear. It would also be clearer to switch the order of the Removable Media and Cyber Assets in the last sentence. {Suggested Revision} Change the definition of Removable Media to: “Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
Yes
EEI supports the removal of the identify, asses, and correct language due to the expectation that NERC will refine its compliance and enforcement process under the Reliability Assurance Initiative (RAI) to move away from a zero tolerance approach to compliance. We expect the new RAI to be finalized prior to final ballot to address the zero tolerance concerns that the identify, assess, and correct language intended to address.
No
Whether the timeframes in the implementation plan are reasonable and appropriate depends upon how and when the other concerns in these comments are addressed. EEI answered no to this question due to the specific concerns described in these comments.

Yes
EEI greatly appreciates the work of the Standards Drafting Team and the NERC staff. We support the efforts to have a consolidated revision to cover both the date sensitive and other FERC directives in a single filing. CIP-002-5.1, CIP-005-5 and CIP-008-5 were not opened for revisions, comments or ballot. These standards contain one or more items that need to be updated to maintain consistency with the CIP standards which were opened. There are also items which need to be addressed to provide clarity for implementation and auditability. We respectfully request that the Revisions Standard Drafting Team make these “conforming changes” and other changes to the three standards regardless of whether they are opened for any other revisions. Examples include: (1) CIP-002-5.1, CIP-005-5 and CIP-008-5 all, in section 5, reference effective dates. These all need to be updated to be consistent with the effective date of the standards which were opened for revision. (2) CIP-005-5 and CIP-008-5, in section 6, reference CIP-003-5, CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5 and CIP-010-1 and CIP-011-1. These references need to be updated to reflect -6 and -2 as appropriate. Although the RSAWs are not included in the Standards Development ballot and comment process, they are an essential aspect of Compliance Monitoring functions related to the NERC Reliability Standards. When reviewing Reliability Standards, RSAWs are reviewed as a fundamental component of the end to end review process much like definitions. As a result, EEI members ask NERC and the Standards Drafting Team to collaborate on the RSAWs to identify how comments filed separately (i.e., the standards comments and RSAW comments) will be addressed to ensure the integrity of the CIP V5, V6 Standards. Specifically, the proposed RSAWs materially change the scope and intent of the standards because they (1) impose new obligations that exceed the requirements of the standards, (2) add unnecessary administrative burdens, and (3) are inconsistent. Please see EEI’s RSAW comments filed separately for additional detailed comments.
Group
Seattle City Light
Paul Haase
No
The term "portable" in "removable media" may add confusion. Suggest striking "portable" and replacing with "removable without powering down cyber system."
Yes
SCL supports the approach to use RAI concepts to take the place of IAC language.
Yes
For consistency across Standards, Seattle supports a change in presentation of controls for LOW-ranked facilities and systems. LPPC and Seattle prefer that the controls for Lows be removed from CIP-003 and moved to the appropriate Part of each applicable Standard (i.e., Awareness activities for LOWs should be found with other Awareness activities in CIP-004-6, Incident Plan controls for LOWs should be found with other Incident Plan controls in CIP-008-6, and so forth). However, Seattle is aware of the substantive additional tracking burden this approach will place on small entities having only LOW-ranked facilities and system, and suggests the following alternative: 1) revised Standards as above, to include all activities for LOW-ranked facilities and system in their appropriate parent Standard. 2) Change the applicability section of these Standards (CIP-003 to CIP-011) to be applicable ONLY to registered entities with ONE or MORE facilities/systems ranked HIGH or MEDIUM through application of CIP-002-5. 3) add a new Standard CIP-012-1 that is applicable ONLY to entities with NO HIGH OR MEDIUM facilities/systems identified through application of CIP-002-5. This Standard simply collects all requirements/controls for LOWs in one place. In no case will requirements/controls for LOWs identified in new CIP-012-1 differ from those in CIP-003 to CIP-011; CIP-012 is intended as a solution that makes clear the obligations for LOW-only entities. Finally, if a new CIP-012-1 Standard is deemed impractical, Seattle strongly recommends that NERC develop an administrative solution that will very clearly identify the

obligations for LOW-only entities, perhaps by maintaining a list or spreadsheet that is kept with the CIP Standards.
Individual
Stacy Bresler
Individual
Individual
Si Truc PHAN
TransEnergie Hydro-Quebec
Individual
Mike Marshall
Idaho Power
No
CIP-003 R2.1 to R2.6: The applicability section of all these requirement parts addresses Low Impact BES Cyber Systems. It is counterintuitive to think that a list of Low Impact BES Cyber System will not be required to show compliance. CIP-002 also explicitly states that a list of Low Impact BES Cyber Systems is not required. This creates increasingly burdensome administrative work on the registered entities. The requirements for the Low Impact Assets should be measureable but not require registered entities to produce a list of Low Impact BES Cyber Systems as it would be contrary to the CIP-002 wording. The wording of these parts should be adjusted to address the Low Impact Assets and not the Low Impact BES Cyber Systems. CIP-003 R2.4 greatly increases the scope of the Low Impact requirements. Registered entities will be required to implement “identified access point(s)” for Low Impact BES Cyber Systems of which registered entities are not required to maintain a list. This will essentially require registered entities to provide a list of all Low Impact BES Cyber Systems which is explicitly stated is not required in CIP-002. Except for the time frame requirement CIP-003 R2.5 mirrors the CIP-008 requirements. Wouldn’t it be more appropriate to word the CIP-008 parts to be more all encompassing rather than creating a new requirement and part that creates additional administrative burden on the registered entities? Incident response is often handled through similar processes regardless of the impact of the system and is then categorized as a part of the incident handling process. By creating separate requirement in CIP-003 and CIP-008 it will different incident response plans each with their own evidence or the same plan that complies with both requirements with duplicate documentation and effort to show compliance with two separate standards. CIP-003 R2.6 is very similar to CIP-004 R1.1 and should be incorporated into CIP-004 R1.1 rather than having to duplicate administrative effort to show compliance with two awareness programs.
No
No issue was noted with the requirement CIP-006 R1.10 as it is written. However, it does little to meet the directive that was given in Order 791 to “create a definition of communication networks and to develop new or modified” standards. Communication components are an important part of the reliability of the grid and a definition of what and how the regulators expect the registered entities to comply with protecting them and all their many potential configurations would be an important step towards better security.
Yes
Yes
No
It is concerning that the “Identify, Assess, and Correct” (IAC) language has been so quickly discarded when it was added to move the regulations away from a zero defect approach. The RAI project certainly has potential but is still in various pilot projects that have not yet born widespread benefits to the industry. There did not seem to be any project teams focused on attempting to reword the IAC language to rectify some of the issues that were voiced and now the industry, that approved the v5 standards with the understanding the IAC language would help to move the regulations away from a zero-defect approach, is left with no time frames or guarantees of what the

RAI will become or when it will be implemented. More work should be done see if there is a way to fix the IAC language prior to it be discarded.
Yes
No
No
Individual
Heather Laws
PNM Resources
No
General #1: Limit the scope of dispersed generation in the CIP-003-6 Applicability section, similar to PRC-005. In section 4.2.2 of the Introduction section, under 4. Applicability, 4.2 Facilities, add the following statement after 4.2.2 All BES Facilities, “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back the reference to CIP-002-5 Requirement R1.3 in CIP-003-6 R2. PNM agrees with the suggested revision posed by EEI. General #2: A number of the requirements are effectively duplicated language of existing CIP requirements. PNM strongly disagrees with the concept that Low Impact controls should be within one requirement. It begs the question why the SDT would not do the same for Medium and High, but the answer is obvious: it is not efficient. Low Impact requirements that are effectively duplicating existing requirements need to be removed and “Low Impact BCS” added to the impacted systems (applicability section) of the respective existing requirements. Having all the Low Impact controls under CIP-003-6 R2 make this requirement a “spaghetti” requirement that the SDT said would not be the updated version of the standards. Entities do not need to deal with the monitoring and enforcement implications of another “spaghetti” requirement if they should happen to have a potential violation of this requirement. R2.1: Update as an open-ended ‘pointer’ to other Low Impact requirements. Suggested alternative re-write: “Review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the topics in all enforceable CIP requirements applicable to Low-Impact BES Cyber Systems.” With such a rewrite, there’s also no reason this could not be changed to a separate CIP-003-6 R1.2 requirement. Rename R1 content to be R1.1, and include initial R1 language using the ‘starter’ language common in most other CIP requirements. R2.2: Does not identify the types of access restrictions required. Strictly speaking, a simple unlocked door still ‘restricts access’, even if it can be readily opened by turning the knob. Is this acceptable? PNM suggests that without clearer language or enforceable guidance, regional auditors will take their own initiative to self-interpret and be highly prescriptive in this regard as to what is ‘acceptable’. Entities will be at the whim of regional variances and auditor discretion. As implied above, adherence to the guidelines is not a reliable expectation to establish compliance assurance unless NERC can forthwith declare Guidance as an enforceable component of the standard. R2.3.1: Escorting where? It is only ever implied that a physical security perimeter of some sort must be established, and yet the only way to enforce and audit compliance with many of the R2 requirements is to physically create one. This sub-requirement also relies on the controls of R2.2, even though R2.2 states as allowing for operational or procedural control. Procedural controls alone cannot be reliably audited vis-à-vis R2.3.1 to ensure escorting. Regional auditors may necessarily force physical controls, regardless, as part of their ‘auditing approach’, undermining the allowances within the standard. The SDT will have pushed Low Impact BCS into Medium CIP-006-6 territory, effectively negating the very reason for writing the remaining separate physical security sub-requirements below. R2.3.2: in order to monitor physical access points they must be identified, which means that, again a physical construct must be defined to identify the access points into it, which means that the perimeter must be controlled at all other non-access locations, which means that the entire exercise of this requirement defaults back to operating effectively similar to CIP-006.

PNMRs concern is that regional auditors will be given significant latitude as to how they wish to interpret the ‘effectiveness’ of the controls, and thus by extension an entity’s compliance with the requirement. • How does one prove that monitoring is continuously implemented, without having some form of logging? R2.4.1: Suggested alternative re-write: “The electronic access point(s) of all external routable protocol paths to Low Impact BES Cyber Systems, if any, must be identified.” Access points are modified by identifying ‘electronic’… otherwise, every routable connection in fact has a physical access point into the facility and it can be readily identified. R2.4.2: Suggested alternative re-write: “For each identified external routable protocol electronic access point, if any, require inbound and outbound access control rules, including the reason for allowing access, and deny all other access.” The terms ‘permissions’ and ‘granting’ could also potentially imply expected authorization activities, which is not what this requirement is supposed to be overseeing. Unfortunately CIP 005-5 R1.3 suffers the same flaw, and should also be fixed. R2.4.3: Since some regional auditing entities do not understand the strict meaning of the words “authentication” and “authorization”, what constitutes authentication in this case needs to be clearly prescribed (NEEDS NEW GLOSSARY DEFINITION). Perhaps a cross-reference to NIST Special Publication 800-63 would be appropriate, or at least a Guideline reference to it. R2.5: This is an unnecessary and duplicative requirement. There’s no clear reason why Low Impact BCS cannot/should not be added to “Applicable Systems” within the CIP-008 standard in lieu of this sub-requirement. Update CIP-003-6 R2.1 to point to this standard. R2.6: This is an unnecessary and duplicative requirement. Again, just add Low Impact BCS to CIP-004-6 R1/R1.1 “Applicable Systems” in lieu of this sub-requirement, and update CIP-003-6 R2.1 to point to this standard. Ironically, this requirement even has additional specific and more-stringent reviews and documentation requirements (assurance of topical coverage annually) than are necessary for Medium and High BCS under CIP-004-6 R1/R1.1. The explanation recently provided by SDT personnel (at the 6/19/2014 SDT webinar) is appreciated, but it nonetheless continues to violate the new NERC standards design methodology.
Yes
Guidelines and Technical Basis Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity’s control.
No
PNMR agrees with the comments posted by EEI.
No
PNMR agrees with the comments posted by EEI.
Yes
PNMR agrees with the comments posted by EEI.
Yes
No
Group
Bureau of Reclamation
Erika Doot
No
CIP-003-6 R2.4.2 - Reclamation suggests that the requirement should be clarified so that restrictive routing schemes are considered sufficient access permissions.
No
CIP-006-6 R1.10 - Reclamation suggests that the requirement should be clarified to account for situations where cabling outside the PSPs is located in the same facility as the separated PSPs and that facility provides physical access only to authorized personnel. For these cases where installation of conduit is not possible and installation of encryption is not technically feasible, it should be clarified that physical access controls to the facility can provide adequate protections and are compliant with the standard. Therefore, Reclamation suggests that the list of acceptable physical access restriction examples in the Measures be updated to include “facilities that provide physical

access only to authorized personnel” in addition to “cabling and components secured through conduit or secured cable trays.”
No
CIP-010-2 R4.1.4 – Reclamation suggests that the drafting team add a bullet to the Measures that allows “an automated scan of the Transient Cyber Asset” prior to use on the ESP network as evidence for satisfying this requirement. CIP-010-2 R4.6 - Reclamation suggests that the drafting team add a bullet to the Measures that allows “an automated scan of the Transient Cyber Asset” prior to use on the ESP network as evidence for satisfying this requirement. CIP-010-2 R4.7 - Reclamation suggests that the drafting team add a bullet to the Measures that allows “an automated scan of the Transient Cyber Asset” prior to use on the ESP network as evidence for satisfying this requirement.
Yes
Yes
Yes
No
No
Individual
Thomas Breene
Wisconsin Public Service
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
No
These comments are submitted on behalf of the following PPL NERC Registered Affiliates: LG&E and KU Energy, LLC; PPL Electric Utilities Corporation; PPL EnergyPlus, LLC; PPL Generation, LLC; PPL Susquehanna, LLC; and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP. Comments: Would like to see the tie between CIP-002-5 R1.3 added back to the requirement, instead of just saying “containing low impact BES Cyber Systems”. Do not understand the removal of this tie in to CIP-002. For R2.4 shouldn’t the Applicable Systems section list “Low Impact BES Cyber Systems with external routable protocol paths Low Impact BES Cyber Systems with dial-up connectivity”, thus allowing Entities without those paths and/or connectivity, the option of not worrying about this requirement and just documenting the absence of the path and/or connectivity. For R2.6 revise the requirement to clarify the intent as follows: Implement a security awareness program that reinforces cyber security practices at least quarterly. At least once every 15 calendar months the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.
Yes
Including them in one place allows for concise understanding, however, a concern is that the auditors will look to the other requirements for measures or expectations of evidence. It needs to be clear, that while the requirement “mirrors” or is similar to one for High/Medium Impact Assets, the only option for audit and evidence resides within CIP-003 R2
No
Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity’s control.
No

No
Add a clarification that entities are not expected to enforce CIP 006 on third party nonprogrammable components that are out of the entity’s control
Yes
We assume this applies to R2, part 2.1.9, since there is no R1, part 1.1.9.
Yes
Individual
Bill Fowler
City of Tallahassee, TAL
No
The City of Tallahassee (TAL) feels that Part 2.4 does not adequately illustrate the measures necessary to prove compliance to the part 2.4.2 requirement. The term ‘representative sample’ needs to be defined specifically. Does this imply a sample of rule sets from more than one access point? A sample of the rule set from a single access point? If more than one access point is identified, then would the entire rule set, or only a partial rule set from a single access point qualify as a representative sample? There can be no ambiguity when direct evidence is required as proof of compliance. Part 2.4.1 states that all external routable protocol paths, if any, must be through one or more identified access point(s). Evidence includes documentation of these paths through identified access points. If there is no requirement to discretely identify low impact BES Cyber Systems, then how can we be expected to provide evidence for this requirement when we are not required to identify the access point in the first place? External routable protocol paths imply the existence of an electronic security perimeter, a specific set of connected assets that form a basis for a defined network structure. There is no language in this requirement to identify an electronic perimeter, therefore no conceptual reason to identify an access point with routable protocol paths that may or may not be external to an undefined barrier. The language of this particular requirement and the measures required to prove compliance are extremely vague. Parts 2.1 – 2.3, and 2.5 are sufficient to address FERC Order No. 791 paragraphs 106-100, and clearly provide substantive objective criteria to sufficiently measure an entity’s protection of low-to-no impact cyber assets. Requiring entities to identify assets (access points) where asset identification is clearly stated as unnecessary, and provide representative samples of configurations for these unidentified assets, assets that function as external access gateways to an undefined electronic security perimeter, could create an unnecessary quagmire of compliance effort. Under the section Guidelines and Technical Basis for part 2.4 it states that the Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. There is an assumption made here that at least one or more external routable protocol and/or Dialup connectivity paths exist and those access paths are being utilized to communicate directly with the asset from a remote location. This language should be rewritten to match the requirements in Part 2.4 – removing any unnecessary ambiguity with regard to direct communications pathways vs. other reasons for necessary connections via remote communications paths; e.g. “The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths, if any, to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected.” Furthermore, the following sentence should be rewritten to state, “In cases where external connectivity is used to gain access to any low impact BES Cyber System at a remote site, electronic access controls should address the risk of using external connectivity.” The final two sentences in this paragraph contain references to ambiguous concepts such as collection and aggregation, without stating specifically what kind of information might be collected and/or aggregated. TAL’s contention is that these two sentences add nothing to the explanation and should be removed entirely. They state that these access controls are required to protect the collection and/or aggregation of low impact BES Cyber Systems, or the collection and/or aggregation of data pertaining to them, or what specifically?
Yes

No
Part 4.3 is identical to Part 4.2. I suggest collapsing 4.3 into 4.2 to include ‘prior to use on applicable systems’. Both requirements are obviously meant to be done prior to use on applicable systems (intent of the standard in the first place), so there is no point in stating the same requirement twice. If the intent of this revision is meant to protect applicable systems, then the only requirement necessary is 4.3. If both requirements must stay, then remove the word ‘detect’ from 4.2 as detection is required prior to use as part of 4.3. It makes the most sense to collapse the two requirements into one and adjust the Measures language to include hardening policies and scanning techniques as part of the traditional antivirus … example.
Yes
No
I have no recommended alternative approach as I believe the original IAC language in the standard identified with a need to change industry perception of the spirit and intent of Critical Infrastructure Protection Reliability Standards to concentrate effective proactive compliance efforts towards identifying and correcting deficiencies rather than being focused on the fact that violations for those deficiencies may exist and subsequently turning the workplace into a reactive, audit documentation mill. The many changes in Violation Severity Levels in the revised standard will effectively result in potential violations regardless of any effort (or lack of effort) on the part of the entity to mitigate those violations. Now, with the IAC language removed, entities are no longer provided a much-needed greater degree of flexibility in detecting and remediating low-risk violations. All and any interpretation of the standards has been placed into the hands of auditors, which contributed to endless anxiety on the part of the entities with prior CIP versions. FERC stated concern over the broad and ambiguous nature of the IAC language as sufficient reason to force NERC to improve upon how the (IAC) language was written. As a result, NERC decided to assume that the enforcement process for low-risk violations would be unworkable, and remove the language altogether. This effectively disenfranchises the entity throughout the compliance auditing process.
No
Given the nature of the removal of the IAC language which results in a measurable change in how compliance programs would function under the new standard, FERC should issue an order to extend the effective date at least another full 6 months for each standard/requirement for which a modification to the language was made.
No
No
Individual
Megan Wagner
Westar Energy
Individual
David Jendras
Ameren
Individual
Ayesha Sabouba
Hydro One
No
Currently, all of the new requirements for addressing FERCs concerns about Low Impact BES Cyber Assets have been shoe horned into the Standard on Security Management Control even though many requirements mirror those covered in other Standards for High and Medium Impact assets. For instance, requirements related to physical access controls for Low Impact assets appear in CIP-003 whereas physical security requirements for other asset types appear in CIP-006. Requirements related to Incident Management for Low Impact assets appear in CIP-003 even though Incident Management for Medium and High Impact Assets is covered in CIP-008, and so on. This leads to a

needlessly confusing set of standards where reference needs to be made to multiple requirement statements in multiple standards simply to determine what needs to be done in a particular subject area. This increases the effort needed to implement the Standards, increases the effort needed to demonstrate compliance, is likely to lead to duplication of effort, and could increase the likelihood that Responsible Entities will overlook or misunderstand some requirements. Requirements for Low Impact assets that mirror requirements appearing in other Standards for High and/or Medium Impact assets should be moved to those other standards. 1. In the text of the first sentence of R2, delete the words “assets containing”. As the wording currently stands, all Low Impact BES Cyber Assets would have to be located within some sort of “container” (eg. a building or yard) and the protections stipulated by Requirements R2.1 through R2.6 would have to be applied to the entire container, not simply to the Low Impact Cyber Assets themselves. 2. For Requirement R2.4: a. Demonstrating auditable compliance with R2.4.1, R2.4.2, and R2.4.3 appears almost certain to require Responsible Entities to create and maintain inventories of Low Impact Cyber systems and their associated access points and permission sets, as well as an inventory of all Low Impact assets with dial-up connectivity. This is not consistent with the statement made in the “Rationale for Requirement R2” which states that, “creating and maintaining an inventory of low impact assets for audit purposes would be unduly burdensome…..”. b. Requirement 2.4.1 refers to an “external” routable protocol path. External to what is unclear. The current wording could be read as “External to the Low Impact BES Cyber System concerned”, external to a Low Impact BES Cyber Asset, external to some (as yet unspecified) “electronic communications perimeter within which the Low Impact BES Cyber System resides”, or perhaps “external to the physical enclosure that “contains” the Low Impact BES Cyber Asset” (as implied by the unmodified text of R2). This needs to be clarified. c. As currently written, Requirement R2.4.2 applies in cases where communication with low impact assets is either routable or non-routable. This requirement provides little, if any, additional security if communications are not routable. d. Clarify whether or not the term “access point” in R2.4.2 includes places where one connects transient devices and/or removable media? 3. Modify the wording in the Table of Compliance Elements as follows: The High VSL for R2 should be revised to read, “…..but failed to address three or more of the topics as required by Requirement R2, Part 2.1 (2.1)…..”
Yes
Request CIP-007 R1 Part 1.2 Rational to be added to guidance and additional guidance provided. Suggest illustrative examples so that Entities and Auditors reach the same interpretation
Yes
1. In CIP-004 Requirement 2.1.9 delete the word “including”. Neither Transient Cyber Assets nor Removable Media are Cyber Assets. 2. In CIP-010: a. Requirement 4.1 refers to “Authorization” of usage, users, locations, acceptable use, and firmware/software. The Requirement should state clearly who it is that can provide this authorization. Possibilities include the CIP Senior Manager or Delegate, a person or group identified in the access management program pursuant to CIP-004 R4 (specifically R4.1), or the “individual or group with authority to authorize baseline changes as per Requirement CIP-010 R1.2. Recommend documented authorization as an option b. In Requirement 4.1.4 delete the word “intentionally”. Software that is installed unintentionally or illicitly should not be permitted unless it is known to be benign. c. In Requirement 4.1.4, reword Requirement 4.1.4 to read, “Operating system, firmware, installed software, including installed updates and patches, on Transient Cyber Assets (per Transient Cyber Asset Capability) d. Reword Requirement 4.3 to read “Use method(s) to detect malicious code on Removable Media and Transient Cyber Assets prior to their use on, or with, applicable systems” e. Reword R4.4 to state, “Remove or disable all malicious code detected on Transient Cyber Assets and Removable Media prior to use in, or with, Applicable Systems”. f. Reword the first portion of Requirement 4.6 to read, “Prior to use, and except under CIP Exceptional Circumstances, evaluate Transient Cyber Assets for modifications that deviate from the authorized configuration”. Reword the second portion of Requirement R4.6 to read, “for a modification that deviates from an authorized configuration, either; a) remediate by returning the Transient Cyber Asset to the most recently authorized configuration prior to use; or b) authorize the new configuration prior to use, including the parameters listed in Requirements 4.1.1 through 4.1.4 3. Reword to state that the transient cyber asset must not be interconnected between a higher security zone and a lower security zone – i.e. must not be “dual homed” 4. There need to be Requirements pertaining to the re-purposing and destruction of Transient Cyber Assets and Removable Media. This could be accomplished by expanding the scope of Applicable Systems in CIP-

011 R2 to include Transient Cyber Systems and Removable Media, or by mirroring the language of that set of Requirements.
Yes
1. The definition of “Transient Asset” should include devices which connect temporarily to EACMS (which are on, not “within”, the ESP) and/or PACS. This would provide a measure of configuration control and malware prevention to systems which are essential to the protection of BES Cyber Assets and their associated networks. For instance, without this protection a Transient Device with a legitimate connection at an ESP access point could, if compromised, jeopardize the effectiveness of the access control and/or the capability of networks or devices within the ESP.
Yes
No
Please provide a clear and consistent time line for implementation of these requirements. Ensure that all new effective and mandatory dates are after their CIP V5 dates. The current format is confusing.
No
Yes
Hydro One supports TFIST recommendations on NERC Project 2014-02 CIP Version 5 Revisions Standard. Drafting Team should be allowed to help clarify and provide guidance for industry issues and items discovered in the pilots. Hydro One also agrees that In particular the following should be addressed by NERC with the SDT representing industry: 1. Transfer Trip: CIP-002-5 R1, ‘transmission stations and substations’ for medium category assets, what some refer to as the “transfer trip” issue. 2. Clarify the term “programmable devices” which is an undefined term open to strongly differing viewpoints. 3. Clarify “effect within 15 minutes” issue and the burden of evidence for proving that something does not exist. Please clarify if diversity vs redundancy can be considered as part of the Entity’s impact assessment (i.e separate system using a different technology) Recommend adding “or” to CIP-010 R4 Part 4.1.4 to make this Part consistent with CIP-010 R1 Part1.1.1. Part 1.1.1 requires a baseline of Operating system(s) (including version) OR firmware where no independent operating system exists; while Part 4.1.4 requires Authorization to include Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability). Part 4.1.4 requires Authorization of both Operating System AND Firmware for a transient device while Part 1.1.1 requires baseline of Operating System OR firmware. We suggest the proper approach is to retain the OR. When applying R4 to a laptop we normally record the OS and version and not look to the firmware BIOS.
Individual
Steve Hamburg
Encari
No
Supporting Comments Requirement R1.2 pertains to a required policy for “Electronic Security Perimeters (CIP-005) including Interactive Remote Access” but the required implementation of that policy appears to have a broader scope in Requirement R2.4.1 which pertains to required processes for “All external routable protocol paths, if any, must be through one or more identified access point(s).” The latter requirement, R2.4.1, is not limited to interactive remote access that is the subject of R1.2. The Rationale for R2 explains the phrase “external routable protocol paths” is used instead of the defined term “External Routable Connectivity” because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term “External Routable Connectivity” in the context of Requirement R2 is not appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems. Inconsistently, the Guidelines and Technical Basis section continues to use the term “external routable connectivity” in the discussion of R2 in the two statements below: “2.3 – The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required.” 2.4 … “An asset has

external routable connectivity due to a BES Cyber System within it having a 3G/4G wireless card on a public carrier which allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.”
No
Supporting Comments The applicable scope of CIP-010-2 R4 is too narrow; it should be expanded to include the EACMS and PACS that are associated with High and Medium Impact BES Cyber Systems. EACMS and PACS need to use method(s) to deter, detect, or prevent malicious code on Transient Cyber Assets (per Cyber Asset capability). The omission of EACMS and PACS from the scope of protection under CIP-010-2 R4 is inconsistent with the protections afforded to EACMS and PACS under CIP-007-6. CIP-007-6 Requirement 3.1 provides that High and Medium Impact BES Cyber Systems, and their associated EACMS, PACS, and PCA must deploy method(s) to deter, detect, or prevent malicious code.
Yes
Individual
Daniel Gibson
KCPL
No
R2 – Usage of the term “external routable protocol paths” should be officially defined by NERC before being able to “judge the sufficiency” of the newly introduced controls. Assumptions a responsible entity could make surrounding this term could lead to violations. The Guidelines and Technical Basis section includes numerous references to “belief” and “intent,” along with descriptions of what entities “should” be doing. The need for such language indicates that the requirement language is not able to stand on its own and results in a need to be audited by the Guidelines and Technical Basis section. In turn, language not intended to be a required action by the entity could result in a perceived additional requirement by those trying to understand the requirement. While the intent of the “Note:” section under CIP-003-6 R2 is understood, there is no way to effectively audit for the successful and complete implementation of CIP-003-6 Table R2 – Low Impact Assets without obtaining an inventory of considered assets and of authorized users. Auditors are not able to reliably issue a judgment of the effectiveness of an internal control or of adherence to requirements without ensuring that samples are pulled from a complete population. Furthermore, entities are not able to perform the functions outlined within the R2 requirements without having lists of authorized users, both for access authentication and monitoring purposes. R2.3.2 – In part because the reference to “physical access point(s)” is not in relation to a defined Physical Security Perimeter, the requirement is actually more stringent than that of CIP-006-6 R1.4 and could require more evidence in support of compliance. An entity may need to prove an evaluation was performed resulting in the derivation of an inventory of all potential access points for all Low Impact BES Cyber Systems at Control Centers. Furthermore, diagrams may be needed to support that monitoring has been considered and defined for all applicable access points. While intended to be helpful in aggregating all Low Impact BES Cyber Systems requirements into a single section, the table has resulted in a web of functionally similar, yet separated requirements that could result in confusion. KCP&L recommends that, wherever possible, the items from CIP-003-6 Table R2 – Low Impact Assets be moved to the appropriate functional section and included as an additional applicable system where requirements are also similar. R2.4 – The requirements established under R2.4 are redundant to CIP-005-5 R1. In order to effectively audit the implementation of such controls, inventories and lists will be required just as they will be for CIP-005-5 R1. Guidelines and Technical Basis Section 2.4 – The two sentences beginning with “The electronic access controls should address…” go beyond the purview of the language of the requirement and serve to dictate what “should” be addressed. It is recommended that these sentences be stricken from the Guidelines and Technical Basis section.

No
CIP-006-6: The current order and applicability for CIP-006-6 is inconsistent and does not logically flow. At no point is a requirement for use of a defined PSP introduced, yet a number of the requirements pertain exclusively to the existence of a defined PSP. Physical Access Control Systems, as defined by the NERC Glossary of Terms, are also not stated as being required. Due to the current combined applicability and requirements, an entity could theoretically have a High Impact BES Cyber System that does not reside in a PSP and does not have a Physical Access Control System. This could result in applicability of only CIP-006-6 R1.3 and R1.10, and a lack of requirement for operational or procedural controls to restrict physical access. While the entity would still have to achieve two or more physical access controls, the requirements never state that a PACS is required for a High Impact BES Cyber System to achieve this or that a PSP is required for any system. KCP&L recommends that either CIP-006-6 R1.1 be updated to require the use of a Physical Access Control System for High Impact BES Cyber Systems or that a new sub-requirement is created to require High Impact BES Cyber Systems to have a Physical Access Control System with defined operational or procedural controls to restrict physical access. In addition, consideration should be given to rewording some monitoring, logging, and alerting requirements to include monitoring, logging, and alerting provisions for non-PSP, physically protected areas. CIP-007-6 The term “nonprogrammable communication components located inside both a PSP and an ESP” is a new source of confusion and may require definition as an official NERC Glossary term. CIP-005-5 requires only for “Cyber Assets” to reside within an ESP. Unofficial guidance has already been communicated by various Regional Entities in support of excluding non-Cyber Asset, nonprogrammable “devices” from the required ESP. Therefore, it is difficult to identify where a “nonprogrammable communication component” that is also not a Cyber Asset would be located inside an ESP. Additionally, while CIP-006-6 defines certain protections that must be afforded to a Physical Security Perimeter, there is no requirement stating that a device must reside within a defined PSP. Therefore, entities are allowed to utilize other operational or procedural control measures for protecting High and Medium impact ESPs. Even if a “nonprogrammable communication component” is defined as part of an ESP, it is possible that the “nonprogrammable communication component” will not reside within a defined PSP. It should also be noted that the addition of such language will result in increased burden for entities by nature of a backdoor requirement for documentation of all considered “nonprogrammable communication components” that are not NERC-defined “Cyber Assets.” The current proposed language applicable only to “nonprogrammable communication components located inside both a PSP and an ESP,” along with other PSP-specific requirements, may serve to discourage entities from creating defined PSPs around BES Cyber Systems.
No
The administrative burdens associated with this are not practical as a response and aligned with the risk introduced to the BES. KCP&L endorses those specific comments submitted by the Edison Electric Institute.
No
KCP&L believes that the definition of Transient Cyber Asset should be clear to ensure no unintended consequences from interpretations by stakeholders involved where direct connections of devices are anticipated. Physical and electronic access control to BES Cyber Systems is a critical component of securing the overall system, and such devices should be protected from inappropriate Transient Cyber Asset connections. But the definition of such lacks clarity and thus will lack consistency in application. The language around the Transient Cyber Asset and Removable media is silent and unclear where EACMS and PACS are concerned. The new definition could read as follows: Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Assets associated with an ESP. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Yes
While KCP&L supports alternative methods of assessing maturity and effectiveness in adherence to the NERC CIP requirements, the “Identify, Assess and Correct” language was an open-ended and unstructured framework that would cause confusion and lead to the expansion of the scope of NERC CIP based on auditor judgment. This concept would be addressed in tools and frameworks accomplished through the Reliability Assurance Initiative (RAI), however, consistency in auditor training and approach will be critical to the success of the RAI program.

Yes
No
We are not aware of additional jurisdictions that should be considered at this time.
Yes
KCP&L would like to endorse those comments made in this question by the Edison Electric Institute.
Individual
Scott Langston
City of Tallahassee
No
The City of Tallahassee (TAL) feels that Part 2.4 does not adequately illustrate the measures necessary to prove compliance to the part 2.4.2 requirement. The term ‘representative sample’ needs to be defined specifically. Does this imply a sample of rule sets from more than one access point? A sample of the rule set from a single access point? If more than one access point is identified, then would the entire rule set, or only a partial rule set from a single access point qualify as a representative sample? There can be no ambiguity when direct evidence is required as proof of compliance. Part 2.4.1 states that all external routable protocol paths, if any, must be through one or more identified access point(s). Evidence includes documentation of these paths through identified access points. If there is no requirement to discretely identify low impact BES Cyber Systems, then how can we be expected to provide evidence for this requirement when we are not required to identify the access point in the first place? External routable protocol paths imply the existence of an electronic security perimeter, a specific set of connected assets that form a basis for a defined network structure. There is no language in this requirement to identify an electronic perimeter, therefore no conceptual reason to identify an access point with routable protocol paths that may or may not be external to an undefined barrier. The language of this particular requirement and the measures required to prove compliance are extremely vague. Parts 2.1 – 2.3, and 2.5 are sufficient to address FERC Order No. 791 paragraphs 106-100, and clearly provide substantive objective criteria to sufficiently measure an entity’s protection of low-to-no impact cyber assets. Requiring entities to identify assets (access points) where asset identification is clearly stated as unnecessary, and provide representative samples of configurations for these unidentified assets, assets that function as external access gateways to an undefined electronic security perimeter, could create an unnecessary quagmire of compliance effort. Under the section Guidelines and Technical Basis for part 2.4 it states that the Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. There is an assumption made here that at least one or more external routable protocol and/or Dialup connectivity paths exist and those access paths are being utilized to communicate directly with the asset from a remote location. This language should be rewritten to match the requirements in Part 2.4 – removing any unnecessary ambiguity with regard to direct communications pathways vs. other reasons for necessary connections via remote communications paths; e.g. “The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths, if any, to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected.” Furthermore, the following sentence should be rewritten to state, “In cases where external connectivity is used to gain access to any low impact BES Cyber System at a remote site, electronic access controls should address the risk of using external connectivity.” The final two sentences in this paragraph contain references to ambiguous concepts such as collection and aggregation, without stating specifically what kind of information might be collected and/or aggregated. TAL’s contention is that these two sentences add nothing to the explanation and should be removed entirely. They state that these access controls are required to protect the collection and/or aggregation of low impact BES Cyber Systems, or the collection and/or aggregation of data pertaining to them, or what specifically?
Yes
No

Part 4.3 is identical to Part 4.2. I suggest collapsing 4.3 into 4.2 to include ‘prior to use on applicable systems’. Both requirements are obviously meant to be done prior to use on applicable systems (intent of the standard in the first place), so there is no point in stating the same requirement twice. If the intent of this revision is meant to protect applicable systems, then the only requirement necessary is 4.3. If both requirements must stay, then remove the word ‘detect’ from 4.2 as detection is required prior to use as part of 4.3. It makes the most sense to collapse the two requirements into one and adjust the Measures language to include hardening policies and scanning techniques as part of the traditional antivirus … example.
Yes
No
I have no recommended alternative approach as I believe the original IAC language in the standard identified with a need to change industry perception of the spirit and intent of Critical Infrastructure Protection Reliability Standards to concentrate effective proactive compliance efforts towards identifying and correcting deficiencies rather than being focused on the fact that violations for those deficiencies may exist and subsequently turning the workplace into a reactive, audit documentation mill. The many changes in Violation Severity Levels in the revised standard will effectively result in potential violations regardless of any effort (or lack of effort) on the part of the entity to mitigate those violations. Now, with the IAC language removed, entities are no longer provided a much-needed greater degree of flexibility in detecting and remediating low-risk violations. All and any interpretation of the standards has been placed into the hands of auditors, which contributed to endless anxiety on the part of the entities with prior CIP versions. FERC stated concern over the broad and ambiguous nature of the IAC language as sufficient reason to force NERC to improve upon how the (IAC) language was written. As a result, NERC decided to assume that the enforcement process for low-risk violations would be unworkable, and remove the language altogether. This effectively disenfranchises the entity throughout the compliance auditing process.
No
Given the nature of the removal of the IAC language which results in a measurable change in how compliance programs would function under the new standard, FERC should issue an order to extend the effective date at least another full 6 months for each standard/requirement for which a modification to the language was made.
No
No
Group
Florida Power & Light
Mike O'Neil
Yes
Based on proposed revisions in the applicability section of the Generator Owner and Generator Operator Reliability Standards for PRC-005-2 (-3) and the approved CIP-002-5.1 Attachment 1 medium impact rating criteria 2.1, the following revisions to the applicability section of the CIP-003-6 Reliability Standard are recommended: Add a statement under 4.2.2 in the Facilities portion of the Applicability Section as follows: 4.2.2 Responsible Entities Listed in 4.1 other than Distribution Providers All BES Facilities. For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in

Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level. Proposed text for the guidelines and technical basis for this change parallels the text for similar changes to PRC-005-2 (-3): Applicability of the Requirements of CIP-003-6 to dispersed power producing resources is qualified in section 4.2.2. The intent is that for such resources, the Requirements would apply only to BES Cyber Systems used from the point where the BES dispersed power producing resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or higher and not at an individual turbine, inverter or unit level.
Group
Iberdrola USA Networks
John Allen
Group
Florida Municipal Power Agency
Carol Chinn
No
FMPA appreciates the SDT’s efforts on this difficult task. We particularly appreciate all the outreach that the SDT has done with the stakeholders, beyond the normal development process outreach. Our comments and balloting positions are intended to be constructive and help improve the revised standards, so they will ultimately be approved. FMPA sees three issues with CIP-003-6. First, requirement R2 has been modified to remove the "IAC" language (as it has been removed from all other places in the CIP standards as well). This unfortunately has reintroduced a zero-defect tolerance due to the wording in R2. Second, while the standard states an inventory isn't required for low impact assets, use of the word "All" in part 2.4.1 implies that an inventory must be done in order to prove compliance. Third, while not a direct responsibility of the SDT, the RSAWs do not provide any level of clarity as to how the Entity can expect to be audited. FMPA suggests that R2 be reworded to address each of these three issues. FMPA proposes the following language (in a table format) to address the first two issues for R2: "Each Responsible Entity shall develop and institute Policies and Procedures designed to meet the following indicators of performance: • The Responsible Entity has an established, formal program for identifying Low Impact Assets. • The Responsible Entity has a process to evaluate the addition or removal of Low Impact Assets that can affect BES operations. • The Responsible Entity has a program to address the company’s ability to detect and respond to compromise of the company’s Low Impact Assets • The Responsible Entity has a program to provide training and awareness to all relevant employees. • The Responsible Entity institutes internal controls and procedures to prevent a recurrence of identified deficiencies This approach is based on the FERC “Policy Statement on Enforcement” Docket PL06-1-000. Specifically, it is taken from the Internal Compliance guidance that FERC has provided and has been instituted by the ERO in evaluating Internal Compliance programs through 13 standard questions. This approach would give entities a substitute for the IAC language promised in Version 5, plus give FERC the assurance that entities will have programs in place that can be audited. The Measures can be devised in a similar fashion to the grading system used by the regions to assess ICPs; and as such, the VSLs can be designed such that the requirement is measurable and “gradable”. FMPA realizes that we are using the word "institute" in the above suggested language. We recognize that the SDT does not like to introduce new terms and/or language when possible, and FMPA supports that. The term "implement" was used in previous versions of the CIP standards. However “Implement” is not appropriate because it creates double jeopardy with the rest of the CIP standards, e.g., a violation of another standard could mean that the policy was not implemented. By using the word "Institute", it would suggest that the policy is in force and able to be enforced by the Responsible Entity, but not requiring ERO enforcement of the policies in this requirement (implement includes enforcement), but rather ERO enforcement is contained in ensuing standards. Use of the word “implement” also introduces the zero defect problem because it can be argued that any defect is a violation of implementing a policy. Hence, a word that means that the entity has adopted and enforces adherence to policies is more appropriate, such as “institute” or “establish”. FMPA suggests this approach for all requirements that formerly contained the “identify, assess and correct” language in Version 5. The removal of this IAC language introduces the zero defect issue. Yes, RAI is “promised”

as a solution to this problem; however, RAI is not “solid” enough for industry to depend on when supporting this standard and it is too important to depend on an unsubstantiated promise. In addition, FERC did not direct removal of the IAC language, but rather directed that the requirements be measurable and auditable. Our suggested alternative meets the FERC directive. If a complete re-write of R2 isn’t possible, FMPA has specific comments on some of the parts of R2. For part 2.4.1, using the word "All" in the requirement could be read to mean an entity has done a complete inventory of low impact assets in order to determine "all" of the communication paths suggested in part 2.4.1. FMPA suggests replacing the word “all” with “identified”, a la 2.4.2. Under part 2.5.1, FMPA does not agree with using the defined term "Cyber Security Incidents". We feel this could add to confusion, as the definition includes "Electronic Security Perimeter or Physical Security Perimeter". FMPA is aware there is an “or” qualifier on the definition that can be used to ignore the use of ESP/PSP terms that do not apply to Low Impact – perhaps having this information in the guidance part of the standard would clear up some confusion. FMPA also suggests limiting the scope of part 2.5 to Low Impact Control Centers and removing any reference that might include out-of-scope terms such as ESP's and PSP's. FMPA is also concerned at the lengthy wording of the VSL for CIP-003-6. With so many "or" statements, it may be difficult to follow. Since all the of the revisions for this balloting had the IAC language removed and there are limited RAI details available at this time, FMPA is voting negative on all of the CIP standards/VRF/VSLs posted for this balloting.
Yes
FMPA supports APPA’s comments on this question. APPA appreciates the SDT providing flexibility to entities in complying with R1 Part 1.10. Having multiple options for controls when physical access restrictions are not possible gives entities an opportunity to select the solution that works for their specific situation. Industry has commented that encryption of data as a sole solution may reduce reliability by adding complexity to the systems and latency to data flow that will not work in a relay control environment. If the SDT removes this flexibility or expands the applicability in future drafts APPA will need to reevaluate its support for the communications controls.
No
FMPA supports SMUD’s comments on this question. SMUD prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of “operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability)” as well as the corresponding Requirement Part 4.6 to “evaluate the Transient Cyber Asset.” SMUD believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a “defined acceptable use” for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. SMUD supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state “Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists.” As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source requirement part. SMUD is concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. SMUD does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. SMUD requests guidance be included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review.
Yes
No comments.
No
See comments under question 1 above.
Yes
No comments
No
No comments

No
In general the RSAWS need a significant amount of improvement. Given the removal of the IAC language in the standards, the RSAWS take on even more importance than before. The SDT could consider performing a non-binding ballot on the RSAWs as allowed for in the Rules of Procedure. At a minimum, the RSAW comments should be posted for transparency. A few specific comments on the RSAWs: • The RSAW for CIP-002 expands the standard greatly and we believe that an entity does have to list low impact assets in order to meet the RSAW requirements. • The RSAW for CIP-003 has a wrong number in 6a of R2.5 (bottom of page 19). It seems like the number 15 needs to be 36 calendar months in part “a” under the line item number 6 which has 36 in it. • We have some concerns with R2.5 items in the standard and at the bottom of page 19 of the RSAW. It adds in more criteria than what is written in the standard requirement (R2.5 and additional sub-requirements). We are unsure what R2.5.1 is asking for when it comes to “classification”. What if the auditor does not agree with our criteria for classification? What happens if we fail to identify a Cyber Security Incident (someone else identifies it)?
Individual
Nick Braden
Modesto Irrigation District
Individual
Chris Scanlon
Exelon Companies
No
In General: Exelon supports the SDT approach to add language to CIP-003, R2. Although we agree that the approach to add greater specificity to the required processes can fulfill the directive related to communication networks in Order 791, Exelon has concerns with the requirements as currently proposed. We are concerned that the revisions blur the distinction between low and medium impact and increase the burden for low impacts beyond the benefits to security and reliability. Exelon voted negative on CIP-003. Significant adjustments are needed for Exelon to support the revisions. Discussion of our concerns and some suggested revisions are offered below. Exelon notes that the low impact category is a comprehensive category bringing into scope all BES Assets that are not medium or high. This expansion of the CIP Standards is significant for the volume of newly covered assets brought into scope. Still, first and foremost, the emphasis, burden and investment of resources must focus on the assets most important to reliability and keep the burden of the requirements commensurate with the risk those assets pose to the Bulk Electric System. Exelon concurs with keeping all the requirements applicable to lows within one Standard (i.e. CIP-003). This Standard structure allows the requirements to include some unique features important to managing the low impact assets including: The specific language that no inventory is required The opportunity to set the compliance obligations at an appropriate level (i.e.; enterprise, site or program level instead of the device level) Exelon recognizes the value that one location for all low requirements may hold for entities with only low impact assets. As an entity with High, Medium and Low Impact assets, we would like the language to allow entities the option to fulfill certain requirements in CIP-003 R2 by incorporating Lows into their processes under associated standards applicable to Mediums. For instance, an entity should have the option to add Low Impact assets to their security awareness programs under CIP -004, R1.1 as a way to fulfill the CIP-003, R2.6 obligation. While not addressed in the proposed revisions, Exelon supports consideration of revision to the CIP-003 Applicability Section 4.2.2 to address dispersed power producing resources. It is important to clarify that security control requirements are set at the point of aggregation to 75 MVA and not at an individual turbine, generating unit or panel level for dispersed generation. The Project 2014-01 SDT is addressing similar concerns in other standards. Since the CIP V5 Revision SDT is currently revising CIP-003, it is a good opportunity to address this issue. Specific Concerns with proposed language: R2: While Exelon supports removal of the IAC language from CIP-003, R2 and the other requirements, our compliance concerns remain around the potential proliferation of compliance documentation, unreasonable compliance and enforcement burdens, and increased compliance risk. R2.1: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. R2.2: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”.

R2.3: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “Control Centers containing Low Impact BES Cyber Systems”. R2.3 Please offer more clarity on who is considered a “visitor” and the record keeping expectations/requirements for them. Discussion in the Guidelines will be helpful. R2.4: In general, R2.4 introduces significant complexity when applied to BES Assets with low impact BES Cyber Systems. This is concerning because even though FERC accepted in Order 791 (P.111) that creation and maintenance of an inventory of Low Impact assets for audit purposes would be unduly burdensome for Responsible Entities and could divert resources away from protection of High and Medium Impact assets, the currently proposed requirements make an inventory inevitable. We preferR2.4 to read similarly to R2.2 by stating: “Implement one or more documented processes that restrict logical access.” R2.4: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. R2.4.2: This subpart is problematic and an aspect that prevents Exelon from supporting the revisions. The administrative documentation burden associated with this subpart shifts the work of the control from protecting access points to documenting aspects of those access points. More problematic is the shift away from keeping the protections and compliance obligations commensurate with the risk posed by sites with low impact BES Cyber Systems. , These sites are low risk to the Bulk Electric System. The potential of the risk and the probability of the risk are low, and the protections in place at High and Medium Impact assets help diffuse the risks presented by the Low Impact assets on the system. The most valuable investment of time, resources, and personnel is in instituting protections at the High and Medium Impact assets and fulfilling the requirements associated with those BES Cyber Systems. R2.4.2 should be stricken. M2.4.2: Explain how the “representative sample” would be acceptable to demonstrate compliance. R2.5: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. Please also provide clear guidance stating that sites with low impact BES Cyber Systems may be covered by an enterprise-wide Cyber Security Incident response plan or other approach, and assurance that a Cyber Security Incident response plan is not required for each site. R2.6: The applicability should clarify that the requirement applies to sites containing Low Impact BES Cyber Systems. Consider revising: “BES Assets containing Low Impact BES Cyber Systems”. R2.6: The proposed requirement language is confusing and seems more restrictive than its counterpart in CIP-004-5, R1.1. Naming the subparts as topic areas adds a compliance demonstration not present for Medium and High. The language should be clarified so entities understand the subpart topics are to be covered within the quarterly program so each of the subpart topics is covered at least once within 15 calendar months. In addition, R2.6 should allow entities with awareness programs under CIP-004, R1.1 to fulfill this CIP-003 R2 obligation through the CIP-004 program. Please consider adding to the Requirement: “If not already covered by fulfillment of CIP-004, R1.1, implement …” Compliance concerns: While Exelon supports removal of the IAC language from CIP-003, R2 and the other requirements, compliance concerns remain around the potential proliferation of compliance documentation, unreasonable compliance and enforcement burdens and increased compliance risk. Enforcing these requirements in a zero-defect approach could prove overwhelming for Responsible Entities and for NERC/Regional Enforcement. Reasonableness in the NERC compliance approach is essential. In some cases, the compliance expectations are influencing the applicability of the requirement language and contradicting language of FERC Order 791. For instance, Order 791 supported the importance of not requiring an inventory; however, the currently proposed language and under the current zero-defect compliance approach, there is not an obvious way to demonstrate compliance to the requirements without having an inventory. This makes the statement in the requirement ineffectual. The Order 791 directive concerning lows (P108) cites “an unacceptable level of ambiguity and potential inconsistency to the compliance process and an unnecessary gap in reliability.” While interrelated, addressing reliability and compliance are separate challenges. Order 791 did not object to the four issue areas as those relevant to apply to low impact assets for reliability. The SDT is challenged to refine the expectations around those control aspects. Concurrently, NERC is challenged to clarify the compliance process. While not the work of the SDT, the Reliability Assurance Initiative (RAI) and the RSAWs are companion pieces to the CIP standard revisions. Unfortunately, the initial draft RSAWs didn’t provide much clarity or relief from the zero defect compliance expectation; however, additional work on the RSAWs can help. Exelon encourages the RSAW development team to continue their work and post revised RSAWs with next iteration of CIP revisions. Concurrently, RAI could use the requirements applicable to Low Impact assets to demonstrate how RAI can alleviate the

compliance concerns and create a reasonable approach to compliance. This may be essential for the passage of revised requirements on Low Impact assets.
Yes
Exelon supports the SDT approach to add requirements to CIP-006 and CIP-007 to apply requirements to non-programmable communication equipment. We agree that this approach fulfills the directive related to communication networks in Order 791. Setting the protection requirements to within an ESP are appropriate and consistent with the components controlled by Responsible Entities. Exelon supports the decision not to define communication networks as a glossary term. The term itself is not used within the revised standards, but the revised requirements address protection of the nonprogrammable communications components identified in Order 791. Use of the terminology is understood within the context of the applicable standards (CIP-006 and CIP-007). Keeping the definition within the CIP context avoids implicating any additional Reliability Standards beyond the scope of the CIP revisions. By not creating a glossary term, the SDT avoids confusing broader discussions of communication networks that may be underway. While supporting the decision not to define communication networks, Exelon asks the SDT to consider whether it is valuable to define “non-programmable communication components.” Exelon voted negative on CIP -006 and CIP-007 to encourage the SDT to make additional refinements; however, Exelon generally supports the revisions. Some requested clarifications and suggested revisions are offered below. CIP-006, R1.10 should further clarify the scope to be only for ESPs with External Routable Connectivity. The relevant concern is with the external connectivity and in bridging PSPs. For settings that have an ESP without External Routable Connectivity, no PSP is required and therefore no bridging of PSPs can occur. The language should be revised to avoid creating an administrative burden that does not provide value. Consider adding to the CIP-006, R1.10 applicability “Medium Impact BES Cyber Systems with External Routable Connectivity at Control Centers and …” OR Revise CIP-006, R1.10 to read: “For ESP’s with External Routable Connectivity, restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same ESP in those instances when …” Please confirm the understanding of the CIP-007, R1.2 applicability, “nonprogrammable communication components located inside both a PSP and an ESP” means the requirements apply to devices that reside within both and does not mean devices within a PSP and devices within an ESP. Discussion in the Guidelines could confirm if others seek confirmation of this intent.
No
Exelon supports the SDT approach to add requirements to CIP-010 and CIP-004 to apply requirements to transient devices and removable media. We agree that this approach fulfills the directive related to communication networks in Order 791; however, Exelon has concerns with the requirements as currently proposed. Exelon’s concern is that, as currently proposed, there is additional administrative burden without sufficient benefit. The requirements should focus on addressing the relevant uses that present a potential to introduce malware, with emphasis on authorization/protections on the device at the time of connection rather than over various protection versions and use of the device rather than the people using it. We are very concerned that the requirements will obligate Exelon to track every use of a transient device regardless of whether contamination occurs or not. This concern is triggered primarily with the “prior to use” language (e.g., R4.6 “Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4”) which indicates use here is every use, and thus must be tracked. The requirements on transient devices should not be more stringent than those on BES Cyber Assets. For example, R4.7 requires that TCAs be evaluated “within 35 days of use of the transient device to ensure patches are up to date” where the requirements for Medium and High BES Cyber Systems allow 35 days to evaluate and 35 days to patch. Exelon voted negative on CIP-010. Adjustments are needed for Exelon to support the revised CIP-010. Some requested clarifications and suggested revisions are offered below. CIP-010, R4.1-4.7: Applicability of the requirements should clearly apply to those Transient Cyber Assets and Removable Media (depending on sub-part) connecting to High and Medium BES Cyber Systems and their associated PCAs. Please consider revising the applicability column to read (depending on sub-part): Transient Cyber Assets/Removable Media connected to High and Medium BES Cyber Systems and their associated PCAs. CIP-010, R4.1 – Please clarify the expectations for authorization of users. Is this to be a list of individuals? If so, a list of names is an overly burdensome administrative task and a problematic compliance risk. The measures also do not seem consistent with the requirement language. The measure starts with the software or

configuration, while the requirement starts with users. The requirement logic should track with the measure by identifying the TCA first and then the authorization information. CIP-010, 4.1.4: Please clarify the expectations, if any, for tracking patch versions on a TCA and preapprovals required if 4.1.4 is updated per 4.6. “Defined acceptable use” in R4.1.3 is more relevant to security than the administrative nature of tracking patch versions. R4.1.4 should be stricken. CIP-010, R4.2 and R4.3 present a zero tolerance evidence challenge. Please discuss further the compliance evidence expectations. Exelon has no objection to being required to use methods to address malware on transient devices. Our concern comes in meeting the measures as written, which suggest evidence may be asked for each use of the process in each case. CIP-010, R4.4 – Clarification of the language is needed to distinguish between discovery of malicious code prior to connection and following connection of the device to a BES Cyber System. The relevant focus of the requirements should be on discovery of malicious code on connected devices and responsive mitigation. Consider revising R4.4: Mitigate the threat of malicious code detected during connection of Transient Cyber Assets and Removable Media. CIP-010, R4.5 is too rigid. Is the intent to require updating signatures prior to use? If so, consider modifying to read: Update signatures or patterns for those methods identified in Parts 4.2 and 4.3 that use signatures or patterns according to the Responsible Entity’s documented signature update process. CIP-010, R4.6 and R4.7 – While Exelon recognizes the added risk level associated with control centers, it’s not clear what circumstances these sub-parts seeks to capture in going beyond the intent of R4.1 and R4.2. Incorporating R4.6 into R4.1 and R4.7 into R4.2 may be warranted; however, this consideration should be given after thorough consideration of revisions to the proposed R4.1 and R4.2. Exelon understand that R4.6 seeks to apply an added authorization step for TCAs being connected to High Impact BES Cyber Systems and to Medium Impact BES Cyber Systems at Control Centers. Since this is associated with the authorization requirements in R4.1, it makes more logical sense to move this to R4.2. R4.7 seeks to allow latitude for Responsible Entities to make updates to TCAs according to a time schedule that may be dictated by other management practices other than a time just before use of the TCA. Exelon supports this flexibility. However, as currently written, the 35 days is more aggressive than for CIP-007, R2.2 and R2.3 that allow 35 days to evaluate and 35 days to install. Since both of these requirements apply to patching, the differences can limit the efficiency and effectiveness of an entity program that manages transient devices and BES Cyber Systems together. Please discuss the limitation of “per device capability” and any expectations for accommodating those without capability and/or any compliance expectations to demonstrate such capability. As presently proposed, Exelon finds the level of rigor placed on TCAs and RMs on par with that in CIP-007 applicable to permanent assets. The sentence in the rationale referencing the relative rigor should be removed.
Yes
No Commnet
Yes
Exelon supports removal of the IAC language from the 17 requirements and finds that this fulfills the Order 791 directive. Exelon continues to have questions regarding the RAI program and its fulfillment of the IAC intent.
No
The revisions to CIP-003, R2 are significant and as currently worded, represent a significant amount of work to implement the associated compliance program. The implementation plan should allow at least a year from the effective date of CIP-003-6. The Implementation Plan should make it clear that CIP-003-6, R2 will replace CIP-003-5 R2. The Implementation plan uses “months” and “calendar months”. Please clarify whether there is a difference between the two terms and, if no difference is intended, use one for consistency.
No Comment
Yes
Guidance: Exelon strongly encourages the SDT to write guidance to more fully explain the underlying intent of the requirement language. We recognize that guidance is not the same as the requirement language, but the information goes to the spirit of the requirement language and helps Responsible Entities establish their compliance programs to fulfill the requirements. Revision Development Timeframes: Exelon supports the SDT efforts to complete revisions in response to all four of the directive issue areas. In particular for the Low Impact asset requirements, completing the revisions will potentially enable Responsible Entities to implement the requirements with a clearer

understanding of the expectations and be able to do so once by skipping to implementation of V6. The Order 791-directed revisions are under development concurrent with industry work to implement the CIP Version 5 requirements, which is a daunting and resource intensive task. Iterative implementations are confusing and costly. RSAWs: (Restated from Q1) RSAWs are companion pieces to the CIP standard revisions. Unfortunately, the initial draft RSAWs didn't provide much clarity or relief from the zero defect compliance expectation; however, additional work on the RSAWs can help. Exelon strongly encourages the RSAW development team to continue their work and post revised RSAWs with next iteration of CIP revisions. RAI: Exelon supports the RAI concept and promise, but this is completely dependent on a greater understanding of and tangible experience with RAI. For Exelon and others, filling this gap may be essential for the passage of revised requirements, in particular for Low Impact assets. Regardless of the revisions, NERC has made commitments for RAI to be in effect in time for the CIP Version 5 implementation deadline. The revisions and RAI program components can work together. For instance, the IAC requirements may offer a useful vehicle to roll out to Responsible Entities the RAI aggregation concept to manage the requirements. As well, the Low Impact asset requirements are prime candidates to demonstrate how RAI can alleviate compliance concerns and create a reasonable approach to compliance for low risk requirement.
Individual
Rich Salgo
NV Energy
No
We generally agree with the approach that the SDT has taken, yet express the following concerns described below: Applicability The scope of dispersed generation in the applicability of this standard should be limited similar to that of PRC-005. We suggest the following be inserted within the section 4.2.2: "For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level." Requirement R2 The scope of R2 should be appropriately limited by restoring the reference to the assets identified in CIP-002-5.1 R1 Part 1.3. Suggest the following revision to R2: "Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Low Impact Assets. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required." Subpart 2.4.1 Clarification is needed that an external routable protocol past is "external" to the asset identified in CIP-002-5.1 R1, Part 1.3 containing low impact BES Cyber Systems. Suggest revising as follows: "All routable protocol paths to and from the asset identified in CIP-002-5.1 Requirement R1, Part 1.3 containing low impact BES Cyber Systems, if any, must be through one or more identified access point(s)." Subpart 2.4.2 As written, there is an implication that the use of a firewall is prescribed, as the term "by default" is used. Suggest revising Subpart 2.4.2 to read "For each identified access point, if any, require inbound and outbound access permissions, deny all other access, and document access permission reasons individually or by group." Part 2.6 As written in this draft, the specificity of what must be covered and the tracking of two time periods are more prescriptive than the requirements for Medium or High Impact BES Cyber Systems. Suggest the following language: "Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months."
No
General agreement; however, we request that clarification be added such that it is clear that entities are not expected to enforce CIP-006 requirements on third party non-programmable components that are not within the control of the entity.
No
We generally agree with the overall approach; however, we have specific concerns as described below. R4 part 4.1 We are concerned that Part 4.1 creates unnecessary administrative burden. For example, authorization generally applies to users. A user of a Transient Cyber Asset should be

authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also appears to overlap with CIP-004-6 R4 Part 4.1 which also addresses authorization.
No
The proposed definition for BES Cyber Asset, in conjunction with the Guidance of the Guidelines and Technical Basis create risk of misinterpretation. While a BES Cyber Asset is defined to “affect the reliable operation of the BES”, the Guidance dwells on the concept of BES Reliability Operating Services. If users interpret that to “affect” reliable operation is to be unable to perform a BES ROS, then certain devices whose loss could immediately preclude the BES ROS would have to be classified as BES Cyber Assets even though they likely do not affect the reliable operation of the BES. We suggest clarification in the Guidance that ensures perfect alignment with the definition. “Removable Media” definition lacks clarity that the portable media must be connected to “applicable systems”. Consider the proposed modification: “Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
No
While the SDT has removed the IAC language from these requirements in accordance with the directive, it nevertheless leaves the industry with an inevitable zero tolerance compliance enforcement paradigm, which is problematic, given that the new Reliability Assurance Initiative may not be in place. It is essential that compliance exception allowances be in place coincident with the removal of the IAC language from these 17 requirements.
Yes
There are references in the unmodified V5 Standards (CIP-002, 005, and 008) which continue to point to superseded versions of the modified Standards.
Group
Duke Energy
Michael Lowman
No
CIP-003: In Part 2.3 of the table, Duke Energy believes that it will be difficult for an entity to determine and monitor physical access points for Low impact BES Cyber assets. These access points may or may not exist for low impact BES Cyber Systems. We suggest the SDT consider requiring Low impact BES Cyber assets at Control Centers have a PSP in order to capture the intent of Part 2.3. In addition, we believe that requiring Low impact BES Cyber Assets to have the same control measures in place as Medium impact BES Cyber assets will become extremely burdensome for the industry and will provide little benefit to reliability. A distinction needs to be made between Medium and Low impact BES Cyber Assets. As an alternative, Duke proposes the following language for Part 2.4.2: "For each identified access point, if any, include the reason for granting access anywhere direct connectivity is allowed to or from the world-wide-web."
No
CIP-006: No comments CIP-007: We suggest the following revision to the Applicable Systems sections of Part 1.2 in Table R1-Ports and Systems: “High Impact BES Cyber Systems and their associated: 1. PCA; and 2. Nonprogrammable communication components used for the connection between applicable Cyber Assets within the same ESP and within a PSP. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components used for the connection between applicable Cyber Assets within the same ESP and within a PSP.” We believe this adds clarity on the expectations for nonprogrammable communication components.

No
CIP-010: (1)Duke energy suggests adding an additional bullet in the Applicable Systems section throughout CIP-010-2 Table R4 – Transient Cyber Asset & Removable Media Protection that states the following: • "A network within a PSP" We believe this is needed for consistency with the definition of Transient Cyber Asset. (2) We are unclear of the need to include 4.1.4 and 4.6 in Table R4. We fail to see the security and reliability benefit of this type of control method. As such, we suggest removing both 4.1.4 and 4.6 from the Requirements section of the CIP-010-2 R4 Table. CIP-004: No Comments
No
Duke Energy offers the following as an alternative suggestion for the definition of Removable Media: Removable Media: Portable media, directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact discs, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory. A Cyber Asset is not Removable Media. We believe the addition of "directly connected," as well as items 1-3 provides more clarity and complements effectively the definition proposed for Transient Cyber Assets.
Yes
No
We suggest making the effective date of the Medium and High impact CIP standards enforceable on the same date(January 1, 2017). Also, we suggest that the Low impact CIP requirements should be enforceable one year later(January 1, 2018). The staggering of effective/enforceable dates as proposed, is confusing to industry stakeholders, and increases the likelihood of avoidable compliance violations. Whereas a consistent, across the board effective date, provides the clarity and consistency on the expectations for implementing the CIP Version 5 standards and revisions.
No
Yes
As stated above, we believe the CIP Version 5 standards and revisions should be effective on the same date for Medium and High impact requirements and a year later for low impact requirements. Again, we feel that having consistent effective dates may prevent compliance violations that can easily be avoidable.
Group
Peak Reliability
Jared Shakespeare
Yes
Yes
Yes
Yes
Peak supports the Standards as revised. However, Peak believes NERC/Regional Enforcement policies should be altered to allow entities to have low-risk, occasional non-compliance of certain NERC Standards without having to expend administration efforts on submitting Self Reports. Concrete threshold reporting criteria for certain Requirements should be set.
Yes
No

Individual
Heather Rosentrater
Avista
Yes
Avista supports the removal of the “identify, asses, and correct” language due to the expectation that NERC will refine its compliance and enforcement process under the Reliability Assurance Initiative (RAI) to move away from a zero tolerance approach to compliance. We expect the new RAI to be finalized prior to final ballot to address the zero tolerance concerns that the “identify, assess, and correct” language intended to address.
Individual
Don Schmit
Nebraska Public Power District
No
While we agree that protecting access to cyber assets is a valuable and a needed direction to move, we don’t believe that the additional level requirements for “Low” assets aligns with the associated risk to the BES. If assets are “Low”, then providing basic physical security and some fundamental access controls meets and is in line with the risk that classified them as “Low”. While the drafting team has tried to show in the guidance what would be acceptable and what would not, in essence they have determined the “how” the requirement will be audited by showing only a firewall solution. There are other methods to control access to facilities. The intent as we read it of the FERC comment was to have BES assets removed from direct internet access. Better language might be drafted that has utilities address that challenge, rather than force access control with firewalls for ALL low assets. This is an enormous burden increase for utilities as there are thousands upon thousands of devices to be covered as low impact, all with minimal risk to the BES. The burden on utilities will be immense as these devices are not static, and must be maintained, patched, and replaced every few years.
No
The FERC order did not require the removal of the IAC language; it does allow us to modify the language. We should either work through a solution together or remove the standard requirements entirely that contain the IAC language. As an industry, we need to find a better tool for reliability than to rely on zero tolerance in standards. We are spending too much of our time on very minor issues and it is diverting our attention away from focusing on the basics of reliability. The CIP standards quickly replaced all other standards as being the most violated due to the zero tolerance language in the standards. We would not have voted for version 5 without the IAC language. We are voting no on this version because the IAC language is being removed. To simply give up and remove it, because we can’t find a better compliance approach is disheartening. Reliability Assurance is a step in the right direction; however it is an enforcement action and not a compliance action. Simply removing the IAC language and saying Reliability Assurance will take care of the minor issues is avoiding the compliance solution. Even with Reliability Assurance, any issue is still a violation. The RSAWs for the proposed CIP Standards identify, at least 89 times for requirements and sub-requirements, where the auditor should find a violation. Reliability Assurance may help simplify the process with enforcement, but it is still a compliance violation. IT IS STILL A VIOLATION!!! The IAC language was attempting to take low risk issues and allow an entity to identify them and fix them

without any enforcement actions. Compliance, to the areas where IAC language was inserted, was tricky in version three; so we added IAC to provide a compliance solution to the requirements where we were constantly chasing violations with no value to reliability. As an analogy from our daily vehicle driving experiences, imagine driving in a vehicle where the speed limit is 45 mph. You approach a speed limit sign of 55 mph. A police officer is standing 10 feet in front of the 55 mph sign, clocks you at 46 mph and hands you a ticket for exceeding the speed limit. You're busted – you did exceed the speed limit in a posted 45 mph zone, but what is the value of the speeding ticket? Now, add NERC compliance to the speeding example and we are expected to self report each time we slightly exceed the speed limit in the above example. The value to public safety isn't controlling the speed of a vehicle that is going one mile per hour above the limit ten feet in front of a speed limit sign, but to prevent someone from excessive speeds that endanger others. Our court system and law enforcement officers have understood this for many years. Why can't we, as an industry, introduce some common sense into our reliability standards and remove zero tolerance? We remember implementing Urgent Action Standard 1200 for cyber security. We implemented the Urgent Action Standard to provide us some time to develop a sound program for cyber security. Many years ago, the need for action in developing cyber security standards was so great that we put the Urgent Action Standard in place to provide protection while we developed the NERC standards. We have deleted most of the Urgent Action Standard documents, but we did find one from February 2004 (over ten years ago). We implemented version one of the CIP standards years later. We have now approved version five and all the previous versions had similar pressures. Version 4 of the CIP standards was replaced before it was even effective. Now, we are working on version six of the CIP standards and want it effective before version five will be enforceable. What are we doing? As an industry, we are trying to implement version five, while maintaining zero tolerance to version three, but we don't know what version six will require us to do, but it will have the same effective date of version five. Does anyone wonder why so many companies are struggling with the CIP standards? We don't need to speed this version of the CIP standards through the system just to have to fix it later, like we have done with all the previous versions. We need to take our time, take a step back and try to get it right this time. We are sensing a lot of frustration in our industry over cyber security standards. The recent expedited development of CIP-014 diverted all of our attention and efforts this year, leaving little time to develop changes to the other CIP standards. We haven't implemented version five of the CIP standards, but we are already changing them before we have any experience with version five. Our recommendation is to slow down and get it right and not just try to get it done.
No
If the language as written for CIP-003-6 Requirement R2 is passed and remains unchanged, then keeping the implementation date of April 1, 2017 is not reasonable and will be difficult if not impossible for utilities to meet. Implementing access control at substations where there is none currently (or it is not as restrictive as the standards ask for) has the potential to cause failures or outages if not implemented carefully. There are numerous assets and logistical locations that would need to be addressed. Secondly, for some locations, implementing these measures may require facility outages that must be planned and coordinated months in advance, particularly in shared facilities. Larger entities will be working in 2015 to implement the High & Medium requirements, and will not turn their attention to "Low" requirements until that work is nearly complete. The resources implementing those requirements are in many cases the same ones that will perform the "Low" work, and their attention cannot be split without the potential for error. Additionally, since these changes will not be approved by FERC until late 2014 at best, we believe the effective dates should be extended using a simple calculation. From the time Version 5 was approved, to the time the changes are approved by FERC, that time should be added to the implementation date. For example, if the changes are approved in November 2014, then we add 1 year to the implementation dates. We would also suggest to make the implementation dates the same for all standards, and not have different implementation dates. It is additional administrative burden for both the entity and the auditor to have to keep a detailed tracking sheet of when each requirement is "effective". Make them consistent and the same to remove the potential error trap created with the multiple effective dates.
Individual

David Thorne
Pepco Holdings Inc.
It would be useful for users of the standards if the requirements for low impact assets outlined in the table for R2 were appended to the appropriate tables in the other CIP standards instead of CIP-003.
Yes
Pepco Holdings Inc. supports Edison Electric Institute’s comments submitted for this project.
Individual
Bob Thomas
Illinois Municipal Electric Agency
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
ATC supports the current language, however, offers one suggestion for consideration. For consistency with the application of similar NERC Glossary terms used for higher applicable impact levels, ATC requests consideration of the addition of the word "interface" following the word "access point" where the term "access point" or "access point(s)" is used in Requirement R2 Part 2.4. in order to allow entities to identify with clarity where cyber ingress and egress controls are implemented for external routable protocol paths.
Yes
Yes
Yes
Yes
Yes
No
Group
PacifiCorp
Sandra Shaffer
No
Low Impact assets: PacifiCorp seeks to clarify that the external routable protocol path referenced in CIP-003-6 requirement R2.4.1 is ‘external’ “to the asset identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems” in the requirement. PacifiCorp also suggests that if the intent of requirement R2.4 is as suggested in the drawings provided in the Guidelines and Technical Basis, that additional language be placed in the requirement to align with the acceptable designs indicated in those drawings.
No

No
No
Transient Cyber Assets: PacifiCorp understands that the CIP-010-2 requirements are intended to apply to Transient Cyber Assets and Removable Media. Accordingly, to heighten clarity for the industry, PacifiCorp recommends that the Applicable Systems for CIP-010-2 requirements should be revised as follows: "Transient Cyber Assets directly connected (and/or as applicable by subpart) Removable Media connected to Medium (or High) Impact BES Cyber System…", similar to the precedent for PACS in CIP-006-5 R1.1. PacifiCorp also recommends that the standards drafting team modify the requirement of "authorize" in CIP-010-2 requirement R4.1 to "document" as authorization implies additional administrative burden not even necessary for all of the applicable systems themselves.
No
Identify, assess, correct: It is PacifiCorp's understanding that compliance exceptions and other Reliability Assurance Initiatives concurrently being developed by NERC are expected to adequately and appropriately address the industry's zero defect concerns in place of the "identify, assess and correct" language that was removed by the 2014-02 standards drafting team. PacifiCorp believes that responsible entities deserve some certainty from NERC of the near-final or final form of these compliance exceptions and the mechanics to avail themselves of these exceptions, from a compliance and enforcement perspective, before they have to vote on these revised standards such that the industry can feel confident their concerns are being addressed.
No
No
Yes
Communication networks: PacifiCorp appreciates the standard drafting team's revisions in relation to communication networks and does not have any suggestions for improvement of the draft language.
Individual
Karen Webb
City of Tallahassee
No
The City of Tallahassee (TAL) feels that Part 2.4 does not adequately illustrate the measures necessary to prove compliance to the part 2.4.2 requirement. The term 'representative sample' needs to be defined specifically. Does this imply a sample of rule sets from more than one access point? A sample of the rule set from a single access point? If more than one access point is identified, then would the entire rule set, or only a partial rule set from a single access point qualify as a representative sample? There can be no ambiguity when direct evidence is required as proof of compliance. Part 2.4.1 states that all external routable protocol paths, if any, must be through one or more identified access point(s). Evidence includes documentation of these paths through identified access points. If there is no requirement to discretely identify low impact BES Cyber Systems, then how can we be expected to provide evidence for this requirement when we are not required to identify the access point in the first place? External routable protocol paths imply the existence of an electronic security perimeter, a specific set of connected assets that form a basis for a defined network structure. There is no language in this requirement to identify an electronic perimeter, therefore no conceptual reason to identify an access point with routable protocol paths that may or may not be external to an undefined barrier. The language of this particular requirement and the measures required to prove compliance are extremely vague. Parts 2.1 – 2.3, and 2.5 are sufficient to address FERC Order No. 791 paragraphs 106-100, and clearly provide substantive objective criteria to sufficiently measure an entity's protection of low-to-no impact cyber assets. Requiring entities to identify assets (access points) where asset identification is clearly stated as unnecessary, and provide representative samples of configurations for these unidentified assets, assets that function as external access gateways to an undefined electronic security perimeter, could create an unnecessary quagmire of compliance effort. Under the section Guidelines and Technical Basis for part 2.4 it states that the Responsible Entity must have implemented processes that

include the external routable protocol and Dialup connectivity paths to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected. There is an assumption made here that at least one or more external routable protocol and/or Dialup connectivity paths exist and those access paths are being utilized to communicate directly with the asset from a remote location. This language should be rewritten to match the requirements in Part 2.4 – removing any unnecessary ambiguity with regard to direct communications pathways vs. other reasons for necessary connections via remote communications paths; e.g. “The Responsible Entity must have implemented processes that include the external routable protocol and Dialup connectivity paths, if any, to the BES asset such that the low impact BES Cyber Systems located at the BES asset are protected.” Furthermore, the following sentence should be rewritten to state, “In cases where external connectivity is used to gain access to any low impact BES Cyber System at a remote site, electronic access controls should address the risk of using external connectivity.” The final two sentences in this paragraph contain references to ambiguous concepts such as collection and aggregation, without stating specifically what kind of information might be collected and/or aggregated. TAL’s contention is that these two sentences add nothing to the explanation and should be removed entirely. They state that these access controls are required to protect the collection and/or aggregation of low impact BES Cyber Systems, or the collection and/or aggregation of data pertaining to them, or what specifically?
Yes
No
Part 4.3 is identical to Part 4.2. TAL suggests collapsing 4.3 into 4.2 to include ‘prior to use on applicable systems’. Both requirements are obviously meant to be done prior to use on applicable systems (intent of the standard in the first place), so there is no point in stating the same requirement twice. If the intent of this revision is meant to protect applicable systems, then the only requirement necessary is 4.3. If both requirements must stay, then remove the word ‘detect’ from 4.2 as detection is required prior to use as part of 4.3. It makes the most sense to collapse the two requirements into one and adjust the Measures language to include hardening policies and scanning techniques as part of the traditional antivirus … example.
Yes
No
TAL has no recommended alternative approach as the original IAC language in the standard identified with a need to change industry perception of the spirit and intent of Critical Infrastructure Protection Reliability Standards to concentrate effective proactive compliance efforts towards identifying and correcting deficiencies rather than being focused on the fact that violations for those deficiencies may exist and subsequently turning the workplace into a reactive, audit documentation mill. The many changes in Violation Severity Levels in the revised standard will effectively result in potential violations regardless of any effort (or lack of effort) on the part of the entity to mitigate those violations. Now, with the IAC language removed, entities are no longer provided a much-needed greater degree of flexibility in detecting and remediating low-risk violations. All and any interpretation of the standards has been placed into the hands of auditors, which contributed to endless anxiety on the part of the entities with prior CIP versions. FERC stated concern over the broad and ambiguous nature of the IAC language as sufficient reason to force NERC to improve upon how the (IAC) language was written. As a result, NERC decided to assume that the enforcement process for low-risk violations would be unworkable, and remove the language altogether. This effectively disenfranchises the entity throughout the compliance auditing process.
No
Given the nature of the removal of the IAC language which results in a measurable change in how compliance programs would function under the new standard, FERC should issue an order to extend the effective date at least another full 6 months for each standard/requirement for which a modification to the language was made.
No
No

Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No
The proposed CIP-003-6 has language that is sometimes inconsistent with the larger framework of the CIP Standards. MMWEC suggests moving the requirements for security controls for BES Cyber Assets associated with Low Impact assets to the appropriate CIP Standards (CIP-004, CIP-005, CIP-006, CIP-008) and revising the language to more closely align with requirements for Medium and High Impact BES Cyber Systems. Additional table entries for applicability to groups of Low Impact BES Cyber Assets should be created as needed. To assist Responsible Entities that only own BES Cyber Systems associated with Low Impact assets, NERC should publish a guidance document that identifies Standards and Requirements that apply to Low Impact BES Cyber Systems. Comments specific to CIP-003-6 2.4 - By avoiding the concepts of Electronic Security Perimeters and Electronic Access Points, requirement 2.4 becomes difficult to interpret and less effective at protecting BES Cyber Systems from unauthorized access. We suggest more closely aligning the requirements for electronic access control with CIP-005-5 requirements for Medium and High Impact assets and moving the requirements to Standard CIP-005. This may require additional requirements, such as the identification of ESPs and EAPs. This may require Responsible Entities to expend more compliance effort than is currently proposed in CIP-003-6 R2.4. The Implementation Plan for these requirements should phase in enforcement over five years in order to address the challenges faced by Responsible Entities with large numbers of geographically dispersed Low Impact assets. This approach has been used in other NERC Standards that affect a large number of assets. (Examples include MOD-025-2, PRC-024-1, PRC-019-1 and others.) The Implementation Plan should require an increasing percentage of Low Impact assets to be compliant each year. Most Responsible Entities know the network architecture and communications capability of BES Cyber Systems associated with Low Impact assets. However, it will take time and resources to sufficiently document and, in some cases, implement additional cyber security controls on those BES Cyber Systems in order to be fully compliant with more stringent CIP Standards. A phased in approach to implementation plan will steadily increase the security of BES Cyber Systems over time.
Yes
MMWEC supports the changes to CIP-006 and CIP-007. However, CIP-006-6 should also include requirements for BES Cyber Systems associated with Low Impact assets.
No
MMWEC supports the comments submitted by SMUD regarding CIP-010 and Transient Assets. Also, CIP-004 should include training and awareness requirements applicable to BES Cyber Systems associated with Low Impact assets.
No
The definition for Removable Media should not be restricted to "portable." Also, the examples are unnecessary. Suggest the definition should be as follows - "Data storage media, connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data." The definition for Transient Cyber Asset should not include examples. Suggest the definition should be as follows - Transient Cyber Asset - A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset.
Yes
No
The Implementation Plan for requirements for BES Cyber Systems associated with Low Impact assets should phase in enforcement over five years in order to address the challenges faced by Responsible Entities with large numbers of geographically dispersed Low Impact assets. Entities with smaller numbers and Control Centers should be 100% compliant sooner than five years. This approach has been used in other NERC Standards that affect a large number of assets. . (Examples include MOD-025-2, PRC-024-1, PRC-019-1 and others.) The Implementation Plan should require an increasing percentage of Low Impact assets to be compliant each year. Most Responsible Entities know the network architecture and communications capability of BES Cyber Systems at Low Impact assets. However, it will take time and resources to sufficiently document and, in some cases,

implement additional cyber security controls on those BES Cyber Systems in order to be fully compliant with more stringent CIP Standards. A phased in approach to implementation plan will steadily increase the security of BES Cyber Systems over time.
Yes
Standards CIP-005 and CIP-008 should be revised to include requirements applicable to BES Cyber Systems associated with Low Impact assets.
Group
Tampa Electric Co.
Beth Young
No
Tampa Electric Company (TEC) participated in the development of Edison Electric Institute’s (EEI’s) comments on the Project 2014-02 CIP Version 5 Revisions and supports the comments as submitted by EEI for CIP-003 R2. TEC also supports the philosophy to provide objective criteria for CIP-003, Requirement R2 and recognizes the need to distinguish terminology in use for R2 from official NERC Glossary of Terms used in the other CIP Standards. For CIP-003, Requirement R2 Part 2.5, TEC recommends a rewrite; it is confusing to use the defined term Cyber Security Incident and Reportable Cyber Security Incident given that the definition only applies to one of the two scenarios that might identify an incident. Proposed alternative language: Utilize one or more programs to address the Registered Entity’s ability to detect and respond to compromise of Low Impact BES Cyber Systems that may be discovered during the course of normal operations. If any deliberate or intentional disruption is discovered, the Entity should notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). At least once every 36 months, test the program used to detect and respond to compromises, conduct a lessons learned or after action discussion, and revise the program to address lessons learned or after action items. If CIP-003, Requirement R2 Part 2.5.6 remains as it stands, TEC recommends removal of the word paper to allow for other types of drills. For CIP-003, Requirement R2 Part 2.6, TEC recommends removing the language at least quarterly and changing the frequency to annual. We do not see that the risk related to the BES from personnel at locations with Low Impact BES Cyber Systems as deserving of the quarterly frequency.
No
For CIP-006, Requirement 1 Part 1.10, TEC considers that the second bullet monitoring the status of the communication link and issuing an alarm or alert is duplicative of the requirements that TEC follows in support of the reliable operation of the BES, specifically as required for COM-001-1.1 R1.1 (provide adequate and reliable telecommunications facilities including internally) and R2 (manage, alarm, test and/or actively monitor vital telecommunications facilities and equipment). TEC considers this requirement part of day to day operation of the Bulk Electric System and not prima facie evidence of a cyber security incident. Alternatively, TEC recommends changing the language of the bullet as follows: Where physical access restrictions to such cabling and components cannot be established, the Responsible Entity shall deploy and document alternative measures such as encrypting data that transits such cabling and components; or monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to appropriate personnel (such as those identified in the BES Cyber Security Incident response plan, Grid Operators within the Control Center, or other individuals charged with responding to the alarm or alert) within 15 minutes of detection.
No
Tampa Electric Company (TEC) participated in the development of Edison Electric Institute’s (EEI’s) comments on the Project 2014-02 CIP Version 5 Revisions and supports the comments as submitted by EEI related to CIP-010 R4 and CIP-004 R1, Part 2.1.9. In addition, TEC provides the following comments for consideration. TEC appreciates the efforts of the SDT to address the FERC Directives for transient devices drafted for CIP-010, Requirement R4. The language in Requirement 4.1 indicates that the authorization is taking place prior to the initial use which is a reasonable expectation. The Guidelines contain the following clarification : For purposes of this standard, "use" is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use. This language in the Guidelines implies that R4 would need to be applied when a device moves between PSPs. This would have the potential to negatively impact the reliable

operation of the BES. Field technicians may be working on issues in one substation and get called to another location to address trouble tickets. Since these substations are not connected to the corporate network (and definitely not connected to the Internet), it would slow the process down if the technician needed to report back to a central location to validate the Transient Device between PSPs. TEC recommends clarification of the Standard and Guidelines to allow for a Transient Device to be validated on a periodic basis instead of on a per use basis between PSP or ESPs. For CIP-010 R4, Parts 4.3, 4.4 and 4.5, TEC is concerned that not all devices will be able to provide the documentation suggested in the RSAW related to the date Removable Media was used and provide adequate documentation related to the method used to detect malicious code. If there is no External Routable Connectivity, TEC is concerned that this requirement would necessitate the introduction of External Routable Connectivity to remote locations to support kiosks or other scanning devices along with expensive system upgrades in order to scan, update, log/track when the removable media was used, comply with this Requirement. The SDT should add the “per device capability” to CIP-010-2 R4 Part 4.3 to address device limitations. Similarly, TEC is also concerned there may be issues with the updates to the signatures under CIP-010 R4 Part 4.5. Since the Removable Media may be infrequently connected to either the corporate network or within a NERC ESP, we will have challenges in updating and tracking the date of A/V signatures on these devices. TEC is also concerned that not all types of Removable Media (Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.) can provide the ability to detect malicious code. TEC recommends that the subpart be updated to include the per device capability language used in other standards; this is implied in the Guidelines where the language includes the following: Part 4.5 requires a process to update signatures or patterns, where applicable. TEC recommends clarification of the Guidelines to allow for Removable Media to be validated on a periodic basis instead of on a per use basis. CIP-010-2 R4.7: For an entity-managed device, the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use. TEC recommends the SDT include potential measures that would be appropriate to vendor Transient Cyber Assets and Removable Media.
Yes
Yes
While TEC is a strong supporter of the Identify, Assess, and Correct (IAC) deficiencies approach to NERC CIP compliance, we recognize the challenge of creating objective measures for the implementation of such a program. Therefore, we agree with the SDT direction to remove the IAC language as proposed. Our understanding is that the approach under consideration is the Reliability Assurance Initiative. There is a need for transparency and open dialog between NERC and Registered Entities related to implementation of the RAI. We expect the RAI to be finalized prior to final ballot to address the current zero tolerance compliance approach that the identify, assess, and correct language intended to address. TEC also recommends that the SDT consider a potential approach to address the removal of the IAC language via the Violation Severity Levels for a future revision, possibly adding thresholds to different levels.
Yes
Not applicable to TEC
Yes
TEC greatly appreciates the work of the Standards Drafting Team and the NERC staff. We support the efforts to have a consolidated revision to cover both the date sensitive and other FERC directives in a single filing. In addition, TEC respectfully requests the SDT consider the adoption of conforming changes in CIP-002, CIP-005, and CIP-008 to address the effective dates and version numbers in the background section to provide consistency.
Individual
Cheryl Moseley
Electric Reliability Council of Texas, Inc.
Yes
None.

Yes
Regarding CIP-006-6 requirement part 1.10, ERCOT requests a CIPC guideline on acceptable encryption protocols, methods, and key management. This could help auditors better understand acceptable practices and reduce the opportunity for individual interpretations by the CEAs. The language, “an equally effective logical protection” can be considered too vague and open to interpretation. Request that the language be modified as, “a compensating measure that provides an equally effective level of logical protection as the items listed above”.
Yes
None.
No
There appears to be a gap in the requirement language regarding media that is connected longer than 30 days (i.e.: permanent asset). Since it is not programmable, it would not qualify as a Cyber Asset and subsequently not become a BES Cyber Asset or BES Cyber System. There are situations where these types of devices are needed permanently, (e.g.: software licensing dongles, flash/USB drives storing bootable image files for appliances, etc.). Request that the 30 day duration be removed from the definition and require CIP-010-2 Parts 4.2 and 4.3 for all removable media. If the definition of Removable Media continues to be limited to 30 days, request a modification of the definition to address what the media is plugged into, similar to Transient Cyber Asset. Recommended definition: “Portable media, connected for 30 consecutive calendar days or less to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset, in order to copy, move and/or access data.” Also, recommend the definition be modified to as: “Removable Media is not a Cyber Asset.”
Yes
None.
Yes
None.
None.
None.
Group
Western Area Power Administration
Lloyd A. Linke
No
The “external routable protocol paths” language in Requirement 2.4 requires entities Low Impact Cyber Systems to provide and comply with “some form of electronic security perimeter,” regardless of risk to the Bulk Power System/Bulk Electric System. Compliance to this requirement would be excessive given the risk associated with Low Impact rated BES Cyber Systems. The language in the CIP Requirements is confusing. On one hand, entities would be required to identify, maintain and comply with “some form of electronic security perimeter” (ESP) for Low Impact rated BES Cyber Systems, on the other, CIP Version 5 (or the proposed Revisions) states that “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” This is contradictive at best and should be clarified. Recommend language changes to address only Low Impact Systems which have direct internet access. Recommend adding language which assesses risk to Low Impact BES Cyber Systems with “external routable protocol paths.”
Yes
No
No
It would make more sense if the implementation were after the CIP Version 5 Standard implementation dates.
Yes

Yes
Recommend that the CIP Standards be aligned with Risk to the BES and that the object of the Standards be clarified. In many cases the SDT refrains from clear language so as not to dictate a particular approach. This leaves the interpretation up to Entities and Auditors who don't share the same perspective. We recognize and appreciate that SDT doesn't want to dictate activities. If the risks being mitigated are clearly understood that could provide the necessary clarity without eliminating varied approaches including technological advances.
Individual
Thomas Foltz
American Electric Power
No
The current wording of CIP-003-6 R2 Part 2.4 should be revised to align more closely with the definition of External Routable Connectivity. Suggested wording: “2.4.1 All bi-directional external routable protocol paths must be through one or more identified access point(s).” If the suggested wording is accepted by the drafting team then the Guidelines and Technical Basis should be revised as well to include the bi-directional clarification. The measure for item 2.4.2 should be revised to remove data diodes. A data diode is not an access point to a low impact BES Cyber System if it is configured in a manner that only transmits information outside the BES Cyber System. There are no inbound access permissions that can be applied since the device is hardware limited. Documenting how outbound traffic is sent provides no security benefit to the BES and would be an unnecessary administrative burden. The current wording of Part 2.6 could be read as a quarterly requirement for the reinforcement of cyber security practices and the 15 calendar month enforcement of Parts 2.2, 2.3, 2.4, and 2.5 above. This wording is more prescriptive than the wording for high and medium impact BES Cyber Systems. The wording should be revised to better align with the CIP-004-5 R1 Part 1.1 wording. This would give the entity the flexibility to determine what items need to be included in its security awareness program based on the current threat environment or detected lapses in cyber security practices. Suggested wording for the 2.6 Requirement – “Implement a security awareness program(s) that reinforces cyber security practices at least once each calendar quarter.” In addition, the wording is confusing in 2.3 – 2.4. If the site has a defined physical boundary (DPB) are the devices outside of the DPB in scope if they are low? Is it possible to define a DPB inside of a building as a site versus the whole site?
No
CIP-007 R1 overlaps with CIP-010 R4. We suggest removing the language from CIP-007 R1.
No
Requirement R4 represents a significant administrative burden. The fact that Transient Cyber Assets and Removable Media are not connected for extended periods of time to a BES Cyber System makes the automated logging and tracking of these devices impractical. To make this a more manageable requirement with less administrative burden Requirement Part 4.1 should be removed or modified to apply to medium impact BES Cyber Systems with External Routable Connectivity. This would align the requirement part with CIP-004-5 regarding the authorization of user access. User authorization is only required for high impact and medium impact with External Routable Connectivity BES Cyber Systems. The authorizing and tracking of Transient Cyber Assets will add a significant documentation burden with minimal increase to cyber security. The most significant threat Transient Cyber Assets pose to BES Cyber Systems is the potential to be a gateway to introduce malicious code. Requirements Parts 4.2, 4.3, and 4.4 should be sufficient to address these concerns on high and medium impact BES Cyber Systems without adding a significant administrative burden. Requirement Part 4.4 appears redundant to CIP-007-5 Requirement 3 Part 3.2. The current wording reads as if the threat of detected malicious code on high or medium impact BES Cyber Systems be mitigated. Suggested wording: “Mitigate the threat of detected malicious code on Transient Cyber Assets and Removable Media associated with or that could be connected to applicable systems.” This will make it clear that the mitigation actions in regards to Part 4.4 need to be conducted on the Transient Cyber Asset and Removable Media. Requirement Part 4.7 suggested wording: “Evaluate Transient Cyber Assets prior to use for security patches related to Part 4.1.4. For security patches that are not up to date take one of the following actions:…..” In addition, AEP would recommend highlighting or separating out the unique differences between these requirements and the ones

earlier in the CIP-010 standard. Also, do the devices have to be dedicated to the ESP and not used on other networks?
Yes
It is unclear why TCAs are being associated with Removable Media in the standard.
Yes
Yes
As long as the timeframe for implementing Low impact systems is not shortened, and the guidance is released with significant time to bring the Low impact systems into compliance.
No
No
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Group
Large Public Power Council (LPPC)
Joe Tarantino
No
The addition of more objective criteria for Low impact BES Cyber System Requirements within CIP-003-6, R2, breaks one of the prime objectives defined when CIP version 5 was being developed that each of the Standards could stand on its own. For entities with Low “and” either Medium or High Cyber BES Cyber Systems, it would be necessary that CIP-003 “always” be referenced when any of the requirements in CIP-004-6 through CIP-011-2 when the Medium and High impact BES Cyber Systems are being designed and implemented, since dependencies are always possible between BES Cyber Systems and the parts of any impact category. It is customary in other control objective families to present controls together, but identify whether there are different impact levels. The CIP standards have implemented this approach using the Applicable Systems table. SMUD appreciates the concerns from smaller Low impact only asset owners that there is far more requirements for Medium and High impact assets than there is for Low impact. Without sacrificing the integrity of maintaining the control objectives together and facilitating a directed set of controls to the Low impact owners, SMUD would recommend to NERC to develop specific targeted outreach documents for these entities that present just the Low impact asset control objectives in a more simplified manner. For example, at SMUD we have different groups that manage certain types of devices such as Electronic Access Control and Monitoring Systems (EACMS). We have created a presentation of a subset of Requirements and Requirement parts that just cover the EACMS so that those subject matter experts have a document for just those items that affect the applicable systems they manage. Additionally, to support this approach from an audit perspective, specific RSAWs could be created for the Low impact requirements that reduce the number of RSAWs that need to be completed by the entities. The inclusion of these objective requirements with a unique table in CIP-003-6 result in Standards language inconsistencies that creates confusion and additional compliance risks. A new definition is now needed for CIP-003-6, R2, Requirement Part 2.4 for the phrase “external routable protocol paths” to ensure that entities and auditors clearly understand the differences between that phrase and the defined term External Routable Connectivity. This would avoid duplicating the confusion seen in earlier versions of the CIP Standards, such as the CIP-002 confusion between Facilities and facilities. The phrase “external routable protocol paths” may create a similar interpretation risk. SMUD recommends that the language added to CIP-003-6, table R2 for Low impact assets be moved to the specific tables in each of the Standards CIP-004-6 through CIP-011-2 where applicable. Specifically, SMUD recommends the following: 1. CIP-003, R2, be modified to return the policy language to: “Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part 1.3, shall implement one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months. 2.1 Cyber Security Awareness; 2.2 Physical

Security Controls; 2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and 2.4 Incident Response to a Cyber Security Incident." This allows the entity to develop specific policies that are relevant to these areas; which is consistent with the intent of the CIP-003 standard. The objective criteria is then moved into the relevant CIP standards. SMUD believes that there needs to be guidance included for entities that also have Medium and/or High impact facilities that acknowledges a separate set of specific policies just for Low Impact is not necessary. Entities are permitted to leverage the policies for Medium Impact and/or High Impact and add the Low Impact applicable requirements. 2. CIP-003, R2, Part 2.1 would be removed and rolled into the Requirement 2 language. 3. CIP-003, R2, Part 2.2 would have Low Impact BES Cyber Systems added to CIP-006, R1, Part 1.1 Applicable Systems table. 4. CIP-003, R2, Part 2.3 would be added to the CIP-006, R2 Visitor Control Program table with a new Part applicable to Low Impact BES Cyber Systems. 5. CIP-003, R2, Part 2.4 would be added to CIP-005 as a new Requirement 3 with each of the current 2.4.1 – 2.4.3 as new Requirement Parts. 6. CIP-003, R2, Part 2.5 would have Low Impact BES Cyber Systems added to the CIP-008 standard maintaining the 2.5.6, 36 calendar month timeframe specific to Low Impact BES Cyber Systems. Additionally, for the existing CIP-008, R3, Requirement Part 3.1 extending the 90 date update cycle for Medium and High Impact BES Cyber Systems to 180 days for Low Impact BES Cyber Systems. For incident response, the SDT presented all but three of the CIP-008 Requirement Parts: 2.2 – Use the Cyber Security Incident response plans(s); 2.3 – Retain records related to Reportable Cyber Security Incidents; 3.1 – set an update frequency to the Plan. SMUD believes that requiring these three other Parts do not impose a significant burden for entities with Low Impact BES Cyber Systems. SMUD believes extending the update cycle for Part 3.1 to 180 days for Low Impact BES Cyber Systems is an appropriate timeframe based on the risk to the BES. 7. CIP-003, R2, Part 2.6 would be added the CIP-004, R1 Security Awareness Program table with a new Requirement Part 1.2 applicable to Low Impact BES Cyber Systems. The language would be updated to read: "Security awareness that, at least once each quarter, reinforces cyber security practices (which may include associated physical security practices)." The proposed language from CIP-003, R2, Part 2.6 created a higher performance requirement than for Medium and High Impact BES Cyber Systems by requiring the specific Low Impact BES Cyber Systems items to be specifically covered each year. 8. With the addition of the CIP-003, R2, Part 2.4 requiring an "access point" for Low Impact BES Cyber System, the exemption for Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters" in the Introduction section, number 4.2.3, Exemptions needs to be updated to include Low Impact BES Cyber Systems since Low Impact BES Cyber Systems do not require an Electronic Security Perimeter, but it still needs to be clear that the stated exemption is still in place for the Low Impact BES Cyber Systems.

Yes

No

SMUD prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of "operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability) as well as the corresponding Requirement Part 4.6 to "evaluate the Transient Cyber Asset." SMUD believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a "defined acceptable use" for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. SMUD supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state "Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists." As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source Requirement Part. SMUD is concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. SMUD does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. SMUD requests guidance be

included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review. One approach to removing use is that for those entities that only use their transient devices a few times a year, they can assess for patches “once every 35 days,” but prepare a mitigation plan that they will install the patch at the next use and assign a date for the mitigation plan. This does not impose the tracking of use related to transient devices and accommodates both approaches for those entities that have included their transient devices within their normal security patch processes and those entities that only use their transient devices on an irregular schedule.
No
SMUD supports the need for definitions associated with Removable Media and Transient Cyber Assets. In reviewing the proposed definition for Removable Media, SMUD believes additional clarity is needed to ensure the definition encompasses the appropriate components. SMUD requests removing the word “portable” from the beginning of the definition and adding “capable of removal without powering down the system” to the beginning of the definition. This removes a need to create a further definition of “portable” and ensures the equipment such as hot-swappable hard-drives are also included. The full requested text of the definition is below. “Removable Media: [delete:"Portable"] Media [add:"capable of removal without powering down the system,"] connected for 30 consecutive calendar days or less, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. A Cyber Asset is not Removable Media.”
Yes
SMUD supports the SDT removal of the IAC and fully supports the efforts of NERC to develop the Reliability Assurance Initiative (RAI) program. SMUD supports the shift from a zero-defect enforcement approach to a risk based method and providing alternative paths of enforcement.
Yes
No
No
Group
DTE Electric
Kathleen Black
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
There is concern regarding the faxct that the physical security requ9rements for lown mpace cyber sysrtems were put into CIP003 rather than CIP006. As we have seen repeatedly in the past, breaking up similarlysituated provisions into different CIP standards creates an interpretative and

administrative burden. It would be recommended that all physical security requirements should be in CIP006 to eliminate any confusion.
Individual
Karin Schweitzer
Texas Reliability Entity
No
All of the criteria in Table R2 are procedural with no performance requirement regarding the inventory of low-impact BES cyber systems. Texas RE recommends that specific performance requirements be added.
No
CIP-006, Requirement R1 Part 1.10--the requirement contains language that is not clear and therefore does not pass the test for NERC's "Acceptance Criteria of a Reliability Standard," item 8. The requirement of "an equally effective logical protection" is ambiguous and does not lend itself to a consistent interpretation of the required performance. If a responsible entity chooses to implement what it considers to be "an equally effective logical protection" (since it is only required to implement one item listed in Part 1.10), it is possible that a reliability benefit will not be achieved.
No
CIP-010, Requirement R4--it is unclear if the word "policies" in the Measures section of Requirement 4.2 is intended to mean application policies or a written policy that requires someone to take a certain action. Texas RE recommends that the SDT clarify the use and intent of this term.
Yes
Yes
Yes
Yes
Entities should be required to demonstrate evidence of the effective execution of controls and not just that they have a policy or procedure.
Individual
Heather Bowden
EDP Renewables North America LLC
Yes
Yes
Yes
Yes
Yes
Yes
No
Group
SRC

Greg Campoli
Yes
The SRC & SWG agrees in general with the requirement approach. Additional considerations below: CIP-003 R2 • p. 8, Since the phrase “external routable protocol path” has significance in the applicability of this standard and has a peculiar meaning, it should be added to the NERC glossary. • p. 8, “The Standard Drafting Team (SDT) intent in using the phrase ‘external routable protocol paths’ is to focus only on the paths to the low impact BES Cyber Systems and not the paths to other networks (e.g., corporate paths).” Does this imply that the phrase does not account for paths from the low impact BES Cyber Systems? • p. 8, “for its assets containing low impact BES Cyber Systems”. What does “containing” mean in this context? The asset is a BES Cyber System or is not. It does not “contain” a BES Cyber System. Suggest changing it to “for its assets that constitute BES Cyber Systems.” There should also be a comma following “[e]ach Responsible Entity” and “BES Cyber Systems” in the first sentence. • R2 Note on page 9 – If a list of low impact BES Cyber Systems is not required, how can this requirement be audited? This statement worked for a policy, but not for the new sub requirements, which must be “performed.” • Table R2 contains a scaled-down cross-reference to other requirements. This should be accomplished by adding “Low Impact BES Cyber Systems” in the Applicable Systems column of applicable requirements rather than setting apart a separate set of requirements for low impact BES Cyber Systems. • R2.5 – Will this require a separate plan or can it be addressed in the CIP-008 plan? Please explain in rationale or guidance.
Yes
The SRC & SWG agrees with the requirement approach. Additional considerations below: CIP-006 R1.10 • Use of encryption should be restricted to approved protocols and methods. Should there be requirements around key management? How will this be audited? • It is not clear in the Requirement text whether an entity can simply choose not to implement physical access restrictions or if it must demonstrate that it cannot for some reason. Although the text leaves open the possibility that physical, as opposed to logical, protections are optional, the phrasing can also be read to imply that restricting physical access is a preferred or default measure. Although the accompanying guidelines state explicitly that entities may implement physical or logical measures, the requirement itself is not as explicit • It is not clear how Regional Entities will assess whether a logical protection is “equally effective.” Will the REs defer to an entity’s judgment, or will there be a process by which entities can receive assurance that a logical protection is sufficiently robust to be “equally effective”? If entities must wait until their next audit to find out whether a measure is equally effective, they may simply ignore this option despite being permitted to develop such measures. More guidance should be provided on what is acceptable (pp. 36-37)
Yes
The SRC & SWG generally agrees with the requirement approach. Additional considerations below: CIP-010 • R4.1 Authorization should include purpose for connecting the TCA, start date/time, duration, and which ESPs the TCA is authorized to connect to. Also, the “caution” on p. 42 should be woven into the requirements that TCAs must be configured not to allow network bridging via wireless or blue tooth. It should be a required configuration check prior to connection. • In Requirement 4, Part 4.1.4, the term “intentionally installed software” is vague. For instance, the accompanying guidance suggests that “notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software” are not intended to be listed in the authorization of a Transient Cyber Asset. However, such an exception is not evident from the requirement language itself. Instead, the term “intentionally installed software” could be reasonably interpreted as covering all software on a Cyber Asset other than malware or other malicious programs. We recommend that the phrase be revised to provide greater specificity with regard to the types of software that should be included in the authorization. • R4.3 Why is there no “deter” or “prevent” for Removable Media? These are required for TCAs. • Malware should be grouped together in CIP-007, not split up in different standards. • In Requirement R4.4, the phrase “mitigate the threat” is ambiguous. For instance, it is unclear what constitutes mitigation after malicious code is detected or what the timeline for such mitigation is. (On the latter point, the current language does not even require that such mitigation be completed prior to use.) We recommend that a specific outcome for such mitigation be clearly expressed as well as language indicating the required timing of such mitigation. • R4.6 – This remediation or updating should be done prior to use as well. Should be more explicit. Could be a loophole. • In

Requirement R4.7, it is unclear whether a single evaluation within 35 days prior to use would be sufficient to comply with the requirement or if the requirement's emphasis is on "ensur[ing] security patches are up-to-date." In addition, it is not clear if a monthly evaluation would be sufficient regardless of how often the Transient Cyber Asset is used, e.g. if an evaluation must be performed prior to each use or if a single evaluation covers all use occurring within 35 days afterward. The accompanying guidance suggests that "rolling" evaluations are acceptable, but the requirement language itself is vague on this point. It may be advisable for the SDT to delete Requirement 4.7 and instead add Transient Cyber Assets to the Applicable Systems for the existing patch management requirement.
Yes
The SRC & SWG agrees in general with the revised definitions. Additional considerations below: • May want to include tape as an example of Removable Media. • Removable Media: need to clarify with respect to what it's connected to, as seen in the definition for Transient Cyber Asset. • BES Cyber Asset and Protected Cyber Asset include clarification on definition of Transient Cyber Asset. These statements should be moved to the definition of Transient Cyber Asset and not woven into other definitions. • Removable Media: Given that Removable Media are not Cyber Assets, if one is connected for more than 31 consecutive days, what happens? Is it somehow subject to certain requirements? • Removable Media: "A Cyber Asset is not Removable Media" – Is this trying to say that Removable Media is not a cyber asset? Need more clarity on this. • What happens if a TCA is connected for more than 30 consecutive days? Is it still a TCA, a BES Cyber Systems, or an undefined asset that is not subject to requirements? • The definition of Removable Media should at least be revised to state that "Removable Media are not Cyber Assets."
Yes
Comments: SRC & SWG agrees with the requirement The approach. Additional considerations below: • When will we see a specific description of the RAI program as applied to CIPv5 standard compliance enforcement and expectations of RE's for collecting evidence to support the RAI process?
Yes
The SRC & SWG agrees with the requirement approach. No additional comments.
Yes
The Canadian SRC & SWG members are not aware of any other provincial or regulatory requirements that need to be considered at this time.
Yes
• The present redline changes to standards look fine as far as addressing FERC's directives for changes to the CIPv5 standards. The SDT is to be commended for bringing these changes to a reasonable state for review and ballot in such a short period given the subjects involved. • There is concern that that the different versioning of the standards may cause confusion. It would be clearer for all to be promoted to the same base version 6.
Individual
Dale Dunckel
Public Utility District No. 1 of Okanogan County
Group
Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Pamela Hunter
No
Southern Company agrees, in part, with the approach for meeting the FERC directive addressing more objective criteria around protections for low impact BES Cyber Systems. Southern fully supports the continued use of the language eliminating the overwhelming burden of creating and maintaining lists of low impact BES Cyber Systems or Assets and lists of authorized users with access to low impact BES Cyber Systems. In addition, Southern fully supports the revisions under CIP-003-6 R2.3 being specifically applicable to Control Centers containing low impact BES Cyber Systems, and the incident response plan testing timeframes (once each 36 calendar months) under CIP-003-6 R2.5. However, Southern will be submitting a "No" vote on the revisions to CIP-003-6 R2 for the following reasons: 1) In the change to the tabular format, the requirements now imply that

they are at the individual low impact BES Cyber System level, rather than at the “Assets containing Low Impact BES Cyber Systems” level. The Applicable Systems column should be amended to state “Assets containing Low Impact BES Cyber Systems.” 2) Under CIP-003-6 R2.1, consider allowing approval of the cyber security policy or policies addressing CIP-003-6 R2 by the CIP Senior Manager “or delegate.” 3) Consider limiting the scope of CIP-003-6 R2.5 to “Control Centers containing Low Impact BES Cyber Systems.” 4) CIP-003-6 R2.5.6 – consider removing the word “paper” in front of “paper drill” to allow for various types of drills to be performed for incident response exercises. 5) Consider the following revisions to CIP-003-6 R2.6: “Implement a security awareness program that reinforces cyber security practices at least once each 15 calendar months” and remove the requirement to reinforce the previous requirement Parts. 6) Consider providing additional clarity in the Guidelines and Technical Basis section on what constitutes “external” in the context of the term “external routable protocol paths.” Is this strictly external to each asset containing low impact BES Cyber Systems (i.e., is every Cyber Asset at the asset considered “internal”)? 7) Consider providing additional information in the Guidelines and Technical Basis section on the use of the term “Cyber Security Incident” as it applies to low impact BES Cyber Systems. Although the defined term uses an “or” statement that would keep the scope of the definition applicable to low impact BES Cyber System, this should be explicitly noted. Southern Company also supports the following GTC comments to this question: GTC is concerned that by borrowing language from Medium Impact requirements, the SDT has introduced a substantial increase in administrative overhead to comply with the standard without an equivalent increase in security. Specifically, maintaining the documentation overhead of justifications for every firewall rule results in a significant amount of man-hours devoted to compliance and not to improving the security of the low impact BES Cyber Assets.
Yes
Southern Company agrees with the approach with meeting the directive in FERC Order No. 791 addressing protections for non-programmable components of communications networks.
No
Southern Company does not agree with the approach taken to address transient devices (Transient Cyber Assets and Removable Media). The new CIP-010-2 R4 requirements place an unachievable amount of responsibility and overwhelming administrative burden on Responsible Entities, specifically with regard to the handling and measures required for cyber assets that are not owned or maintained by the Responsible Entity, but for which there is significant dependence in order to ensure reliable operation of the Bulk Electric System. These new Standards, as well as the Guidelines and Technical Basis addressing these new Standards, strive more towards the prohibition of the use of TCAs and Removable Media, rather than providing achievable security Standards that a Responsible Entity could successfully implement. Southern Company provides the following comments to the SDT for consideration: 1) The Measures of CIP-010-2 R4.1 only address requirement R4.1.4 applicable to authorized baselines of TCAs and do not address examples of evidence for authorization of Users, Locations, or acceptable use, nor examples of how a Responsible Entity can demonstrate “prior to initial use.” 2) CIP-010-2 R4.1.2 – Southern recommends that acceptable use should not be required to be “authorized” for each initial use of a TCA, but should be separated to allow for addressing acceptable use at the policy/procedure level. See the below comments for additional recommendation/revision. 3) Under CIP-010-2 R4.6, where the requirement calls CIP-010-2 R4.1.4, the Applicable Systems are different between the two requirements. The Applicable Systems under CIP-010-2 R4.1 should either be changed from Mediums to Medium Impact BES Cyber Systems at Control Centers and their associated PCAs to match R4.6, or CIP-010-2 R4.6 should be re-written to include moving R4.1.4 into R4.6. Consider the following: CIP-010-2 R4.1: Define acceptable use of Transient Cyber Assets, and the process to authorize usage of Transient Cyber Assets, except for CIP Exceptional Circumstances. Authorization shall include: R4.1.1 - Users, individually or by group/role; R4.1.2 – Locations, individually or by group/role. CIP-010-2 R4.6: Evaluate TCAs, prior to use, and document the authorized baseline configuration of the TCA. Evaluation shall include authorization of: R4.6.1 – OS, Firmware, and intentionally installed software on TCAs (per Cyber Asset capability); R4.6.2 - For a modification that deviates from the state in Part 4.6.1, either: Remediate by returning the TCA to the state in Part 4.6.1; or Update Part 4.6.1. If the above suggested language is considered and/or included, the comments on changing the Applicable Systems under R4.1 may be ignored – no change to the Applicable Systems in R4.1 or R4.6 would be necessary given these revisions to R4.6. 4) Requirement R4.1 places a lot of

overhead on the Responsible Entity to simply maintain lists, rather than contribute significantly to security or reliability. Southern Company requests consideration that requirement R4.1 and R4.6 be applicable to just High Impact BES Cyber Systems and their associated PCAs. 5) The requirement to authorize and inventory all software on a TCA places an undue burden on those instances where a vendor needs to use their devices with their proprietary or licensed software in order to maintain or upgrade a BES Cyber System to maintain reliability. We suggest the SDT give thought to how a Responsible Entity can "authorize" proprietary hardware/software on a vendor TCA when the RE has very limited control over that device and limited or no understanding of the proprietary software contained therein. How can a Responsible Entity reasonably be expected to prove "initial use?" Does it serve a greater reliability purpose to tell vendors they cannot use their proprietary hardware or software to maintain BES assets? Or that they must buy another license of any licensed software so it can be installed on the Responsible Entity's TCA device? While we understand this is an area of increased risk, we suggest that checking patch levels and updated anti-malware use on the TCA (per Cyber Asset capability) is sufficient without inventorying the vendor's device and all that is on it and creating a baseline configuration for a device that is not owned or managed by the RE. Creating and maintaining such a list has little to no reliability benefit. The point should be to reasonably assure the RE that no malware is present on the device prior to connection a BES Cyber System. As an example, there is no reliability benefit to inventorying that a vendor device has "Siemens WinCC 7" software installed. The benefit to reliability is in scanning that system to see if that copy of WinCC has been compromised by Stuxnet. 6) Under the Guidelines and Technical Basis section, Page 41, under Section: Requirement R4: - consider removing the bullets under "Examples of these devices include…" and simply state "Examples of these devices include, but are not limited to, laptops, desktops, or tablets used for testing, maintenance, configuration changes, and/or vulnerability assessments." 7) Under the Guidelines and Technical Basis section, Page 42, first paragraph at the top of the page - consider having additional guidance on what does NOT constitute a single use. For example – Does use within the same PSP, but for different Cyber Assets at varying impact levels (high & medium) require a new evaluation? Is a new evaluation required prior to use for each instance that a TCA moves from one PSP to another at the same impact level, regardless if the authorized user maintained possession of the TCA, and/or the timeframe for traveling between PSPs is during the same day/week? 8) Under the Guidelines and Technical Basis section, Page 42, section Requirement Part 4.1, No. 1. – consider striking the term "physical proximity" as this is not required by the Standard as written, and would be impossible to prove. Recommend the following change – "This is intended to provide documentation of those personnel authorized to use TCAs." Also – consider striking "unescorted physical access" from the last sentence as there could be instances of personnel with authorized electronic access to the applicable system, but who are not authorized for unescorted physical access to the PSP it is contained within (e.g., periodic vendor support where the vendors are authorized for electronic access to the applicable systems, but are escorted to those systems to perform maintenance and/or troubleshooting.) 9) Under the Guidelines and Technical Basis section, Page 43, under the Section: Requirement Parts 4.2, 4.3, 4.4, 4.5: - the last sentence for the paragraph starting "Part 4.5 requires…" states that "process is to include testing and installing of updated signatures or patterns." This sentence should be struck as it is beyond the scope of the requirement written for CIP-010-2 R4.5. Although it is addressed in CIP-007-6 R3, it is not a requirement in CIP-010-2 R4.5. Southern Company also supports SMUD's comments on this question: 10) SMUD prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of "operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability)" as well as the corresponding Requirement Part 4.6 to "evaluate the Transient Cyber Asset." SMUD believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a "defined acceptable use" for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. SMUD supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. 11) If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state "Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists." As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source requirement part. 12) SMUD is

concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. SMUD does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. SMUD requests guidance be included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review. Southern Company also supports the following EEI comments to the question: CIP-010-2 Requirement R4, Part 4.1: EEI members are concerned with unnecessary administrative burdens created by Part 4.1. For example, Authorization generally applies to users. A user of a Transient Cyber Asset should be authorized to use the particular asset with certain software installed, for a particular purpose at a particular location(s). The way Part 4.1 is written suggests that four different authorization processes are needed: one for users, one for locations, one for acceptable use, and one for software/firmware. A requirement for four different processes for user authorization adds additional, unnecessary administrative record-keeping. This language should be edited to make it clear that only one user authorization process is required. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (CIP-010-2 Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. Southern Company also supports the following GTC comments to the question: In CIP-010-2 Requirement Part 4.4, the SDT proposes language that states that the entity must mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media. The threat for Transient Cyber Assets and Removable Media is not important. The BES Cyber Asset should be protected from detected malicious code on the Transient Cyber Asset or Removable Media. The SDT should consider resolving this issue by eliminating 4.4 and modifying 4.2 and 4.3 as follows: “Use method(s) to detect malicious code on [the Transient Cyber Asset or Removable Media] prior to use on applicable systems and, if detected, do not allow of the use of [the Transient Cyber Asset or Removable Media] until the threat of the detected malicious code to the applicable systems has been mitigated.”
No
Southern Company provides the below comments to the SDT for consideration with regard to new or revised definitions: 1) Removable Media definition should be more specific to the higher risk forms of media, such as USB media, and other diagnostic type devices. 2) Transient Cyber Assets, as written and defined, could include Removable Media as well, which could be interpreted at audit to include additional requirements for Removable Media. The Removable Media definition says that a Cyber Asset is not Removable Media, but the Transient Cyber Asset definition does not exclude it. Southern Company suggests both definitions need to be mutually exclusive for clarity.
Yes
Southern Company fully supports this approach to simply remove the IAC language from the 17 applicable requirements given the development and supporting processes of the Reliability Assurance Initiative (RAI). Southern Company commends NERC on the RAI effort and fully supports it as an alternative to the IAC language and a move away from a zero tolerance approach to compliance.
Yes
Southern Company agrees that the timeframes established in the revised Implementation Plan are reasonable and appropriate.
Yes
Southern Company also supports the following GTC comments to the question: GTC recommends that the SDT clarify the meaning of “associated with” in CIP-002. This clarification comes as a result of the CIP Version 5 Implementation Study and is therefore consistent with the SDT’s SAR. NERC has recently indicated that location is a determinant factor when classifying cyber asset impact. (Reference page 111 from the slides delivered by NERC Compliance at the June CIPC: http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/Presentations%20--%20June%2010-11,%202014.pdf) As such, the SDT should update CIP-002 Attachment 1 Section 2 to indicate that medium impact BES Cyber Assets are those “associated with and located at” the Facilities meeting the criteria of Attachment 1 section 2 in order to clarify the intent of the Standard.

Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
SCE&G agrees with the approach to address the directive concerning Low Impact assets from FERC Order No. 791. With regards to CIP-003-6 R2.4.1, SCE&G believes the SDT must clarify the term "external routable protocol paths". SCE&G proposes the following language to clarify the term: "All external routable bi-directional protocol paths, if any, must be through one or more identified access point(s). With regards to CIP-003 R2.2, SCE&G believes the language "to restrict physical access" included in the requirement is different from what is described in the Technical Guidelines. The Guidelines state that CIP-003 R2.2 can be accomplished using a fence and a lock. Inherently a fence does not "restrict" access; instead, it is a point of demarkation and establishes a boundary. A determined adversary can circumvent a fence in many ways including: climbing over, cutting through, etc. To truly "restrict" access entity's would have to implement additional controls beyond a lock and fence. To align with the controls described in the Technial Guidelines, which SCE&G agrees are adequate for Low Impact Assets, the SDT should consider the following revision: "Implement one or more controls to establish a physical boundary and implement access control(s) to allow access only to legitimate users."
Yes
No
SCE&G believes the SDT needs to reconsider the authorizations and baseline configuration records required under CIP-010 R4.1. Recording such authorizations and configurations will be administratively burdensome for entities. Personnel authorized for access to High and Medium BES Cyber Systems should not require additional authorizations to use Transient Cyber Assets. SCE&G proposes the SDT revise the requirement to require procedures defining the acceptable use of Transient Cyber Assets and a listing of authorized Transient Cyber Assets. Such a list needs to be generic allowing entities to authorize groups of Transient Cyber Assets (e.g. flashdrives issued by the entity). Per NIST 800-53 MA-5, entities should also be allowed to designate personnel with required access permissions to supervise the maintenance actiivities of personnel who do not possess the required access authorizations.
No
SCE&G believes the SDT needs to reconsider the authorizations and baseline configuration records required under CIP-010 R4.1. Recording such authorizations and configurations will be administratively burdensome for entities. Personnel authorized for access to High and Medium BES Cyber Systems should not require additional authorizations to use Transient Cyber Assets. SCE&G proposes the SDT revise the requirement to require procedures defining the acceptable use of Transient Cyber Assets and a listing of authorized Transient Cyber Assets. Such a list needs to be generic allowing entities to authorize groups of Transient Cyber Assets (e.g. flashdrives issued by the entity). Per NIST 800-53 MA-5, entities should also be allowed to designate personnel with required access permissions to supervise the maintenance actiivities of personnel who do not possess the required access authorizations.
No
NERC has advised that the IAC language will be replaced by the RAI process. Final ballot on the removal of the IAC language must not occur until RAI is approved. It is unreasonable to ask entities to remove such language without an approved alternate process to take its place.
No
Implementation has been negatively impacted by the everchanging state of the CIP V5 standards. To ensure cost-effective and appropriate implementation for their customers and shareholders, entities do not want to extensively begin implementation until the target stops moving. As is now the case, entities have lost precious months on the already time constrained implementation timeframe. This, in addition to the delay in the much needed Transition Guidance from the NERC Implementation Study, must be taken into consideration by NERC/FERC. Steady-state standards and clear transition guidance are essential to entities being able to successfully implement the new CIP

standards. SCE&G proposes that all standard implementation start dates be revised to reflect the completion of the CIP V6 revisions and the issuance of the Transition Guidance from NERC.
No
No
Individual
Joshua Andersen
Salt River Project
No
The Requirements proposed in 2.1, 2.2 and 2.3 provide appropriate controls for Low Impact Cyber Systems. However, the “external routable protocol paths” language in Requirement 2.4 requires entities with Low Impact Cyber Systems to provide and comply with “some form of electronic security perimeter,” regardless of risk to the Bulk Power System/Bulk Electric System. Compliance to this requirement would be excessive given the risk associated with Low Impact rated BES Cyber Systems. Additionally, entities would be required to identify, maintain and comply with “some form of electronic security perimeter” (ESP) for Low Impact rated BES Cyber Systems, yet additional revisions state that “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” This is contradictive at best and should be clarified. Recommend language changes to address only Low Impact Systems which have direct internet access. Recommend adding language which assesses risk to Low Impact BES Cyber Systems with “external routable protocol paths.”
Yes
No
CIP-010-6 R4.1.4 requires the Entity to “identify and document the Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability).” And in 4.6, the Entity is required to “Evaluate Transient Cyber Assets, prior to use, for modifications that deviate from Part 4.1.4.” For entities that depend on vendors and contract support personnel to maintain the Reliability of the Bulk Electric System, this becomes a great administrative challenge. This requirement becomes dependent upon the number of Transient Devices, the number of vendors, contractors or support personnel, and the type and variance of Transient Cyber Assets and tools used to perform their job duties. The challenge in requiring a baseline of firmware alone far exceeds the vulnerably and risk to the BES Cyber Asset. Recommend changing the language in requirements R4.1.4 and R4.6 to address Entity owned-maintained Transient Devices separately from Vendor or Contracted Support owned-maintained Transient Devices. This allows entities to reasonably develop and implement Administrative and Technical Security Controls for Transient Devices based on risk, yet monitored from a compliance standpoint. Recommend language changes to require “the implementation of a Transient Device Security Baseline for Entity and Vendor/Contracted Support Transient Devices.” This allows Entities to implement controls yet maintain the flexibility to address multiple device types and functions. This also allows Entities and their vendors or contracted support personnel to implement Administrative and Technical controls of Transient Devices based on risk. Recommend language changes to require sampling of Transient Devices Security Baseline. This allows Entities a mechanism for monitoring both Entity and Vendor/Contracted Support personnel owned-maintained Transient Devices. Recommend language changes to require a security policy for Transient Devices which includes a requirement for Transient Devices with direct access to BES Cyber Systems. This allows Entities to establish and implement Administrative Controls for Transient Devices.
Yes
Yes
No

Recommend changing the Implementation Plan time schedule to fall after the CIP Version 5 standards implementation dates.
No
No
Group
Associated Electric Cooperative, Inc. - JRO00088
Phil Hart
No
AECI agrees with NRECA comments. Regarding 2.3.1 - Escorted should be removed. Typically, these facilities are smaller work environments that can manage appropriate access to visitors via a policy without the need to require escort. Regarding 2.4.2 - This requirement should be removed or reduced to not include inbound and outbound access permissions, and more importantly remove the reason for granting access. This requirement is a very specific control that FERC specifically stated was not needed. Although this is common practice for most entities, the compliance burden created to prepare for audit exceeds the benefit gained in reliability. Management of all firewall rules at all low impact facilities is a tremendous effort for small entities, and the largest gain in reliability is realized with the creation of processes to address these items, not specifically listing each. If requirement 2.4 stated "Implement one or more documented processes that collectively address the following…" and it is understood that entities would only be required to have implemented procedures that consider these items, and not specifically list them, then AECI would argue this more accurately represents the FERC order by creating a requirement that could be used to evaluate the sufficiency of a program without developing specific controls such as this draft currently has. The corresponding measure would also need to include language that allows for flexibility of procedures to not include every specific inbound and outbound permission rule. Entities with sufficient resources and capability could include specific listings of these rules to demonstrate exceptional compliance, however those without the means would not be held liable for over-specific controls on facilities that have no impact to the BES.
No
AECI agrees with NRECA comments.
No
AECI agrees with NRECA comments.
No
AECI agrees with NRECA comments.
Yes
AECI agrees with NRECA comments.
No
AECI agrees with NRECA comments. It would be very advantageous if industry was allowed to triage compliance on LIAs, similar to the FAC-008 alert. More significant impact LIA facilities would be addressed first in implementation plans while less significant facilities would receive additional time to become compliant.
Yes
AECI agrees with NRECA comments.
Individual
David Revill
Georgia Transmission Corporation
No
We are concerned that by borrowing language from Medium Impact requirements, the SDT has introduced a substantial increase in administrative overhead to comply with the standard without an equivalent increase in security. Specifically, maintaining the documentation of justifications for every

firewall rule results in a significant amount of man-hours devoted to compliance and not to improving the security of the low impact assets. We instead recommend the following language for CIP-003 R2: R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3 (assets containing low impact BES Cyber Systems), shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2.1 Review and obtain CIP Senior Manager approval at least once every 15 calendar months for a cyber security policy that addresses CIP-003-5, Requirement R2, Part 2.2. 2.2 The Responsible Entity shall implement one or more documented processes that collectively address the following topics: 2.2.1 Operational or procedural control(s) that restrict physical access to low impact BES Cyber Systems; 2.2.2 Access control(s) to restrict electronic access to low impact BES Cyber Systems via the asset's external routable protocol connections and Dial-up Connectivity, if any; 2.2.3 Cyber security incident response including conditions for activation of the response plan(s), roles and responsibilities of responders, and determination if an identified Cyber Security Incident is a Reportable Cyber Security Incident with notification of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law; and 2.2.4 Security awareness for the Responsible Entity's personnel that, at least once each calendar quarter, reinforces cyber security practices. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.
Yes
Yes
No
Similar to its comments on Low Impact, we disagree with simply borrowing requirement language from Medium impact requirements for Transient devices. In this case, we believe that the SDT has provided unnecessary administrative overhead and introduced constructs that are not ideal for transient devices. Requirement part 4.1 requires authorization, but provides little security benefit. In particular, the SDT proposes that defined acceptable be authorized. Almost all companies have an existing acceptable use policy. However, it seems this may not be the intent of the SDT. The SDT should be clearer about the intent so that it is simply requiring entities to create lists and perform administrative exercises in order to prove compliance. In requirement part 4.4, the SDT proposes language that says that the entity must mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media. The threat for Transient Cyber Assets and Removable Media is not important. It is the BES Cyber Asset that should be protected from detected malicious code on the Transient Cyber Asset or Removable Media. The SDT could resolve this issue by eliminating 4.4 and modifying 4.2 and 4.3 as follows: "Use method(s) to detect malicious code on [the Transient Cyber Asset or Removable Media] prior to use on applicable systems and if detected, do not use this [Transient Cyber Asset or Removable Media] until the threat of the detected malicious code to the applicable systems has been mitigated."
Yes
Yes
No
Yes
We recommend that the SDT clarify the meaning of "associated with" in CIP-002. This clarification comes as a result of the CIP version 5 implementation study and is therefore consistent with the SDT's SAR. NERC has recently indicated that location is a determinant factor when classifying cyber asset impact. (Reference page 111 from the slides delivered by NERC Compliance at the June CIPC: http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/Presentations%20--%20June%2010-11,%202014.pdf) As such, the SDT should update CIP-002 Attachment 1 Section 2 to indicate that medium impact Cyber Assets are those "associated with and located at" the Facilities meeting the criteria of Attachment 1 section 2 in order to clarify the intent of the standard.
Individual

Nathan Mitchell
American Public Power Association (APPA)
No
APPA agrees that some of the changes the SDT has made in the draft standards address the recommendation in order 791 the Commission “defining with greater specificity the processes that responsible entities must have for Low Impact facilities under CIP-003-5.” However, APPA believes the SDT has gone too far in certain aspects of this specificity to include requirements that impose compliance costs that exceed the reliability benefit to the BES. Cost of compliance with CIP standards must be in line with the risk of malicious actions that could cause instability, uncontrolled separation or cascading failures. The thresholds for the high and medium impact categories were selected to ensure that specific security controls are in place in facilities that can cause instability, uncontrolled separation or cascading failures. The programmatic controls for low impact facilities were designed to ensure security policies and procedures covered all BES Cyber Systems. In particular, APPA believes the SDT has not taken into consideration this cost to risk evaluation in the development of the new requirements in CIP-003 R2 Part 2.3. The new requirement in Part 2.3.1 which requires escorted access for visitors will impose a significant burden without a commensurate reduction in cyber security risk for reliable operation of the BES. APPA believes the cost of developing and implementing a documented process for escorted visitor access for Control Centers that control multiple facilities by voice instruction only is out of line with the risk to reliable operation of the BES. For example, APPA members report that CMEP personnel rely on FAQs developed for previous versions of CIP standards to conclude that Control Centers that “control” remote Facilities through voice commands only are subject to the CIP standards. See NERC link: http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf (Question 9). If it was the intent of the SDT to limit the scope of 2.3.1 to Control Centers with capability to control multiple facilities automatically or remotely, this must be stated specifically in the standard. Ultimately, APPA recommends that the SDT remove 2.3.1 since this requirement would not significantly reduce the risk of instability, uncontrolled separation or cascading failures on the BES. The intent of segmenting out Low Impact facilities was to assure that programmatic controls were in place for those facilities that had “Low Impact” on the BES. The compliance burden on these systems must be in proportion to its impact on the BES. APPA recommends that the SDT evaluate compliance costs in any changes they make to the revised standards prior to the final ballot.
Yes
APPA appreciates the SDT providing flexibility to entities in complying with R1 Part 1.10. Having multiple options for controls when physical access restrictions are not possible gives entities an opportunity to select the solution that works for each specific situation. Industry has commented that encryption of data as a sole solution may reduce reliability by adding complexity to the systems and introducing latency to data flow that will not work in a relay control environment. If the SDT removes this flexibility or expands the applicability in future drafts APPA will need to reevaluate its support for the communications controls.
No
APPA supports the comments of SMUD on this question
No
APPA supports the comments of SMUD on this question
Yes
APPA supports the removal of the Identify, Assess, and Correct (IAC) language from the 17 requirements. APPA encourages the SDT to provide guidance to NERC staff on the development of the proposed RSAWs. This guidance will give regional auditors insight to the intent of the SDT in drafting the standards and the reliability outcomes. APPA members would appreciate a commitment from NERC staff to timely complete development and publish details of the RAI program to give industry an indication of the proposed enforcement discretion program. This may give them more confidence to cast an affirmative vote for these changes in the final ballot.
No
If the draft requirements for Low Impact Control Centers remain then a new implementation date for these requirements must be considered. APPA recommends a 1 year extension to April 1, 2018 for Low Impact Control Centers since entities will need time to budget and implement security controls

in addition to developing compliance plans. Due to the uncertainty created by this revision process and not knowing what the Commission will order or when the final rule will be issued, the SDT needs to revise the implementation options for CIP-003-6 R2. APPA recommends modifying the implementation plan for CIP-003-6 to become enforceable 2 years after Commission approval or April 1, 2017, whichever is later.
Yes
The SDT proposals will increase the compliance burden by adding requirements to the Low Impact sections. APPA urges NERC to survey registered entities, especially small entities, to estimate the real compliance cost of CIP V6 Revisions before the standards are submitted to FERC for approval. APPA in its comments to the Commission in the CIP V5 NOPR asked that FERC require NERC to do this survey. However in P261 of the Final Rule FERC stated, “To the extent that entities provide NERC with such information, we encourage NERC to submit the cost data along with the associated new or revised Reliability Standards requirements.”
Individual
Nicholas Lauriat
Network & Security Technologies
No
Proposed "Transient Cyber Asset & Removable Media Protection" requirements 4.3 and 4.6 of CIP-010-2 compel malicious code detection (4.3) and an evaluation of current configurations against a previously established baseline (4.6) “prior to use.” These two requirements are unacceptably ambiguous by virtue of the fact a “use” is not defined within the language of any CIP V5 requirement. The SDT has attempted to define “use" in the Guidelines and Technical Basis section as follows: "For purposes of this standard, ‘use' is considered to be the interaction between transient devices and applicable systems. The interaction between transient devices and multiple applicable systems within the same ESP or PSP would be considered a single use.” However, as NERC representatives often point out, guidelines are non-binding. Moreover, N&ST believes the suggested definition of “use,” if widely adopted as an audit benchmark, could create unacceptable and counter-productive administrative and compliance burdens for Responsible Entities. If a technician used a laptop to test BES Cyber Systems at a Control Center and then drove directly to the backup Control Center, the Responsible Entity would be at risk of being found non-compliant with R4.6 unless the prescribed evaluation was performed before the technician used that same laptop to perform similar BES Cyber System testing. N&ST appreciates the importance of minimizing the risk of introducing malicious code to BES Cyber Systems via transient devices and removable media. However, N&ST believes these requirements should be modified to avoid a negative impact on BES operations. One option the SDT might consider is to make R4.3 and R4.6 time-based requirements (e.g. every 30-60 days), with the additional provision of requiring R4.3 malicious code detection and R4.6 evaluations to be performed “prior to use” for any transient devices or removable media that have been used for any purpose other than for interaction with applicable systems.
Individual
Thomas Standifur
Austin Energy
No
The addition of more objective criteria for Low impact BES Cyber System Requirements within CIP-003-6, R2, breaks one of the prime objectives defined when CIP version 5 was being developed that each of the Standards could stand on its own. Entities with Low “and” either Medium or High Cyber BES Cyber Systems, it would be necessary that CIP-003 “always” be referenced when any of the

requirements in CIP-004-6 through CIP-011-2 for the Medium and High Impact BES Cyber Systems are being designed and implemented, since dependencies are always possible between Cyber Systems part of any impact category. The inclusion of these objective requirements with a unique table in CIP-003-6 result in Standards language inconsistencies that creates confusion and additional compliance risks. A new definition is now needed for CIP-003-6, R2, Requirement Part 2.4 for the phrase “external routable protocol paths” to ensure that entities and auditors clearly understand the differences between that phrase and the defined term External Routable Connectivity. This would avoid duplicating the confusion seen in earlier versions of the CIP Standards, such as the CIP-001 confusion between Facilities and facilities. The phrase “external routable protocol paths” may create a similar interpretation risk.
Yes
No
AE prefers to remove CIP-010, R4, Requirement Part 4.1.4 requiring the maintenance of “operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability) as well as the corresponding Requirement Part 4.6 to “evaluate the Transient Cyber Asset.” AE believes that this is a list making administrative activity. Requirement Part 4.1.3 has already established a “defined acceptable use” for Transient Cyber Assets that establishes how these assets are to be used within the Responsible Entity. Transient Cyber Assets are not expected to be treated like a BES Cyber Asset or associated Protected Cyber Asset considering the use of these assets may be subject to ownership by a contractor or vendor where obtaining all of this information may not be possible. AE supports the use of inventory, assignment, acceptable use, malicious software prevention and patching for these assets as reasonable controls to ensure the devices reduce the risks posed to BES Cyber Systems. If CIP-010, R4, Requirement Part 4.1.4 is not removed, SMUD requests that the language be aligned with CIP-010, R1, Requirement Part 1.1.1 to state “Operating system(s) (including version) or [emphasis added] firmware where no independent operating system exists.” As presented, the CIP-010, R4, Requirement Part 4.1.4 is a greater expectation than the source requirement part. AE is concerned with CIP-010, R4, Requirement Part 4.7 and an interpretation that entities would have to track both the 35 day update timeframe and each use to be able to show performance to the Requirement Part. AE does not believe that the tracking of use is the key outcome of this Requirement Part; instead it is the patching of the Transient Cyber Asset that is the expected outcome. AE requests guidance be included to clearly state that the tracking of each use is not expected to be maintained, but that there is evidence associated with a 35 day review.
Yes
Yes
Yes
No
No
Individual
Michelle D'Antuono
Ingleside Cogeneration, LP
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
No
NRECA understands that the approach to add greater specificity and auditability to the required processes in CIP-003 R2 can fulfill the FERC directive in Order No. 791. However, NRECA has

concerns with the requirements in the current proposed draft. From a policy level, we are concerned that the revisions go beyond what the FERC directive required and that the distinction between low and medium impact BES Cyber Systems is becoming less and less clear. Additionally, the current proposed revisions are increasing the financial, compliance and operational burdens on entities for low impacts beyond the benefits it will provide to BES security and reliability. The emphasis, burden and investment of resources for entities must continue to focus on their finite resources on addressing the most impactful first (High and Medium), and then the least impactful (Low). NRECA believes that the primary focus on cyber security must remain with the Medium and High Impact classified facilities. By definition, Low Impact facilities are categorized as low because failure or degradation of those assets have minimal to no impact on BES reliability. The financial, compliance and operational burdens must be commensurate with the risk to the reliability of the BES, which specifically applies to preventing instability, cascading or uncontrolled separation of the BES. It is difficult to see how the CIP-003 R2 revisions and additions could help to limit BES instability, cascading or uncontrolled separation. NRECA requests that the SDT demonstrate how all changes to CIP-003 R2 will contribute to preventing instability, cascading or uncontrolled separation of the BES. NRECA is concerned that by borrowing language from Medium Impact requirements, the SDT has introduced a substantial increase in administrative overhead – staffing and financial -- to comply with the standard without a commensurate impact on BES reliability and security. Specifically, maintaining the documentation of justifications for every firewall rule results in a significant amount of man-hours devoted to compliance and not to improving the reliability and security of the low impact assets. NRECA instead recommends the following language for CIP-003 R2: R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3 (assets containing low impact BES Cyber Systems), shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] 2.1 Review and obtain CIP Senior Manager approval at least once every 15 calendar months for a cyber security policy that addresses CIP-003-5, Requirement R2, Part 2.2. 2.2 The Responsible Entity shall implement one or more documented processes that collectively address the following topics: 2.2.1 Operational or procedural control(s) that restrict physical access to low impact BES Cyber Systems; 2.2.2 Access control(s) to restrict electronic access to low impact BES Cyber Systems via the asset's external routable protocol connections and Dial-up Connectivity, if any; 2.2.3 Cyber security incident response including conditions for activation of the response plan(s), roles and responsibilities of responders, and determination if an identified Cyber Security Incident is a Reportable Cyber Security Incident with notification of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law; and 2.2.4 Security awareness for the Responsible Entity's personnel that, at least once each calendar quarter, reinforces cyber security practices. An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Mandating specific controls could have the undesirable consequence of stunting the development of the range of controls necessary to protect the diversity of Low Impact assets. Entities should be afforded discretion to utilize their experience and expertise to develop controls that protect their assets commensurate with the BES reliability risk posed. At this juncture, a one-size-fits-all approach that imposes greater obligations on Low Impact BES Cyber Systems would simply increase costs and burden, without commensurate benefits, to both the Registered Entities and the Regional Entities charged with ensuring compliance with the CIP standards. NRECA supports the SDT position that entities subject to the Low Impact BES Cyber System requirements in CIP-003-5 R2 to keep an inventory or list to help ensure that they have properly identified and categorized the location of its BES Cyber Systems. However, the currently proposed requirements all but require the development of such a list. NRECA request that the SDT revise the requirements so that such a list is not indirectly or directly required. Requiring entities to maintain a discrete list of Low Impact BES Cyber Systems, as opposed to the location of such assets, will involve considerably more time and cost, again without any commensurate benefit to BES reliability and security. While not the work of the SDT, RAI and the RSAWs are companion pieces to the CIP V5 standard revisions. Unfortunately, the initial draft RSAWs don't provide the needed clarity or relief from the zero defect compliance expectation. NRECA encourages NERC to continue their work and collaboration with the SDT and to post revised RSAWs with next comment and ballot period for CIP V5 revisions. Regarding RAI, NRECA recommends that NERC use the requirements on Low Impact assets to demonstrate how RAI can alleviate the compliance concerns and create a reasonable approach to compliance. This may be essential for the passage of revised requirements on Low Impact assets. Additionally, if RAI is not adequately explained and clearly understood before the next comment and ballot period, NRECA believes that ballots for the CIP V5 revisions may be

negatively impacted. Some “affirmative” ballots may change to “negative” without a better understanding of RAI and how it relates to the CIP V5 revisions.
Yes
NRECA views Requirement CIP-007 R1.2, as only specifying how to be compliant with other requirements within the suite of CIP Standards. Adding duplicative requirements only increases the compliance burden and audit confusion, without commensurate value to increased BES security and reliability. NRECA requests the SDT review this issue and remove duplicative requirements from the CIP standards. NRECA is concerned that the new and undefined term of “nonprogrammable communication components.” We request that the SDT provide more clarity around the meaning of the this term. NRECA requests additional guidance related to CIP-006 R1.10 on what constitutes adequate physical protection of connectors joining separate conduit sections. This is needed to minimize confusion at audit.
No
NRECA recommends the SDT remove new CIP-010 R4.1.4. Defining users, locations and acceptable use of these devices should be sufficient to protect these devices from unauthorized or harmful use. This requirement expands in R4.6 and R4.7 and becomes extremely difficult to manage. A detailed listing of all software and hardware is not necessary to fulfill requirements R4.6 and R4.7. An effective change management procedure coupled with documents required in R4.1.1 R4.1.2 and R4.1.3 will allow for objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity’s protections without the need for a prescriptive list. Further, compliance with R4.6 and R4.7 will likely be met through the use of software whitelisting, not documentation. A documented list of operating system, firmware, and software on transient devices is not needed for such an implementation and provides no benefit to BES reliability and security which should be focused on preventing instability, cascading and uncontrolled separation of the BES.
No
NRECA believes the Transient Cyber Asset definition language is overly broad. Using "directly connected" would apply to any programmable device, whereas the focus should be towards devices that can infect, alter, or transfer files to a BES Cyber Asset. Recommended language for a revised definition is as follows:: Transient Cyber Asset: A Cyber Asset directly connected, and able to infect, alter, or transfer files to BES Cyber Assets, for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. NRECA disagrees with the SDT’s borrowing requirement language from Medium impact requirements for Transient devices. In this case, we believe that the SDT has provided unnecessary administrative overhead and introduced constructs that are not ideal for transient devices. Requirement part 4.1 requires authorization, but provides little security benefit. In particular, the SDT proposes that “defined acceptable use” be authorized. Almost all companies have an existing acceptable use policy. However, it seems this may not be the intent of the SDT. The SDT should be clearer about the intent so that it is not simply requiring entities to create lists and perform administrative exercises in order to prove compliance. In requirement part 4.4, the SDT proposes language that says the entity must mitigate the threat of detected malicious code for Transient Cyber Assets and Removable Media. The threat for Transient Cyber Assets and Removable Media is not important. It is the BES Cyber Asset that should be protected from detected malicious code on the Transient Cyber Asset or Removable Media. The SDT could resolve this issue by eliminating 4.4 and modifying 4.2 and 4.3 as follows: “Use method(s) to detect malicious code on [the Transient Cyber Asset or Removable Media] prior to use on applicable systems and if detected, do not use this [Transient Cyber Asset or Removable Media] until the threat of the detected malicious code to the applicable systems has been mitigated.”
Yes
NRECA believes removal of IAC language clarifies those requirements and what is expected during audit; but without RAI adequately explained and clearly understood before the next comment and ballot period, NRECA believes that ballots for the CIP V5 revisions may be negatively impacted. Some “affirmative” ballots may change to “negative” without a better understanding of RAI and how it relates to the CIP V5 revisions.
No

NRECA has several significant concerns with the proposed Implementation Plan (IP). First, it appears that the IP is posted only for comment, but not for ballot. NRECA asserts that this potentially violates the NERC Standards Process Manual (SPM). While there are many references in the SPM requiring the IP to be balloted, NRECA directs SDT and NERC attention to SPM Sections 4.4.3, 4.6, 4.8, 4.16 for provisions that clearly require the IP to be balloted. In this current formal comment and ballot period, entities can only submit comments on IP – there is no provision or ability to cast a ballot on the IP as the SPM requires. NRECA requests that this potential SPM violation be addressed expeditiously as possible to ensure the CIP V5 revisions are developed in clear compliance with the FERC approved NERC SPM. NRECA believes the proposed IP does not adequately provide enough additional time to comply with the currently proposed revisions and new requirements to the CIP V5 standards. For those revised and new requirements, NRECA requests additional time be included in the IP that matches the time entities were originally provided upon FERC's approval of CIP V5. If the original amount of time that was provided for CIP V5 was adequate then, it should also be adequate for revised or new requirements for the CIP V5 revisions. This is especially critical for the new requirements in CIP-003-6 R2. NRECA also requests that the SDT consider using the same additional time for compliance for all revised or new requirements under the current CIP V5 revision project. One of NRECA's members estimates that its implementation burden for the currently proposed CIP-003-6 R2.4.2 will take over 4000 hours initially and 2000 hours annually. Depending on the final requirements, these estimates could increase.
Yes
NRECA supports addressing FERC's four directives in the current project. Industry needs stability, closure, and a steady state of CIP standards so that industry can comply with a non-moving target of requirements. NRECA supports the RAI concept, but is seeking greater understanding of and informative experience with RAI. For NRECA and its members, filling this gap may be essential for the passage of revised requirements, in particular for Low Impact assets. Low Impact asset requirements are ideal to demonstrate how RAI can alleviate the compliance concerns and create a reasonable approach to compliance.
Group
Bonneville Power Administration
Andrea Jessup
No
Although the proposed controls and objectives are clear as written, BPA believes they are insufficient to adequately provide protection of the BES. If the low impact assets represent the majority of the BES, the proposed NERC CIP standards should address risk due to aggregated impact and reduce the extremely large attack surface. BPA suggests the requirement language should include an annual assessment of BES LIA to baseline and monitor their security status. In addition, BPA believes the LIA requirements should be distributed throughout each of the proposed standards (CIP-002 through CIP-014.)
No
Although the proposed scope is clear and auditable, BPA believes the control coverage is insufficient to provide adequately assured protection of the BES. If the low impact assets represent the majority of the BES, and non-routable communications are no longer considered "safe," the proposed NERC CIP standards should address risks related to all open system interconnection layers (physical to application.) Attacks against communication networks have evolved where protocol types are no longer relevant.
No
While BPA agrees that CIP-010 R4 addresses the risks related to High and Medium impact assets, the proposed requirement language should also address Low Impact Assets. In addition, BPA suggests requirement language should be added to include implementation of Transient Device baselines, with periodic sampling, for entity and vendor managed devices. Entities may also consider removing direct-access to BES assets by Transient Devices (e.g. jumpbox, proxy, etc.) Furthermore, standards addressing transient devices must acknowledge the nature of these devices and the fact that the responsible entity does not always exercise continuing controls over these devices. Policies, procedures, and technological solutions must focus on transient devices at the time of connection

and on controlling the interfaces to the system rather than attempting to exercise continuous control over control over a device of a transient nature.
Yes
No
BPA supports the removal of the IAC language and the move away from “zero defect” requirements. However, BPA believes the lack of clearly defined measures results in inconsistent audit approaches and findings. In addition, BPA expects the RAI will be fully vetted publicly.
Yes
The additional timelines are sufficient. However, BPA suggests that all CIP Version 5/6 requirements become effective on this revised date to avoid confusion, with the exception of Low assets which are afforded a minimum of an additional 12 months before the initial compliance date.
No
No
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
Yes
No
CIP-006 R1.10: “monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection…” When does “detection” actually occur? A 15 minute window for notification is typically not sufficient to respond to an automated alert during regular business hours, and would be impossible after hours. The last bullet of R1.10, “an equally effective logical protection” is ambiguous. Who/what would determine the effectiveness of logical protection other than the two previous bullets? Tri-State suggests removing this bullet. Tri-State believes that there is still a need to define what a communication network is. This was ordered by FERC and we do not agree that this has been clarified in the current draft.
Yes
How does the SDT anticipate that RE’s enforce/assess Transient Cyber Assets and Removable Media that are owned and maintained by consultant services? CIP-004 R1 should read R2 in the question above. For R2.1.9, it reads better as “…and interoperability with other Cyber Assets, including Transient Cyber Assets and Removable Media.”
Yes
No
The FERC Order “directed NERC to remove the “identify, assess, and correct” language or to propose modifications that addressed the Commission’s concerns about the ambiguity and enforceability of that language.” Tri-State feels that the IAC language is helpful and the removal solution attempted was overly complicated and left gaps that were not all adequately addressed. The removal of identify, assess, and correct also diminishes the value of the standards. It would have been much simpler to have “proposed modifications that addressed the Commission’s concerns about the ambiguity and enforceability of that language.” The easiest solution is to define “identify, assess, and correct” as one defined term rather than as three separate words. Tri-State also recommends that the term “deficiencies” when referenced with IAC language be changed to “possible violations” as defined in NERC’s Compliance Monitoring and Enforcement Program to remove ambiguity.
Yes
No

No
Individual
Bill Temple
Northeast Utilities
No
In an effort to differentiate the compliance responsibilities for entities between Medium and Low Impact Assets, the SDT has in effect ended up creating a greater burden on entities to create, manage and define programs that meet compliance. The requirements of this revision are inconsistent and overly complex. Examples include but may not be limited to; ¬ Ambiguous and inconsistent terms “External Routable Paths” versus “External Routable Connectivity”. ¬ More restrictive requirements for Low Impact Assets. ¬ Inconsistent Testing Time frames. ¬ Instances where there was a Failure to extend implementation Time frame beyond the original version 5 effective compliance date.
Yes
Please expand on the expectations for meeting this requirement with regard to "patch panels". 1. If the Cyber Assets in the ESP are meeting the requirements by disabling unneeded ports on the device, is there any action needed on the patch panel? 2. The patch panel may have connectors that are not used or may be connected to ports that are disabled. Is signage or tamper tape truly required on the patch panel in that situation?
No
Please expound upon the “CAUTION” statement in the Guidelines and Technical Basis. For example, would it be permissible to have a Transient Cyber Asset use a secure wireless network to only access a secured network drive containing relay configuration data. For Transient Cyber Assets, please consider adding a statement in the Guidelines and Technical Basis from CIP-007-5 R3 “If a specific Transient Cyber Asset has no updateable software and its executing code cannot be altered, then that Transient Cyber Asset is considered to have its own internal method of deterring malicious code.” With the proliferation of IEC61850 substations, test equipment with proprietary software and executing code are commonly used. Please provide examples where a transient cyber asset had wireless enabled such that the transient cyber asset was not an electronic access point.
Yes
Yes
No
CIP-003-6 R2 compliance enforcement date needs to change from the version 5 compliance enforcement date. (April 1st 2017). Recommend Nine months after the compliance enforcement date of version 5 (February 1st 2018
No
Individual
Jen Fiegel
Oncor Electric Delivery Company LLC
No
Oncor supports comments submitted by EEI and Southern Company
Yes
Oncor supports comments submitted by EEI and Southern Company
No
Oncor supports comments submitted by EEI and Southern Company with the following additional comments: CIP-010-2 R4.1 – Authorize the usage of Transient Cyber Assets prior to initial use, except for CIP Exceptional Circumstances. This requirement places a lot of overhead to maintain lists

or some form of documentation that documents for each transient cyber asset that connects to a Medium Impact BES Cyber System and tying it to some defined initial use time to show compliance. Most of the assets in Medium Impact BES Cyber systems are assets in substations that don't have communication external to the substation therefore the stated "initial use" would be hard to determine let alone document to the level of accuracy needed to establish compliance. Additionally, this burdensome requirement of creating and maintaining such lists adds little or no benefit to reliability or security. Oncor's requests consideration that requirement 4.1 not be applicable to Medium Impact BES Cyber Systems. A better alternative would be authorized users whose transient devices meet 4.1.4 compliance of having pre-authorized operating system, firmware, and intentionally installed software.
No
Oncor supports comments submitted by EEI and Southern Company
Yes
Oncor supports comments submitted by EEI and Southern Company
No
Oncor supports comments submitted by EEI
No
Yes
Oncor supports comments submitted by EEI
Individual
Judy VanDeWoestyne
MidAmerican Energy Company
No
Limit the applicability for dispersed generation to the point where those resources aggregate to greater than 75 MVA to a common point of interconnection at 100 kV or above and not at an individual turbine, inverter or unit level in the CIP-003-6 Applicability section similar to PRC-005. This applicability change would apply only in CIP-003-6 standard for the low impact asset requirements. See comments on question 8. // Table titles in other standards reflect the requirements not the applicability. We recommend changing the table title for consistency to: "CIP-003-6 Policies, Processes, Plans and Programs." // Background Section 6: With the addition of the tables, the Introduction Background Section 6 should include a paragraph referencing the tables and the "Applicable Systems" Columns in Tables section that is included in the Background section for other standards. ***The paragraph for CIP-003-6 Background Section 6 would be: "Requirement R2 opens with, "Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 –Policies, Processes, Plans and Programs." The referenced table requires the applicable items in the procedures for the requirement's common subject matter." Insert the Applicable Systems boiler plate from other CIP standards into the Background Section 6 for CIP-003-6 with regard to Requirement R2. // In R2: Add back: "for its assets identified in CIP-002-5.1 Requirement R1.3" in CIP-003-6 R2 for clarification. ***Revise the requirement to: "Each Responsible Entity for its assets identified in CIP-002-5.1 Requirement R1.3 containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in CIP-003-6 Table R2 – Policies, Processes, Plans and Programs. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning] Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required." // Requirement R2, Part 2.1 – An entity may not have a low impact BES Cyber System at a Control Center (R2.3) and therefore R2, Part 2.3 is not applicable. ***Revise the requirement text to: "that collectively address the applicable topics in CIP-003-6, Requirement R2, Parts 2.2 -2.6." // Requirement R2, Subpart 2.4.2 - Remove "by default" as it implies the use of a firewall, which limits access control options. For example, an entity could use access control lists on a router or switch to provide security for traffic control. However, routers and switches do not do this by default. This will allow entities more options on how to accomplish traffic control. Include allowance for access permission reasons by individual or group in the requirement. ***Revise requirement R2.4.2 to: "For each identified access point, if any, require inbound and outbound access permissions and deny all other

access. Document access permission reasons individually or by group.” // Requirement R2, Part 2.6 - The specificity of what must be covered and tracking two time periods is more prescriptive than the requirements for medium and high impact BES Cyber Systems and is not commensurate with the risk. The proposed revision uses language from the medium/high impact requirement (CIP-004-R1.1) with the time period adjusted to once every 15 calendar months to differentiate for the lower risk. Cyber security awareness can be addressed during annual training for employees and contractors in addition to other ongoing cyber security awareness communications. Remove references to other subpart requirements as all subparts may not apply to all entities. ***Revise requirement to: “Implement a security awareness program that reinforces cyber security practices at least once every 15 calendar months.” // Guidelines and technical basis – Clarify the drawings by more specifically identifying the external routable path(s). It appears that users of the guidelines are to infer the business network is a separate external routable protocol path. Please reconsider the drawings.

Yes

We agree with the approach to address protections for nonprogrammable components of communication networks. // We have concerns regarding the removal of the “identify, assess and correct” language. See comments on question 5. // We recommend an addition to the guidelines and technical basis for CIP-006-6 R1.10 to capture FERC’s clarification that entities are not expected to enforce this requirement on third party nonprogrammable components that are out of the entities’ control.

No

No changes are needed for the malicious code and signatures/patterns Parts 4.2, 4.3, 4.4 and 4.5. // We do not agree with Part 4.1. FERC’s Order 791 noted the approach to addressing the risks associated with transient devices should be done without imposing unduly burdensome requirements on responsible entities. The controls in Parts 4.1 should be revised to reduce burden. Subpart 4.1.1 should not require users to be authorized for the Transient Cyber Asset if users are already authorized for the applicable systems. Duplicate authorization would be unduly burdensome. Subpart 4.1.2 and 4.1.4 are unduly burdensome by requiring the additional obligation of authorization for locations and software. FERC’s directive can be addressed by documenting the locations and software, without requiring authorization. Subpart 4.1.3 and 4.1.4 require documenting defined acceptable use, operating systems or firmware, which is exceeds FERC’s directive. Part 4.6 references Subpart 4.1.4. // We recommend revising Part 4.1 to only address user authorization. We recommend a separate part for documenting locations. We recommend a separate part for documenting software. Retain the applicable systems in 4.1 for the revised 4.1 and the two new Parts (High and Medium Impact and associated PCA.) *** Recommended text *** Part 4.1 – “Authorize, except for CIP Exceptional Circumstances, users individually or by group/role for electronic access to the Transient Cyber Asset when it is not required to authorize users for electronic access to the applicable systems to which the user is connecting. Authorization is based on need, as determined by the Responsible Entity. (When users are already authorized for electronic access to the applicable systems the user is connecting to, additional authorizations for the Transient Cyber Asset are not required.) OR Designate organizational personnel with required electronic access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required electronic access authorizations.” This is from NIST 800-53 Control MA-5, which provides an option for escorted electronic access. FERC Order 791 paragraph 136 refers to the MA and MP NIST controls. ***Recommended text Part 4.X – “Document locations of applicable systems, individually or by group/role where the Transient Cyber Assets can be directly connected to applicable systems. Document if the Transient Cyber Asset may be directly connected to non-applicable systems. A list of non-BES locations is not required.” (Separate Transient Cyber Assets are not required for different BES impact levels or non-BES and are not practical for substations.) *** Recommended text Part 4.Y – “Document software installed on Transient Cyber Assets (per Cyber Asset capability.)” // In Part 4.6, revise the reference to Subpart 4.1.4 to the new Part 4.Y. // We propose a few changes for Part 4.7. ***Revise the requirement to: “Evaluate Transient Cyber Assets, within 35 calendar days prior to use, for applicable security patches and take one of the following actions: (bullet) Apply the applicable patches; or (next bullet) Create a mitigation plan; or (next bullet) Revise an existing mitigation plan. // The goal is to protect the applicable system(s) to which the Transient Cyber Asset will be connected. To clarify this, the structure of the applicable systems column should be revised to follow the model used for PACS in CIP-006-5 R1.1. For

example, ***revise applicability to: “Transient Cyber Assets directly connected to (bullet) High Impact BES Cyber Systems and their associated PCA, (next bullet) Medium Impact BES Cyber Systems and their associated PCA”. If this change is made the guidance won’t need to be revised, Requirement R4: This requirement applies to any transient devices...” // Guidance also suggests, “It may be reasonable to have separate Transient Cyber Assets for each impact level.” It is not reasonable. It would be cost-prohibitive and complicated to track. // “Prior to use” for every transient device every time the device is moved from one ESP (or PSP) to another is not practical for the associated level of risk.
No
We agree with the revised definitions and with the new definition for Transient Cyber Assets. However, although the definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to, the definition for Removable Media does not name what Removable Media are connected to. Also, the final sentence sounds backwards. We recommend the following ***revised definition: “Removable Media: Portable media, connected for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset, that can be used to copy, move and/or access data. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
No
We agree with the standard drafting team’s approach to remove the “identify, assess and correct” language and the concept of compliance exceptions to address the resulting gap. However, we are concerned compliance exceptions have not been implemented for all entities. Similar concerns were expressed at the MRC pre-meeting on July 16. NERC can support Standard Drafting Team efforts by implementing compliance exceptions prior to the second or final ballot.
No
The implementation plan should provide for skipping CIP version 5 in the scenario where CIP version 6 is ordered before the CIP version 5 effective date (for medium and high, for example), but results in a CIP version 6 effective date after the CIP version 5 effective date. The implementation plan may not be supported until the low impact asset requirements are approved.
No comments.
Yes
Limit the applicability for dispersed generation to the point where those resources aggregate to greater than 75 MVA to a common point of interconnection at 100 kV or above and not at an individual turbine, inverter or unit level in the CIP-003-6 Applicability section similar to PRC-005. Suggested revision: Under the Introduction section, 4 Applicability, 4.2 Facilities, ***add the following statement after 4.2.2 All BES Facilities: “For dispersed power producing resources identified through Inclusion I4 of the BES definition, the only BES Cyber Systems that meet the low impact rating criterion 3.3 in Attachment 1 of CIP-002-5.1 are any shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of dispersed generation units from the point where those resources aggregate to greater than 75 MVA to a common point of connection at 100 kV or above and not at an individual turbine, inverter or unit level.” This change should be made in conjunction with adding back “for its assets identified in CIP-002-5.1 Requirement R1.3” in CIP-003-6 R2. The SAR for the CIP version 5 revisions project 2014-02 includes the following statement, “This project may also consider input that may be provided from CIP version 5 transition activities, for example from the NERC transition study or CIP Version 5 transition program.” At least one NERC transition study participant has identified the need to address dispersed generation in the CIP standards. Also, the dispersed generation project 2014-01 SAR includes the following phrase, “for standard drafting teams developing new or revised Standards, so that they do not incorrectly apply requirements to dispersed generation unless such an application is technically sound and promotes the reliable operation of the BES.” // Correct the errata in the Guidelines and Technical Basis for CIP-007-5 R2.2 in the last sentence of the second to last paragraph where it references a TFE. Technical feasibility exceptions are not included in Requirement R2.2 of CIP-007-5. // MidAmerican Energy Company supports Edison Electric Institute comments. MidAmerican Energy Company thanks the Standards Drafting Team for their technical competence, diligent work and collaboration with industry.
Individual

Michelle Clements
Wolverine Power Supply Cooperative, Inc.
Individual
Dan Gibson
Kansas City Power & Light
No
R2 – Usage of the term “external routable protocol paths” should be officially defined by NERC before being able to “judge the sufficiency” of the newly introduced controls. Assumptions a responsible entity could make surrounding this term could lead to violations. The Guidelines and Technical Basis section includes numerous references to “belief” and “intent,” along with descriptions of what entities “should” be doing. The need for such language indicates that the requirement language is not able to stand on its own and results in a need to be audited by the Guidelines and Technical Basis section. In turn, language not intended to be a required action by the entity could result in a perceived additional requirement by those trying to understand the requirement. While the intent of the “Note:” section under CIP-003-6 R2 is understood, there is no way to effectively audit for the successful and complete implementation of CIP-003-6 Table R2 – Low Impact Assets without obtaining an inventory of considered assets and of authorized users. Auditors are not able to reliably issue a judgment of the effectiveness of an internal control or of adherence to requirements without ensuring that samples are pulled from a complete population. Furthermore, entities are not able to perform the functions outlined within the R2 requirements without having lists of authorized users, both for access authentication and monitoring purposes. R2.3.2 – In part because the reference to “physical access point(s)” is not in relation to a defined Physical Security Perimeter, the requirement is actually more stringent than that of CIP-006-6 R1.4 and could require more evidence in support of compliance. An entity may need to prove an evaluation was performed resulting in the derivation of an inventory of all potential access points for all Low Impact BES Cyber Systems at Control Centers. Furthermore, diagrams may be needed to support that monitoring has been considered and defined for all applicable access points. While intended to be helpful in aggregating all Low Impact BES Cyber Systems requirements into a single section, the table has resulted in a web of functionally similar, yet separated requirements that could result in confusion. KCP&L recommends that, wherever possible, the items from CIP-003-6 Table R2 – Low Impact Assets be moved to the appropriate functional section and included as an additional applicable system where requirements are also similar. R2.4 – The requirements established under R2.4 are redundant to CIP-005-5 R1. In order to effectively audit the implementation of such controls, inventories and lists will be required just as they will be for CIP-005-5 R1. Guidelines and Technical Basis Section 2.4 – The two sentences beginning with “The electronic access controls should address…” go beyond the purview of the language of the requirement and serve to dictate what “should” be addressed. It is recommended that these sentences be stricken from the Guidelines and Technical Basis section.
No
CIP-006-6: The current order and applicability for CIP-006-6 is inconsistent and does not logically flow. At no point is a requirement for use of a defined PSP introduced, yet a number of the requirements pertain exclusively to the existence of a defined PSP. Physical Access Control Systems, as defined by the NERC Glossary of Terms, are also not stated as being required. Due to the current combined applicability and requirements, an entity could theoretically have a High Impact BES Cyber System that does not reside in a PSP and does not have a Physical Access Control System. This could result in applicability of only CIP-006-6 R1.3 and R1.10, and a lack of requirement for operational or procedural controls to restrict physical access. While the entity would still have to achieve two or more physical access controls, the requirements never state that a PACS is required for a High Impact BES Cyber System to achieve this or that a PSP is required for any system. KCP&L recommends that either CIP-006-6 R1.1 be updated to require the use of a Physical Access Control System for High Impact BES Cyber Systems or that a new sub-requirement is created to require High Impact BES Cyber Systems to have a Physical Access Control System with defined operational or procedural controls to restrict physical access. In addition, consideration should be given to rewording some monitoring, logging, and alerting requirements to include monitoring, logging, and alerting provisions for non-PSP, physically protected areas. CIP-007-6 The term “nonprogrammable communication components located inside both a PSP and an ESP” is a new source of confusion and may require definition as an official NERC Glossary term. CIP-005-5 requires only for “Cyber Assets”

to reside within an ESP. Unofficial guidance has already been communicated by various Regional Entities in support of excluding non-Cyber Asset, nonprogrammable “devices” from the required ESP. Therefore, it is difficult to identify where a “nonprogrammable communication component” that is also not a Cyber Asset would be located inside an ESP. Additionally, while CIP-006-6 defines certain protections that must be afforded to a Physical Security Perimeter, there is no requirement stating that a device must reside within a defined PSP. Therefore, entities are allowed to utilize other operational or procedural control measures for protecting High and Medium impact ESPs. Even if a “nonprogrammable communication component” is defined as part of an ESP, it is possible that the “nonprogrammable communication component” will not reside within a defined PSP. It should also be noted that the addition of such language will result in increased burden for entities by nature of a backdoor requirement for documentation of all considered “nonprogrammable communication components” that are not NERC-defined “Cyber Assets.” The current proposed language applicable only to “nonprogrammable communication components located inside both a PSP and an ESP,” along with other PSP-specific requirements, may serve to discourage entities from creating defined PSPs around BES Cyber Systems.
No
Although we agree with the overall approach the Standards Drafting Team has taken, we answered no to this question due to specific concerns described in the comments submitted by the Edison Electric Institute. While we have previously stated that additional controls are necessary in this area for security and to ensure reliability, implementation of such controls will need to occur with a view toward practicality and sustainability.
No
KCP&L believes that the definition of Transient Cyber Asset should be clear to ensure no unintended consequences from interpretations by stakeholders involved where direct connections of devices are anticipated. Physical and electronic access control to BES Cyber Systems is a critical component of securing the overall system, and such devices should be protected from inappropriate Transient Cyber Asset connections. But the definition of such lacks clarity and thus will lack consistency in application. The language around the Transient Cyber Asset and Removable media is silent and unclear where EACMS and PACS are concerned. The new definition could read as follows: Transient Cyber Asset: A Cyber Asset directly connected for 30 consecutive calendar days or less, to: (1) a BES Cyber Asset, or (2) a network within an ESP. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. Note: Clarity needed for issues identified previously.
Yes
While KCP&L supports alternative methods of assessing maturity and effectiveness in adherence to the NERC CIP requirements, the “Identify, Assess and Correct” language was an open-ended and unstructured framework that would cause confusion and lead to the expansion of the scope of NERC CIP based on auditor judgment. This concept would be addressed in tools and frameworks accomplished through the Reliability Assurance Initiative (RAI), however, consistency in auditor training and approach will be critical to the success of the RAI program.
Yes
No
We are not aware of additional jurisdictions that should be considered at this time.
Yes
KCP&L would like to endorse those comments made in this question by the Edison Electric Institute.
Individual
Kalem Long
The Empire District Electric Company
No
Parts 2.2 through 2.6 all require us to "implement one or more documented processes that..." However, the measures are about the documentation of operational controls, and nothing to prove implementation. There is an inconsistency between the requirement and what will be needed to show compliance to the requirement.

No
Though the intent is appreciated, CIP-006 Part 1.10 adds ambiguity with the verbiage "an equally effective logical protection." An entity may believe that they are compliant with full evidence, but this may not meet what auditor believes is "equally effective."
Yes
No
EDE agrees with EEI's comments: "There is a consistency issue. The definition for Transient Cyber Assets is very specific about what Transient Cyber Assets are directly connected to; however, the definition for Removable Media is not. It can be implied that the definition refers to connection to applicable systems, but it is not clear. It would also be clearer to switch the order of the Removable Media and Cyber Assets in the last sentence. {Suggested Revision} Change the definition of Removable Media to: “Portable media, connected for 30 consecutive calendar days or less, to applicable systems. Examples of portable media that can be used to copy, move and/or access data include, include but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. Removable Media are not Cyber Assets.”
Yes
Though Empire votes to approve the removal of IAC, we agree with SPP that "We do appreciate the clarity that removing the IAC language will provide. There is a concern that we are being asked to approve standards based on a program that is currently under development. By the time that a Responsible Entity will see how RAI is applied in audit situations, these standards, with the IAC language removed, will long have been voted upon."
Yes
No
No