Individual or group. (70 Responses)
Name (51 Responses)
Organization (51 Responses)
Group Name (19 Responses)
Lead Contact (19 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (15 Responses)
Entity's Name: (70 Responses)
Question 1 (51 Responses)
Question 1 Comments (55 Responses)
Question 2 (48 Responses)
Question 2 Comments (56 Responses)
Question 3 (50 Responses)
Question 3 Comments (56 Responses)
Question 4 (48 Responses)
Question 4 Comments (56 Responses)
Question 5 (47 Responses)
Question 5 Comments (56 Responses)
Question 6 (50 Responses)
Question 6 Comments (56 Responses)
Question 7 (46 Responses)
Question 7 Comments (56 Responses)

Group
Tennessee Valley Authority
Brian Millard
No
1. CIP-003-6 R2 - The Registered Entity (RE) appreciates the work of the SDT; however, the RE objects to the requirement in CIP-003-6 to develop cyber security plans for Low Impact assets. Creation of cyber security plans for Low Impact assets adds nothing in terms of increased reliability and should therefore be eliminated. The SDT should consider incorporating the policy requirements applicable to Low Impact assets into the appropriate existing standards. Any requirements associated with cyber security awareness for Low Impact systems should be written into CIP-004. Any physical access control requirements for Low Impact systems should be written into CIP-006. Any electronic access control requirements for Low Impact systems should be written in CIP-005. Any Cyber Security Incident Response requirements for Low Impact systems should be incorporated into CIP-008. Moving the required policy into the appropriate standard more effectively addresses the directive to address Low Impact assets. Placing security controls for remote access, physical security, incident response, and cyber security awareness into a standard governing security management is both confusing and

inconsistent with the existing standards framework. 2. CIP-003-6 R2 VSL - The SDT should consider the VSL associated with CIP-003 R1 and R2 in context. Failure to document or implement a security plan for a Low Impact system inherently poses less risk than for Medium or High Impact systems, yet the VSL rating for both is Severe. The VSL for Low Impact systems should be lower than for High or Medium Impact systems. 3. CIP-003-6 Attachment 1 - The requirements in the security plan belong in the requirements section of the standard, not as an attachment, as noted in comment #1 above. Element 2 addresses physical access controls for the Low Impact BES Cyber System Electronic Access Point (LEAP). LEAPs are not required to be established until September 1, 2018 per Element 3. As written, however, the requirement to physically protect LEAPs would begin five months before they are established. Element 3.1 , Electronic Access Controls states: “For any Low Impact External Routable Connectivity, establish a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all other access.” The RE is concerned that without specific language to clarify or limit the applicable scope, the establishment of a LEAP would assume the establishment of an ESP, which may inappropriately subject those systems to CIP-005-6 R1. Similarly, establishing controls to permit “only necessary inbound and outbound access and denies all other access” may inappropriately bring CIP-007-6 R1 in to scope. Attachment 2 of Element 3 states that documentation may include “inbound and outbound connections (e.g. IP addresses, ports, services) for any Low Impact BES Cyber System Electronic Access Point are confined to only those the Responsible Entity deems necessary”. This is essentially a restatement of the “Measures” in CIP-007-X R1, which implies this requirement is in scope as well. The RE suggests the SDT revise the Attachment 1 and Attachment 2 language to clearly delineate the respective scope for Low Impact systems versus Medium and High Impact systems. 4. CIP-003-6 Attachment 2 - Attachment 2 does not offer much clarity beyond what is already documented in Attachment 1. The RE suggests that example evidence be documented in a table format similar to that used in CIP-004 -CIP-011 and provide supplemental guidance regarding the type(s) of evidence that would document compliance with the standard. 5. CIP-003-6 Guidelines and Technical basis - The guidance for R2 states “Using the list of assets from CIP-002, the intent of the requirement is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the protections of all low impact BES Cyber Systems.” This guidance is in direct contradiction with CIP-002-5 R1.3 which states a discrete list of Low Impact BES Cyber Systems is not required. The SDT should consider whether a Low Impact system list should be generated as a result of the requirements in CIP-002-5, or revise the guidance in CIP-003-6 R2 to remove language that is contingent upon a Low Impact system list.
No
1. Low Impact External Routable Connectivity (LERC) Definition - Because LERC is communication between Low Impact BES Cyber Systems and Cyber Assets outside the asset, it would not include communication that is routed through a non-BES Cyber Asset such as a historian or jump host located in a DMZ. In those cases, a BES Cyber System would not be communicating outside the asset. The RE suggests the SDT clarify that the intent is to exclude this type of communication. 2. Low Impact BES Cyber System Electronic Access Point (LEAP)

Definition - The term “allows” in the definition is too broad and could inappropriately include assets such as switches, hubs, or other transport devices. The RE suggests using the term “controls” or “restricts” instead.
No
1. Guidelines and Technical Basis - Requirement 4 Attachment 1 Removable Media Page 43 states the following: “Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.” The statement that “…user(s) must have authorized electronic access to the applicable system…” is not a CIP requirement and should not be included in the Guidelines and Technical Basis section of the document. Additionally, it is not necessary that a user of an authorized removable media device have electronic access to the applicable system. An individual with physical access to a system could be connecting removable media for someone with electronic access but working remotely. 2. CIP-010-6 R4 and Attachment 1 - The required elements and R4 refer to “documented plan(s) for Transient Cyber Assets and Removable Media”. Neither requirement 4, the three pages of Attachment 1 “Required Elements for Plans”, Attachment 2, nor the CIP-010-2 Definitions include a clear definition for what constitutes a “plan”. Certain sections indicate that policies could suffice, but in other sections it only requires “documentation” and seems to purposefully leave out “policies”. The language as written may intend to allow entities flexibility for how a “plan” is documented, but may have the unintended consequence of deferring to the judgment of the auditor to determine what level of “documentation” constitutes a “plan”. The RE suggests the SDT clarify the requirement that a ”plan” can be any type of documentation defined by the RE that meets the “Required Elements for Plans for Transient Cyber Assets and Removable Media” in Attachment 1.
Yes
Yes
Yes
No
Group
Northeast Power Coordinating Council
Guy Zito
No
Request clarification on where the dividing line is between Element 4 (Cyber Security Incident Response) and EOP-004. The Element references in Attachment 2 should match the Elements in Attachment 1, otherwise industry could draw incorrect conclusions. Recommend adding

“As needed” to the beginning of Attachment 1 4.7 because not every incident/test needs an updated Incident Response Plan.
No
Recommend removal of “and controls” from the Technical Guidance on Low Impact Cyber System Electronic Access Point (LEAP) to be consistent with the Definition of LEAP. Currently, the LEAP Technical Guidance says “is the interface on a Cyber Asset that allows and controls the LERC,” while the LEAP Definition says “A Cyber Asset interface that allows the Low Impact External Routable Connectivity.”
No
For clarity, suggest revising Attachment 1 2.1 from “each Responsible Entity shall use one or a combination of the following methods: ” to “each Responsible Entity shall use at least one or a combination of the following methods: ” For clarity, suggest revising Attachment 1 2.2 from “each Responsible Entity shall use one or a combination of the following methods:” to “each Responsible Entity shall use at least one or a combination of the following methods:” As written, Attachment 2.3 requires each Entity to review each vendor’s policies/procedures. This may be too burdensome for the industry. Suggest a different solution is needed. Recommend changing from “Responsible Entities shall determine whether additional mitigation actions are necessary ” to “Responsible Entities may determine whether additional mitigation actions are necessary ” Attachment 1 1.2 covers Transient Cyber Asset authorization, however there is no corresponding part for vendor/contractor authorization. Suggest adding a part for Responsible Entity authorization of vendor/contractor use of Transient Cyber Assets.
No
Based on the new definitions, it is unclear on whether a cyber asset can be classified as multiple asset types and would therefore be subject to multiple levels of requirements, i.e. a BES Cyber Asset or a Protected Cyber Asset can also be a Transient Cyber Asset. If a BES Cyber Asset or a PCA also meets the definition of Transient Cyber Asset, there is nothing in the language that says one classification supersedes or precludes another. Solely based on the definitions, it would appear that an entity would have to classify an asset by all the definitions that apply. Recommendations: • Add the following sentence to definition of Transient Cyber Asset: "A Cyber Asset that meets the definition of BES Cyber Asset shall not be considered a Transient Cyber Asset." • Add a minimum requirement to the PCA definition. “If a PCA is connected for less than 30 days then it is a TCA and more than 30 days it is a PCA.”
Yes
Yes
Yes
To avoid industry confusion, recommend changing “elements” to another label such as “plan elements” or “items.” Recommend quality assurance review before future postings, to avoid reviewers’ confusion or need to decipher how to connect related information.

Group
Colroado Springs Utilities
Shannon Fair
Agree
CSU agrees with the changes to CIP-003-6, R2 including the use of Attachment. CSU recommends the following edit to Attachment 1: “Each Responsible Entity shall reinforce, at least once every 15 calendar months” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle.
Yes
CSU supports the new definitions for Low Impact External Routable Connectivity and Low Impact BES Cyber Systems Electronic Access Point.
Yes
CSU agrees and supports the changes that were made to CIP-010-2, R4.
Yes
CSU agrees with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. Since “Media” is itself not a defined term, CSU recommends either defining “Media” or not capitalizing the term.
Yes
CSU agrees and supports the proposed implementation plan deadlines for CIP-003-6, R2.
Yes
CSU supports the removal of the IAC language from the 17 requirements based on the FERC directive.
No
Individual
Steve Hamburg
Encari
Yes
No
The LERC definition requires clarification as to the external connectivity that is the focus of the definition. Suggest that "outside the network" replace "outside the asset." The definition should read: Low Impact External Routable Connectivity (LERC): Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the network containing those low impact BES Cyber System(s). Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

Yes
No
It remains unclear as to whether a Transient Cyber Asset can also be considered as a BES Cyber Asset. If the intent is to exclude Transient Cyber Assets from the classification of BES Cyber Assets, the definition of Transient Cyber Asset should expressly state, "Transient Cyber Asset: A Cyber Asset, (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) directly connected for 30 consecutive calendar days or less, capable of transmitting executable code 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 Cyber Asset meeting the definition of a Transient Cyber Asset may be excluded from classification as a BES Cyber Asset."
Yes
Yes
Yes
The definition of BES Cyber Asset has been modified to remove the exclusion of Transient Cyber Assets. This creates confusion as to whether a Transient Cyber Asset may still be considered a BES Cyber Asset since the definition of Transient Cyber Asset does not indicate whether a Transient Cyber Asset may be excluded from the classification of a BES Cyber Asset.
Individual
Alshare Hughes
Luminant Generation Company, LLC
Yes
We recommend the revisions below to improve or clarify the current draft language. 1) Attachment 1, Element 2 – Recommend removal of “Based on need” qualifier that renders requirement to “restrict physical access” more stringent that comparable requirement for Medium Impact BES Cyber Systems without External Routable Connectivity (CIP-006 R1.1). Also recommend removal of “based on need” language in corresponding Attachment 2, Element 2, Item 2. 2) Attachment 2, Element 4 – The requirements include identification, classification and response in 4.1 and incident handling in 4.4. There appears to be an overlap and redundancy with these terms. Recommend revision to 4.1 to “Identification and response to …”. 3) Attachment 1, Element 4.7 – The current language unconditionally mandates the updating of the incident response plan regardless of need. Recommend revision to: "Updating the Cyber Security Incident response plan, if necessary as determined by the Responsible Entity, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident. If no updates are deemed necessary, this decision should be recorded within 180 days." Also recommend revision of language in

corresponding Attachment 2, Element 4, last paragraph. 4) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – The last sentence discussing LERC is not clear. Recommend revision to The SDT intends that IED to IED communications be exempt from any requirement to use an electronic access point, even if there is Low Impact External Routable Connectivity. Through this exemption, the SDT intends to not preclude the use of time-sensitive reliability enhancing data exchanges.” 5) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – In language describing LEAP, recommend replacing "internal interface" with "an interface" and dropping the "facing the low impact BES Cyber System" language. Well-intentioned but may confuse implementers 6) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – Sentence “However the LERC between assets,… must also pass through the single LEAP” should be revised to say, “…must also pass through a LEAP.” 7) Guidelines and Technical Basis, Discussion of R2, Attachment 1, LEAP discussion – Delete “physically” from “unidirectional gateway that physically enforces outbound-only data flows”. Change “LEAP are not to be considered EACMS…” to “A LEAP is not to be considered an EACMS…”. Change “However they are required” to “However it is required”. Delete last sentence (“It is also not the intent of the SDT…” or change to: “A LEAP is not required for any BES Asset where there are low impact BES Cyber Systems but no LERC". 8) Guidelines and Technical Basis, Discussion of R2, Attachment 1, Electronic Access Controls discussion – Within the first main section on page 34 beginning with “The electronic access controls…”, recommend replacing “shall” with “should” in the second sentence. This would be more appropriate language for guidance. 9) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – in the diagram for Reference Model 2, change “an LEAP” to “a LEAP”. 10) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – Cyber Security Incident Response, first paragraph – “For assets that do not have LERC…” raises the question of whether the assets that do have LERC should have “real time monitoring.” There is no monitoring requirement in R2 so this sentence should be deleted. 11) Guidelines and Technical Basis, Discussion of R2, Attachment 1 – Cyber Security Incident Response, second paragraph – per previous comments update to plan(s) within 180 days of a test or an actual incident should only be required if the Responsible Entity determines revisions to the plan are necessary.
Yes
Yes
We recommend the revisions below to improve or clarify the current draft language. 1) Attachment 1, Element 1.3 – “Live operating system and software executable only from read-only media” is not sufficiently clear. Suggested revision: “Use of operating system software and other required executables installed from read-only media.” 2) Attachment 1, Element 1.4 – Suggest revision of element title to “Malicious code prevention or mitigation” AND begin first sentence with “To prevent or, if necessary, mitigate the introduction of malicious code,…” 3) Attachment 1, Element 1.5 – Suggested revision of element title to “Unauthorized use prevention or mitigation” AND begin first sentence with “To prevent or, if necessary, mitigate the impact of unauthorized use,…” 4) Attachment 1, Element 2.2 – Suggested revision of “…live operating system and software executable only from read-only media” to ”…operating system software and other required executables installed from read-only media”

to add clarity. 5) Attachment 2, Evidence for Element 1.3, 1.4, 1.5, 2.1, 2.2 – Suggest deletion of last sentence in each of these statements as the current language introduces a loophole. The requirements in Attachment 1 are written to provide flexibility to “do A, or B, or C, or something else to mitigate risks” so there should be no circumstance under which an entity can assert it is not possible to do anything to mitigate the security risks. 6) Guidelines and Technical Basis, Discussion of Element 1.4 and 3.2 – The last sentence should be deleted. The statement “Entities should also consider whether the detected malicious code is a Cyber Security Incident” suggests a requirement that is not included in any “R” statement in the draft language. 7) Guidelines and Technical Basis, Discussion of Element 1.5, first bullet – Suggested revision of “…Physical Security Perimeter or other physical location that manages unauthorized physical access…” to “…Physical Security Perimeter or other physical location that manages physical access…”. 8) Guidelines and Technical Basis, Discussion of Element 1.5, second bullet – Disk encryption will not protect a Transient Cyber Asset from unauthorized physical access. Suggested revision: “Full disk encryption with authentication is an option that can be used to mitigate the risks associated with unauthorized physical access to a Transient Cyber Asset.”
Yes
Yes
Yes
Individual
Thomas Haire
Rutherford EMC
No
No
No
No
Yes
No
The IAC language provided more proactive results based approach to truly identify, assess, and correct problems rather than follow standards.

No
Individual
Dan Bamber
ATCO Electric
Yes
Yes
Yes
No
ATCO Electric Transmission requests further clarification on the Removable Media definition. In the scenario where a USB stick (removable media) is connected to a laptop (transient cyber asset) would these two items, together, be considered removable media or a transient device?
Yes
Yes
No
Individual
Dan Roethemeyer
Dynegy
No
For physical access controls, the draft reads that physical access be restricted 2 ways (1) the asset or location..... and (2) the Low EAP. I don't understand why it has to be both. Suggest changing the "and" to an "or". Also, if (2) is required, that would seemingly require an asset inventory list which is not required for Low impact assets.

Individual
Heather Laws
PNM Resources, Inc
Agree
EEI
Individual
Mike Marshall
Idaho Power
No
The main issue is with section 3 of Attachment 1. There has been no good explanation given for how this requirement will be audited without providing a list of Low Impact BES Cyber Systems which contradicts the wording of CIP-002. Additionally, the "Rationale for Requirement R2" states that "there continues to be no compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber Systems." Yet the entities are to identify (without maintaining a list) all of the Low Impact Cyber Systems that require these electronic access controls. It seems that the v5 standards need to settle into some level of stability and then address further security concerns such as the ones addressed in section 3 of the Attachment 1 in a later version or at the very least revise the wording to be more clear with what will be required, how it will be approached, and how it will not be in conflict with other CIP standards.
Yes
Yes
Yes
No
The time frames still do not provide enough time for entities to adjust to and increase of scope of this magnitude.
Yes
No
Individual
Debra Horvath
Portland General Electric
Agree
Edison Electric Institute

Individual
John Brockhan
CenterPoint Energy Houston Electric LLC.
No
Attachment 1, Element 4.7 - CenterPoint Energy agrees with EEI’s comment. Element 4.7 implies that the Cyber Security Incident response plan should be updated within 180 calendar days after completion of a Cyber Security Incident response plan(s) or actual Reportable Cyber Security Incident. However, this may not always be the case. CenterPoint Energy recommends adding the words “, if needed” after “180 calendar days.”
No
CenterPoint Energy generally agrees with requirement R4 and the documentation of a plan to address Transient Cyber Assets and Removable Media. As written in the Guidelines and Technical Basis for R4 Attachment 1, Elements 2.1, 2.2, and 2.3, the requirement allows entities the ability to review the assets to the best of their capability and meet their obligations. Additionally, entities are to document and implement their procedures to mitigate security vulnerabilities and malicious code. In Attachment 1 under Element 2.3, CenterPoint Energy believes that the Responsible Entity should determine the frequency of mitigation actions for Transient Cyber Assets owned or managed by vendors or contractors as noted in the documented plan required in R4. As it is currently written, it can be interpreted as requiring Responsible Entities to perform mitigation methods stated in Elements 2.1, 2.2, and 2.3 each time the vendor or contractor-owned device is connected to a BES Cyber System. This would be operationally inefficient if the vendor is connecting to multiple BES Cyber Systems consecutively within the trusted environment. For example, if a vendor is updating firmware at multiple substations, the Responsible Entity may scan/review the vendor-owned Transient Cyber Asset for security patches and antivirus once, prior to connecting to the first BES Cyber System. The review would be valid and effective for the duration of the firmware update at multiple substations as long as the Transient Cyber Asset is not connected to an unsafe/untrusted environment and is used within the protected environment. CenterPoint Energy recommends adding clarification to the Guidelines and Technical Basis under “Requirement 4 Attachment 1 Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors” for Elements 2.1, 2.2, and 2.3. CenterPoint Energy suggests the following wording to be added to Elements 2.1, 2.2, and 2.3, “prior to connecting their devices to the applicable systems within the trusted environment.” Attachment 1, Element 3.2 - CenterPoint Energy agrees with EEI’s comment. This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 does not allow for these options. Also, Element 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. CenterPoint Energy recommends changing “scan Removable Media outside of the BES Cyber System” to “use a method to scan

Removable Media for malicious code and a procedure to respond to detected malicious code.”
Yes
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).
Individual
Jo-Anne Ross
Manitoba Hydro
Yes
Yes
Yes
Yes
Yes
Yes
No
Group
Dominion
Greg Dodson
No
1. The R2 Attachment 1 Element 2 and Attachment 2 Element 2 Part 2 that describe authorization “based on need” for physical security controls is problematic and should be removed. The concept appears to be the same as used in CIP-004 R4.1 where you should have some justification of the business need for authorization of electronic and unescorted physical

access and access to BES Cyber System Information, the SDT used it in a different context in CIP-003-6. However, the guidance states, “The requirement does not imply that a specific business need must be documented for each access or authorization of a user for access. The SDT intent is that this need at the higher level be documented such that the requirement cannot be interpreted to mean that any and all access must be restricted. The requirement does not imply that a specific business need must be documented for each access or authorization of a user for access.” A policy level document that requires no action is merely an administrative burden that doesn’t meet the minimum elements of a properly developed Standard. The clause “based on need as determined by the Responsible Entity” should be removed from [Element] 2. Physical access controls in CIP-003-6 – Attachment 1, and item 2 of Element 2 in CIP-003-6 – Attachment 2 should also be removed. 2. The guidance associated with R2 (page 31 of 37 in the clean version) states, “The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do meet the definition of having a 15-minute adverse impact so some protections are needed.” This guidance is should be reworded for clarity as follows: “The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they dostill meet the definition of having a 15-minute adverse impact so some protections are needed.” As stated, the wording creates confusion between “low impact” and “no impact”. 3. The guidance associated with R2 Attachment 1 (page 33 of 37 in the clean version) states “Low Impact BES Cyber System Electronic Access Point (LEAP) – is the interface on a Cyber Asset that allows and controls the LERC.” This language doesn’t match the definition. The sentence should be changed to, “Low Impact BES Cyber System Electronic Access Point (LEAP) – A Cyber Asset interface that allows Low Impact External Routable Connectivity.” 4. Element references in Attachment 2 should match the Elements in Attachment 1, otherwise industry could draw incorrect conclusions. 5. By not placing like requirements throughout the standards, there’s an opportunity to violate more than one requirement. For example, with Cyber Security Awareness and Incident Response, if a facility has all impact levels and a Cyber Security Incident occurs, there’s the potential to violate both CIP-008-5 and CIP-003-6. 6. Requirement [part, element] 4.7 in CIP-003-6 – Attachment 1 assumes that the incident response plan will require an update, which may be an incorrect assumption. The phrase, “as required” should be appended to 4.7. 7. CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation: Change Subpart 1.2.2 to “Physical access controls.” 8. CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation: Add “, if needed,” after “180 calendar days.” 9. CIP-003-6 Attachment 2 and Guidelines and Technical Basis for element 2: Attachment 2 (examples of evidence) for element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for element 2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation: Include “perimeter controls” under element 2, Attachment 2 in the example: “(e.g., card key, special locks, perimeter controls).
No

1. In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation: Clarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to allow for point-to-point communications (e.g., over fiber) to use routable communication protocols for time sensitive protection and/or control functions.
No
1. For clarity, suggest changing 2.1 from “each Responsible Entity shall use one or a combination of the following methods:” to “each Responsible Entity shall use at least one or a combination of the following methods:” 2. For clarity, suggest changing 2.2 from “each Responsible Entity shall use one or a combination of the following methods:” to “each Responsible Entity shall use at least one or a combination of the following methods:” The phrase “(per Transient Cyber Asset capability)” should be added to 1.5 and 2.2 as is insinuated in the guidance (“If a Transient Cyber Asset is unable to perform…”). 3. CIP-010-2 Attachment 1: The use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is unnecessary and implies a second step such as approval of who can use the TCA, where, and how, which is unclear – the plan should identify the users, locations, and uses of the TCA. Recommendation: Remove “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. 4. CIP-010-2 Requirement R4 ends with “include the elements in Attachment 1”, although the first sentence in Element 1 says “include each of the element provided below” the actual “elements” are not labeled “elements” as in Attachment 2, which references the elements in Attachment 1. Recommendation: Add “Element” before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses.
Yes
Yes
Yes
No
Individual
Joe O'Brien on behalf of Jerry Freese
NIPSCO
These commments are copied from an EEI Draft which we support. If EEI has submitted comments than these may be redundant. Thanks
No
Comment 1.1: CIP-003-6 Rationale for Requirement R2: “Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised.” Aggregating low impact BES Cyber Systems across multiple assets does not reflect a true risk-based assessment and therefore this sentence is

not accurate. Recommendation: Delete this sentence. Focuses on Rationale, not requirement Comment 1.2: CIP-003-6 – Attachment 1: The language in Element 1 “using one or a combination of the following” is inconsistent with the Element 2 language “through one or more of the following.” Recommendation: Change the language in Element 1 to “through one or more of the following.” Minor wording issue Comment 1.3: CIP-003-6 – Attachment 1: CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation: Change Attachment 1, Element 2 to “Physical security controls” to be consistent with the language of the standard. Please edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs) to CIP-003-6 R1 are consistent. Comment 1.4: CIP-003-6 Requirement R2 ends with “include the elements in Attachment 1”, although the first sentence in Element 1 says “include each of the elements provided below” the actual “elements” are not labelled “elements” as in Attachment 2, which references the elements in Attachment 1. Minor format issue. Recommendation: Add “Element” before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses. This would also be helpful for Attachment 1 in CIP-010-2. Comment 1.5: The “(LERC)” and “(LEAP)” acronyms are missing in Element 2, 3, and 3.1, which makes it harder to identify the use defined phrases in these elements. Recommendation: Add the “(LERC)” and “(LEAP)” to elements 2, 3, and 3.1 to make it easier to identify the acronym. Minor format issue Comment 1.6: CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation: Add “, if needed,” after “180 calendar days.” Point of clarification; valid Comment 1.7: CIP-003-6 Attachment 2 and Guidelines and Technical Basis for Element 2: Attachment 2 (examples of evidence) for Element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for Element 2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation: Include “perimeter controls” under Element 2, Attachment 2 in the example: “(e.g., card key, special locks, perimeter controls). Valid inconsistencies; Comment 1.8: CIP-003-6 Guidelines and Technical Basis, Requirement R2 Attachment 1 bold text subtitles on page 32: The subtitles are inconsistent with the element language in Attachment 1. Recommendation: Change the subtitle language to “Requirement R2 Attachment 1 – Cyber Security Awareness” and “Requirement R2 Attachment 1 – Physical Security Controls” (see Comment 1.2 above). Valid point of clarification
No
Comment 2.1: Use of “allows” in the LEAP definition does not allow for the use of an unmanaged hub. An unmanaged hub, which does not support access controls and may be merely acting as a central connecting point, could be considered an interface that “allows” Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs. Recommendation: Change “allows” to “controls” to allow for the use of unmanaged hubs as appropriate. Please also make sure this is changed in the Guidelines and Technical Basis and anywhere else the LEAP

definition is provided. Valid definition modification Comment 2.2: Because the acronyms LEAP and LERC are used to help simplify the terms defined and used in the standard, it would help to include the acronyms each time the terms are spelled out in full in the definitions and in the standards and related guidance. Recommendation: Insert the acronyms "(LERC)" and "(LEAP)" as they are spelled out in the definitions. Minor format issue Comment 2.3: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation: Change the exclusion sentence to: "Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols)." Alternatively, Cclarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to include point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions. Valid point of clarification Comment 2.4: The definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation: In the Guidelines and Technical Basis for CIP-003-6, where LEAP is described, move the sentence "LEAP are not to be considered EACMS…" to create a second paragraph and add "However a LEAP can be implement within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself." Valid point of clarification Comment 2.5: LERC definition or CIP-003-6 Guidelines and Technical Basis for Requirement R2 Attachment 1 – Electronic Access Controls: The following scenario is unclear: {Low impact BES Cyber System (e.g., control system) ---- |1| ---- Cyber Asset (e.g., data historian) ---- |2|} ---- Location X Where: {} represents the asset/site boundary, |1| represents a firewall or electronic access point (in this case firewall 1), and ---- represents a bi-directional routable communication Based on the language of the definition and CIP-003-6 it is unclear whether there is a LERC and LEAP in this scenario and if there is LERC, which firewall is the LEAP. The Guidelines and Technical Basis for CIP-003-6 say "the electronic access controls should address the risk of using the asset's LERC to gain access to the low impact BES Cyber Systems." However, this scenario would require an adversary to gain access to not one but of two access points, – the firewalls on either side of the Cyber Asset (firewall 2 and then firewall 1) to get access to the low impact BES Cyber System. Whereas, the examples provided all show one access point, the LEAP, which requires controls. Recommendation: Add this scenario to the CIP-003-6 Guidelines and Technical Basis, Responsible Entity to have the flexibility choose the LEAP, either firewall 1 or firewall 2. Valid point of clarification
No
Comment 3.1: CIP-010-2 R4: The placement of "under CIP Exceptional Circumstances," is awkward. Recommendation: Move "under CIP Exceptional Circumstances" up in the

sentence, such that it reads “…shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s)…” Minor format issue Comment 3.2: CIP-010-2 Attachment 1: The use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and 2 it is implied by the language of 1.2 and 1.3. The language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization for the Transient Cyber Asset. The redundancy creates uncertainty in the interpretation of the standard. It could be interpreted to imply a second step in addition to the R4 plan. In other words, in addition to the R4 plan for Transient Cyber Assets and Removable Media, which includes the 1.2 and 3.1 authorization elements, the Responsible Entity must also have a separate, formal approval process plan to identify authorized users, authorized locations, and authorized uses for Transient Cyber Assets and a separate formal approval process to identify who is authorized to use and where they are authorized to use Removable Media. We believe the intent of the Standards Drafting Team is that the plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address thesee authorization elements. This flexibility will allow the Responsible Entity to either write a plan that specifically defines who is authorized to use the Transient Cyber Asset(s) for which uses and locations or include a separate authorization process, which may include a formal approval process, in the plan that identifies the users, locations, and uses authorized for the Transient Cyber Asset(s). It will also give the Responsible Entity the same flexibility for Removable Media authorizations. This flexibility is particularly needed for Responsible Entities that rely on contractor use of Responsible Entity managed Transient Cyber Assets and Removable Media who have less control over the contractor, i.e., the control is defined by a service agreement or contract. Giving the Responsible Entity flexibility on how to define the authorization process will allow them to align these requirements with their vendor contracts. Recommendation: Remove “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. Alternatively, clarify in the Guidelines and Technical Basis under Element 1.2 and 3.1 that the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 does not require a formal approval process for each user, location, and use of the Transient Cyber Asset (or Removable Media), but gives the Responsible Entity the flexibility to develop an authorization plan that either directly defines authorization or requires a specific authorization process. This allows Responsible Entities to align their Transient Cyber Asset and Removable Media authorizations with their vendor contracts for use of Responsible Entity managed Transient Cyber Assets. Valid point of clarification Comment 3.3: CIP-010-2- Attachment 1 Elements 1 and 2 are grouped by whether a Transient Cyber Asset is owned or managed by the Responsible Entity or by a vendor or contractor. The intent of this grouping is good because it considers the level of control by the Responsible Entity. However, the actual groupings could result in a Transient Cyber Asset that falls under both element 1 and 2. For example, if a Responsible Entity owns the Transient Cyber Asset, but a contractor manages its use under a service management contract. Another scenario is that the vendor owns the Transient Cyber Asset, but the Responsible Entity manages it. For these scenarios, it is unclear whether the Responsible Entity should include element 1 or 2 or both elements in their R4 plan(s). Recommendation: Remove “Owned or” from elements 1 and 2. Comment 3.4: CIP-010-2 - Attachment 1, Element 2.3: “Responsible Entities shall determine whether additional mitigation actions are necessary…” requires a statement that says no additional mitigation measures were identified as necessary, which creates an unnecessary administrative burden. Also, Element 2.3 is an element that should be addressed by the R4 plan for Transient Cyber Assets and Removable Media, the way Element 2.3 is written makes it look like a requirement rather than a plan element, which also causes confusion as to the frequency of review for elements 2.1 and 2.2. Element 2.3 as written suggests that a Responsible Entity must use the 2.3 and 2.4 mitigation methods prior to each connection of a vendor-owned Transient Cyber Asset in order to determine whether additional mitigation measures will be needed. This can be overly burdensome and unnecessary when a vendor is moving from system to system in a single day. Also, a Transient Cyber Asset may be owned by the Responsible Entity and managed by a vendor or owned by the vendor/contractor and managed by the Responsible Entity. The use of “vendor- or contractor-owned” in 2.3 is not consistent with these scenarios (see comment 3.3 above).We recommend restructuring Element 2.3 to make it clear that this – determining whether additional mitigations are needed before the vendor-owned Transient Cyber Asset is connected – is an element of the plan that should be addressed to manage the associated risk and not that elements 2.1, 2.2, and 2.3 need to be used prior to each connection. Recommendation: Change Element 2.3 to:Add “necessary” before “such actions.” Also, clarify in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how to manage vulnerability and malicious code reviews of their vendors or contractors and require additional mitigation actions. For example, one entity may require a vendor to plug a Transient Cyber Asset into a kiosk to scan for vulnerabilities and malicious code before each connection. However, this approach may not be feasible for all entities, so defining a process to initially and periodically check and audit vendor/contractor processes for vulnerability and malicious code mitigation. Specifically, “prior to connecting the vendor- or contactor-owned Transient Cyber Asset” does not require that 2.1, 2.2, and 2.3 before each connection, but that the Responsible Entity should define a process to manage the use of vendor- or contractor- managed Transient Cyber Assets to mitigate vulnerabilities and malicious code. Also, change “owned” in 2.3 to “managed.” Comment 3.5: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped. Recommendation: Make it clear in the Guidelines and Technical Basis that “mitigate” and “mitigation” does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system that the Transient Cyber Asset or Removabl ???e Media is used on. Also, it may be impossible to detect every piece of malicious code. Mitigation is meant to reduce security risks, but elimination of all risk is impossible. Comment 3.6: CIP-010-2 – Attachment 2, Element 3.2: This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the

Responsible Entity to take any action other than scanning Removable Media at some point in time. Recommendation: Change “scan Removable Media outside of the BES Cyber System” to “use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code.” Comment 3.7: CIP-010-2 – Attachment 2, Element 1.2: The second sentence under Element 1.2 is a restatement of Attachment 1, Element 1.2 and is not an example of evidence. Recommendation: Remove the second sentence under Attachment 2, Element 1.2: “The documentation must…” to keep the text in Attachment 2 focused on examples of evidence and not include requirements. Comment 3.8: Guidelines and Technical Basis for R4, Attachment 1, Element 1.1: inventories of Transient Cyber Assets is allowed by individual or group – individually or by asset type, therefore language under Element 1.1 should be consistent, allowing inventory of devices or device type. Recommendation: Add “or device types” to the second sentence: “pre-authorize and inventory of devices or device types or authorize devices or device types at the time of connection or use a combination of these methods.”
No
Comment 4.1: Transient Cyber Asset Definition: The “and” in the parenthesis after “A Cyber Asset,” is confusing. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. Also, the parenthetical for the examples is misplaced; it refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, “directly connected” may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Recommendation: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) 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.” Also, if the intent is for the Transient Cyber Asset definition to apply to both routable and non-routable communications, clarify this in the Guidelines and Technical Basis for CIP-010-2.
No
Comment 5.1: CIP-003-6, Attachment 1, Element 2 compliance date of April 1, 2018: According to the Implementation Plan, the Element 2 physical access controls must be applied to LEAPs by April 1, 2018; however, the LEAPs are not identified under Element 3, which must be applied by until September 1, 2018. Recommendation: Change the compliance date for Element 2 to September 1, 2018 to allow time for the LEAPs to be identified under Element 3 and the physical access controls to be applied to them under Element 2. Alternatively, leave the compliance date for physical access controls to “the asset or the locations of the low

impact BES Cyber Systems within the asset” as April 1, 2018 and change the compliance date for requiring physical access controls to the LEAPs to September 1, 2018.
No
Comment 6.1: CIP-011-2 R1/CIP-011-X: Information protection item CIP-003-4, R4.3 allowed for annual assessment of adherence to the BES Cyber System information protection program and development of an action plan to remediate any identified deficiencies. This language provides a risk management approach: identifying the information that needs to be protected, implementing procedures to protect that information, and annually assessing adherence to that policy and incorporating lessons learned. Without the R4.3 language, any violation of the procedure will result in a Severe violation of the requirement and under the Violation Severity Level table for R1. Only a Severe level is listed for if plan is not documented or implemented, therefore if the plan is documented and partially implemented (i.e., deficiencies are found), then it is a Severe VSL. Recommendation: Add a part 1.3 to R1 to address this concern: “The Responsible Entity shall, at least annually, assess adherence to its procedures for protecting and securely handling BES Cyber System Information, including identification, protection, and handling; document the assessment results; and implement an action plan to remediate deficiencies identified during the assessment.” Adjust the Violation Severity Level table for R1 accordingly. Also, change the language of the existing Severe VSL to tier possible violations into lower levels commensurate with the risk.
No
Individual
Leonard Kula
Independent Electricity System Operator
No
We disagree with the revised structure of CIP-003-6. The concept of using tables to articulate the requirements is effective in all other standards and should be equally effective in CIP-003-6. The proposed structure introduces inconsistency of structure which is confusing. Attachments should not be used to articulate requirements. Attachment 1 is a list of requirements and should be treated as such within the main body of the standard. Attachments should only be used for guidance or informational items, not requirements that must be complied with.
No
The definition for LERC states that "Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s)." We suggest that the statement should include both BES Cyber Systems and BES Cyber Assets as LERC should apply to both systems and assets and should read: Bi-directional routable communications between low impact BES Cyber Asset(s)/BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s)/BES Cyber Asset(s).

No
We disagree with the structure approach to address transient cyber assets in a separate requirement as it leads to inconsistent approaches between BES Cyber Systems/Assets and transient assets. We suggest that it would be much simpler and more efffective if transient assets were added to the Applicable Systems column where appropriate throughout the standards. It is not clear why R4 substantially deviates from the table format of the sub-requirements. If it is necessary to have a separate requirement for transient assets we recommend that R4 be revised to reflect the table format of the sub-requirements and not use an attachment. It is not appropriate to put sub-requirements in an attachment, they should reside in the main body of the document along with the requirement wording as is done for all other CIP standards.
No
The definition of Removable Media refers to media that are "capable of transmitting executable code to: ". We suggest that the word "transmitting" is incorrect and should read "transferring". Media such as floppy disks do not transmit but one can transfer executable code from the disk to another media.
Yes
Yes
No
Individual
Dave Francis for Terry Bilke
MISO
NO COMMENT
NO COMMENT
Yes
MISO supports the changes made by the SDT to Requirement R4 and Attachment 1. ATTACHMENT 1: The posted language for Attachment 1, Element 2.3 requires, “Responsible Entities shall determine whether additional mitigation measures are necessary…”, intending the entity make an affirmative decision to allow the device to connect. It is recommended revising as, “Responsible Entities shall determine whether any additional mitigation actions are necessary to clarify and entity may allow connection of the device without requiring modifications. GUIDELINES AND TECHNICAL BASIS: The posted language for the Transient Cyber Assets in Attachment 1, Element 1 allows for authorization to be done individually or by asset type; however the Guidelines and Technical Basis for Element 1 does not discuss the ability to authorize based on a group of assets. SMUD recommends language be added to allow “authorization individually or by groups of assets” to the Guidelines and Technical Basis for Element 1.1.

Yes
MISO supports the changes made by the SDT to these definitions.
Yes
MISO supports the changes made by the SDT to the implementation plan.
Yes
MISO supports the removal of the IAC language from the 17 requirements and the continued work by NERC to develop the Reliability Assurance Initiative.
No
Individual
Tony Eddleman
Nebraska Public Power District
No
Recommend the requirements for physical security of low assets be deleted. This requirement is repetitive of safety requirements in the National Electrical Safety Code (NESC), Section 11 - Protective arrangements in electric supply stations, paragraph 110 General requirements. The NESC includes requirements to protect the public from high voltages. The safety aspects of the NESC are more stringent than the requirements in the proposed NERC standard and public safety is a higher concern than the less likely occurrence of security concerns at a low impact asset. Specifically the proposed CIP-003-6 requires: Element 2: Examples of evidence for element 2 may include, but are not limited to: 1. Documentation of one or more access controls (e.g. card key, special locks), monitoring controls (e.g. alarm systems, human observation), or other operational, procedural or technical physical security controls to restrict physical access to both: a. The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and b. The Cyber Asset, if any, containing the Low Impact BES Cyber System Electronic Access Point. 2. Documentation showing that the physical access restrictions cited above are based on need, which may include, but is not limited to, a policy describing the high level operational or business need(s) for physical access. The proposed NERC requirement allows technical physical security controls to restrict physical access to both. A fence with a locked gate, which is required by the NESC appears to meet the proposed NERC requirement to restrict physical access to both the asset and the cyber asset. The other suggestions in the draft standard could be provided in a best practices document. The requirement for physical security of low assets should be deleted.
No
The LERC should specifically exclude communications aided relaying used for pilot relaying protection. Also, there is a high risk of confusion when using technical jargon in NERC definitions. Both of these definitions fall within this high level of confusion. If a national reliability standard requires too much technical jargon, it is written at the wrong level for its purpose. The reliability standard should be written to avoid the use of these definitions.
No

While the language in the proposed requirements is a good practice, it creates significant compliance burden for entities to maintain documentation to prove compliance; plus, additional resources will be required to implement compliance controls that yield minimal risk reduction for the reliability of the BES. Transient devices will be a source of possible violations in future internal compliance reviews for self reports and also compliance audits. Section 1.2 of Attachment 1 is not needed and should be removed. Requirements already exist for anyone having access to protected cyber systems. Section 1.2 puts an entity in double jeopardy of violating multiple requirements for one action. The same comments apply to section 3.1 of attachment 1 and this requirement should be removed.
No
As stated in previous comments, we do not support the removal of the IAC language. Removal of the IAC language is a return to zero tolerance and RAI does not magically make a violation disappear. Our suggestion is to delete any requirement from the standard that contains IAC language. This is our opportunity as an industry to remove the sections, develop better language as FERC allowed, or face multiple violations of these zero tolerance requirements for many years. We've rushed through all the previous versions to meet a deadline. This is the time to work on a solution and get a better standard. We are working to meet compliance deadlines for version five standards while making changes to the standards – this can't be a good practice. FERC approved the version five standards; they didn't remand them back. We have an official compliance date to meet for version five. Worse case, let's use the IAC language as currently approved.
Yes
The NERC CIP standards have resulted in numerous violations to registered entities and have been difficult to implement. These standards must get to a steady state and changes to the standards should be limited to an absolute minimum.
Group
Seattle City Light
Paul Haase
SMUD
No
Seattle City Light supports the proposed CIP v5 revisions, but remains concerned about the compliance aspects of providing protections for Low-rated systems and assets. Our primary concern is that in a multi-impact rated program (high, medium and low), any failure to fulfill a requirement such as Attachment 1, Element 1 Cyber Security Awareness or Element 4 Cyber Security Incident Response, could result in violation of CIP-003-6, R2, CIP-004-5, R1 and CIP-008-5, i.e. a single compliance failure could result in multiple violations. NERC recently was queried about this concern, and the response (which follows) was not especially reassuring: "Responsible Entities may choose to implement multi-impact rated programs to address low, medium, and high impact BES Cyber Systems. It is possible the same facts and circumstances

may indicate noncompliance of both the requirements applicable to low impact BES Cyber Systems and the corresponding requirements applicable to high and medium impact BES Cyber Systems. That the same act or omission may result in two separate violations is not unique to the CIP V5 standards. For example, the same failure to act immediately could constitute a violation of both TOP-001-1a R2 and TOP-008-1 R1. NERC’s Sanction Guidelines provide that one penalty may be assessed where there are multiple violations arising from a single act or common incidence of noncompliance. Therefore, if a penalty is assessed at all, it would not be duplicated. In addition, the disposition of any noncompliance is based on the level of risk posed to the reliability of the BPS. Therefore, in the event one or more of the instances of noncompliance poses a minimal risk, a number of streamlined options is available, including treatment as a compliance exception. As with any noncompliance, a determination of whether compliance exception treatment will be appropriate in a given case will depend on the facts and circumstances." In particular, the reply by NERC staff cites examples in other Standards where a single omission or failure could violate two or more requirements of different Standards. It is Seattle's understanding, however, that addressing this 'double-standard' redundancy issue throughout the Standards is one of the objectives of the present Standards clean-up effort (as recommended by the Independent Experts report, P81 effort, the ongoing 5-year reviews, and the object of “world class” standards). In particular, the two TOP standards identified by NERC as examples today are being replaced with new TOP versions (in final ballot as this is written) that address this very ‘double-standard’ issue NERC cites as a ‘reason’ it’s OK to have possible double jeopardy written into CIP v5. It is not OK. It is not world class. Newly written Standards should not include a known deficiency that industry resources now are being used to eliminate in other Standards. That NERC Saction Guidelines address potential aggregation of duplicative violations into a single penalty is welcome, but it treats the symptom of the problem rather than the cause.
Individual
Eric Ruskamp
Lincoln Electric System
No
The term Bulk Power System in the Rationale for Requirement R2 should be replaced with Bulk Electric System. The requirements outlined in Attachment 1, Element #4 for Low Impact assets are virtually identical to the requirements outlined in CIP-008-5 for High and Medium Impact BES Cyber Systems. While these requirements are appropriate for the High and Medium Impact BES Cyber Systems, they are overly onerous for the Low impact assets as the

requirements are not appropriately scaled to reflect the lower criticality of the assets the requirements are aiming to protect. This is especially true for the Low Impact assets that do not include External Routable Connectivity. These incident response requirements should only be required of High and Medium Impact BES Cyber Systems and therefore removed from Attachment 1, Element #4, or at minimum they should only apply to the Low Impact assets that have External Routable Connectivity. Without External Routable Connectivity, the only compromise to the BES is to the single BES Low Impact asset itself. According to the Rationale for Requirement R2, “these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised”. The Attachment 1 as written does not recognize the lower risk of the Low Impact BES assets.
Group
FirstEnergy
Mark Koziel
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does support EEIs recommendations for improving the wording of the requirements and related standards language.
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does support EEIs recommendations for improving the wording of the definitions and related standards language.
No
FirstEnergy does not agree that the CIP Standards adequately specify the scope of devices that can be classified as Transient Cyber Assets. The definitions and standard language make it unclear whether a Transient Cyber Asset needs to be treated as a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity makes a temporary routable connection between a Transient Cyber Asset and an ESP, would this Transient Cyber Asset also have to meet the requirements for the BES Cyber System or for a connected PCA? In other words, could the BES Cyber System requirements also be construed to apply to a Transient Cyber Asset that is temporarily connected? Recommendation: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) 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 included in a BES Cyber System and is not a Protected Cyber Asset (PCA).”
No
FirstEnergy does not agree that the CIP Standards adequately specify the scope of devices that can be classified as Transient Cyber Assets. The definitions and standard language make it unclear whether a Transient Cyber Asset needs to be treated as a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity makes a temporary routable connection between a Transient Cyber Asset and an ESP, would this Transient Cyber Asset also have to meet the requirements for the BES Cyber System or for a connected PCA? In other words, could the BES Cyber System requirements also be construed to apply to a Transient Cyber Asset that is temporarily connected? Recommendation: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) 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 included in a BES Cyber System and is not a Protected Cyber Asset (PCA).”
Yes
Although we agree with the overall approach the Standards Drafting Team has taken, FirstEnergy does support EEIs recommendations for improving the implementation plan.
Yes
No Comment
No
No Comment
Group
MRO NERC Standards Review Forum
Joe DePoorter
Yes
CIP-003-6 R2 Att. 1 Element 2 – Recommend removing “based on need” for two reasons: 1. CIP-006-5 R1.1 – Requires controls to ‘restrict’ physical access, but it does not require authorizations or “based on need” for medium impact BES Cyber Systems that do not have External Routable Connectivity. This is an example of a requirement that is more prescriptive for low than for mediums because of the additional documentation associated with “based on need”. 2. It is unclear how to interpret this part of the requirement due to the placement of the phrase “based on need”, particularly with “, if any,”. CIP-003-6 R2 Att. 1 Element 4 – Draft 2 added two more parts with 4.6 (record retention) and 4.7 (incident response plan updates.)

Recommend adding “if needed [required]” to 4.7. If the plan is okay, entities should not be required to update it.
Yes
Definitions – Low Impact BES Cyber System Electronic Access Point (LEAP) – Recommend replacing “allows” with “controls” Low Impact External Routable Connectivity (LERC.).
Yes
CIP-010-2 R4 Att. 1 Elements 1.2 and 3.1 – Recommend removing ‘Authorized’ because it adds requiring someone to approve/authorize these items. This additional level of documentation is more burdensome for low impact BES Cyber Systems. Entities would still be required to “specify” users, locations and use (individually or by group) for Element 1.2 and “specify” users and locations (individually or by group) for Element 3.1.
Yes
Yes
Yes
Yes
Implementation plan – Recommend changing the implementation date for physical access controls from April 1, 2018, to Sept. 1, 2018, because physical access controls must be applied to LEAPS, which don’t have to be identified until the electronic access controls implementation date of Sept. 1, 2018. CIP-010-2 Guidelines and Technical Basis Element 1.1 - Insert “type” with references to devices. For example, “…pre-authorize and inventory of devices or device types; or authorize devices or device types at the time….” CIP-011-2(X) R1.2 – Recommend going back to language similar to what was required in CIP-003 versions 3 and 4 R4.3, which stated: “The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.” There was no change from version 3 to version 4. The original version 5 mapping document indicates “no significant changes” when it was moved from CIP-003 to CIP-011 R1.3. However, R1.3 was removed from version 5 when the IAC language was incorporated. Now that IAC has been removed, the V3 text or something close to it should be retained. Possible revision: “The Responsible Entity shall, at least annually, assess adherence to its BES Cyber System Information protection program, including identification, protection and handling; document the assessment results; and implement an action plan to remediate deficiencies identified during the assessment.”
Individual
Karin Schweitzer
Texas Reliability Entity
No

1) Rationale for Requirement R1: Texas Reliability Entity, Inc. (Texas RE) recommends replacing “its” with “a Responsible Entity’s” in the second sentence of the first paragraph. The proposed revised language would read as follows: “The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity’s BES Cyber Systems.” 2) Requirement R1.2: Texas RE recommends the following elements be added to the Cyber Security Plan for Low Impact systems to reduce the risk to Medium and High Impact BES Cyber Systems: information protection, recovery functions, system security functions and configuration change management functions. By definition, Low Impact systems are those deemed not as critical to the BES as Medium or High Impact systems. However, in today’s integrated EMS networks, a vulnerability in a Low Impact system is imposed on Medium and High Impact BES Cyber Systems. Therefore the aforementioned items should be included in the Low Impact system Cyber Security Plans.
No
Low Impact BES Cyber System Electronic Access Point (LEAP): Texas RE requests the SDT consider including the functional definition that is already included in CIP-003-6, Attachment 1, Paragraph 3.1 within the proposed definition of a LEAP. In addition, we suggest striking the last sentence of the definition because it appears to be in conflict with the Electronic Access Control or Monitoring Systems (EACMS) definition that becomes effective April 1, 2016. The FERC approved EACMS definition includes all BES Cyber Systems and is not restricted to Medium or High Impact BES Cyber Systems; therefore, the LEAP definition should not exclude Low Impact BES Systems. Texas RE suggests the following change to the definition: “Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that allows Low Impact External Routable Connectivity and permits only necessary inbound and outbound access and denies all other access.”
No
1) Requirement R4: It appears the SDT may have inadvertently excluded low impact BES Cyber Systems. FERC directed in Order 791, Paragraph 136, that requirements should consider “processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact).” Texas RE recommends the following revision to Requirement R4: “Each Responsible Entity, for its high impact, medium impact, and low impact BES Cyber Systems and associated Protected Cyber Assets, shall implement one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1, except under CIP Exceptional Circumstances.” 2) Measure 4: Proving compliance may be difficult for a registered entity since there is no requirement to maintain any identification nor connection records that validate whether the device was connected for 30 consecutive days. This could be remedied with the addition of the following language to M4: “including but not limited to a list of in-scope transient devices, and manual or automated logs showing connection periods…” The proposed revised language would read as follows: Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable elements in Attachment 1 and additional evidence, including but not limited to a list of in-scope transient devices, and manual or automated logs showing connection periods to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional

examples of evidence per element are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.
Yes
No
Texas RE suggests that the proposed implementation time periods are excessive by 12 months, particularly for administrative documentation. Therefore, Texas RE recommends the following changes for implementation for CIP-003-6: CIP-003-6: April 1, 2016 (no change) CIP-003-6, R1, R1.2: April 1, 2016 CIP-003-6, R2: April 1, 2016 CIP-003-6, Attachment 1, Element 1: April 1, 2016 CIP-003-6, Attachment 1, Element 2: April 1, 2017 CIP-003-6, Attachment 1, Element 3: September 1, 2017 CIP-003-6, Attachment 1, Element 4: April 1, 2016
Yes
No
Individual
David Jendras
Ameren
Agree
Ameren supports EEI comments for Project 2014-02 CIP V5 revisions.
Individual
Andrew Pusztai
American Transmission Company LLC
Yes
ATC has no comment.
Yes
ATC has no comment.
Yes
ATC has no comment.
Yes
ATC has no comment.
Yes
ATC appreciates the SDTs consideration of previous comments, and supports the adjustments in the implementation plan that accommodate for the time necessary to be successful in implementing elements 2 & 3 for Low Impact pursuant to CIP-003-6. Thank you.
Yes

ATC has no comment.
No
Individual
Oliver Burke
Entergy Services, Inc.
No
Entergy recommends aligning the Electronic Access Controls language with the Physical Access Controls language to allow the Responsible Entity the latitude to design controls that are consistent with needs dictated by the Responsible Entity’s configuration.
No
In general, Entergy disagrees disagree with the creation of new acronyms that are applicable only to for Low Impact BES Cyber Systems.
Yes
Yes
Yes
Yes
No
Individual
Venona Greaff
Occidental Chemical Corporation
Yes
Occidental supports the structure of CIP-003-6, including Attachment 1.
Yes
Occidental supports the proposed new definitions of Low Impact External Routable Connectivity and Low Impact BES Cyber System Electronic Access Point. We appreciate the level of clarity that the two new definitions provide.
Abstain
Abstain
Yes

Occidental supports the tiered deadlines for the aspects of CIP-003-6 and believe them to be reasonable and appropriate.
Yes
Occidental supports the removal of the IAC language in the time frame ordered by FERC as well as the continued work by NERC to develop the Reliability Assurance Initiative.
No
Individual
Scott Berry
Indiana Municipal Power Agency
Yes
IMPA supports the SMUD comment on Attachment 1: SMUD does suggest an important edit to Attachment 1, Element 1 to clarify the obligation. The posted language requires “Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:…” Literal reading of this obligation means that entities are required to perform security awareness on a specific 15 month cycle. To align this obligation with that of CIP-004-5, R1, Part 1.1, SMUD requests the following edit: “Each Responsible Entity shall reinforce, AT LEAST ONCE every 15 calendar months, its cyber security practices, using one or a combination of the following methods.” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle.
No
IMPA supports the EEI comments regarding Attachment 2 of CIP-010-2: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped.
Yes
IMPA supports the removal of the wording and understands that NERC proposes to use the RAI program to keep these 17 requirements from becoming “zero” defect requirements. However, IMPA would like to see the RAI program be approved by the NERC Board and FERC before considering an “affirmative” vote on the CIP standards. In addition, the RSAWs need work with providing clarity and guidance for the compliance expectations of the CIP standards, especially since the IAC wording has been removed.
Individual

Candace Morakinyo
Wisconsin Electric Power Company
Agree
Edison Electric Institute (EEI)
Individual
Michelle D'Antuono
Ingleside Cogeneration LP
Agree
Occidental Chemical Corporation
Group
ACES Standards Collaborators
Trey Cross
Yes
The changes made to the formatting also assist entities in implementing the requirements through the use of attachment 1 and 2.
Yes
Yes
Additional guidance as to what is ‘not’ considered a transient device could be beneficial to the industry and would remove any possible confusion or assumptions.
Yes
Yes
We would like the drafting team to consider modifying the implementation dates for electronic access and physical security to be 18 months from the effective date of April 1, 2017. Physical security implementations, depending on the site(s), could have long durations and require additional budget cycles to implement across a diverse geographic and multiple asset types.
Yes
Moving from a zero defect compliance approach to a risk-based compliance is critical to the success of implementing CIP version 5. There has been significant progress made with Reliability Assurance Initiative. If RAI is not fully implemented and well understood by industry well in advance of the effective date of the CIP standards, there will be a significant increase in violations without a commensurate benefit to reliability. We are cautiously optimistic that RAI will be implemented in time for implementation of version 5 of the CIP standards.
Yes
(1) We support the CIP v5 Revisions Standards Drafting Teams’ (SDT) efforts in minimizing the impact of Low Impact Facilities implementation by not requiring an asset inventory list,

allowing of grouping of assets for physical security and flexibility of restricting electronic access. (2) Because CIP Version 5 revisions will impact the smaller utilities, cooperatives, load serving entities, and distribution providers significantly, it is beneficial to these entities to approve CIP 5 revisions without further changes (so that they are steady-state) to allow for the impacted entities to plan, budget and implement CIP Version 5. (3) Approval of the changes to Identify, Assess, and Correct language removal, network communications security, Low Impact requirements and Transient Device requirements is recommended by ACES.
Individual
Amy Casuscelli
Xcel Energy
No
Xcel Energy has concerns about the requirements applicable to Low Impact assets. The revised language states that there is no expectation to keep a list of individual low impact BES Cyber Systems and their associated cyber assets or to maintain a list of authorized users. It is unclear how compliance evidence of required electronic access controls per Attachment 1, Element 3 can be shown without such lists. Additionally, this appears to be in contradiction of the FERC directive to fix by adding specific requirements. It would seem the precedent used for Medium Impact without External Routable Connectivity of just documenting operational and procedural controls would be sufficient. This ambiguity in Requirement language is concerning since Xcel Energy will have over 600 low impact substations; an 850% increase in those subject to NERC CIP Compliance with a resulting significant financial impact to implement electronic access controls at these low impact substations. While the proposed standard allows an option or a combination of either access controls, monitoring or defining operational and procedural controls for Low Impact assets, these requirements are still beyond those of Medium Impact Assets without External Routable Connectivity. With these recommendations, it appears that more value is being placed on Low Impact Assets than Medium Impact without External Routable Connectivity so the Medium Impact Medium Impact without External Routable Connectivity language should be modified and/or Low Impact should follow the same requirements as Medium Impact without External Routable Connectivity. However, since Low Impact Assets are by definition those with low risk to the BES, the original Version 5 requirement simply requiring documentation of physical controls would seem sufficient. Given the number of Low Impact Assets, with the requirements in CIP-003-6 Attachment 1, more time will be spent addressing Low Impact facilities and assets than High or Medium. The R2 revision introduces a requirement to have ‘plans’ for each of the four areas for Low Impact systems. Previously the requirement was only to have policies/procedures/controls. This creates an additional administrative burden to bundle the policies/procedures/controls into a ‘plan’ and should be removed. Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. We recommend the addition of [if needed] after “180 calendar days.” Attachment 2 (examples of evidence) and Guidelines and Technical Bases for element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for element

2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistences make the language of the Standard in Attachment 1 vague and unclear. We recommend revising the Guidelines and Technical basis to include all example controls in one reference, and indicate that the minimum requirement for perimeter control shall include fences with locked gates and site access policies only. The language should indicate that additional controls, such as CCTV, card key access and special locks may be used as desired but exceeded the minimum requirement. In the Guidelines and Technical basis section the SDT uses the Version 3 term, special locks but outside of what is in the standard, does not define this term. Is a propriety key considered a special lock or what is the definition of “restricted keyway”?
No
The definitions for both LEAP and LERC are not clear. The LEAP definition would suggest that a logical network extends beyond a physical boundary, as the LEAP does not necessarily have to reside at the same location as the low-impact BES Cyber Systems. If the LEAP is not an EACMS, then what control is being applied to this asset classification? The definition for LERC is also unclear. The phrase “Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s).” is unclear if it is referring to access to/from a system or network.
Yes
Yes
No
We do not support the revised language providing for tiered deadlines for low impact assets.
Yes
One of the greatest advantages of the IAC language was to allow the industry to focus on security and move away from administrative burden of no to minimal risk issues. The idea of Internal Controls and RAI seems to be a good alternative, but has yet to be fully defined, leaving more burden on the industry, the regions and NERC to document and enforce minimal issues under the FFT program.
No
Individual
Megan Wagner
Westar Energy
Agree
Westar Energy supports the comments submitted by Edison Electric Institute (EEI).
Individual
Patrick Farrell

Southern California Edison Company
Yes
Yes
No
The revised language in CIP-010-2, Requirement 4 is unclear with respect to "under CIP Exceptional Circumstances." We would recommend revising the language to state: "Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the elements in Attachment 1." We believe that this clarifies the language of this requirement. Additionally, SCE would suggest that Elements 1 and 2 of Attachment 1 be revised to clarify the levels of review required based on the control exercised by a Responsible Entity over a Transient Cyber Asset (TCA). The language should be revised to describe the requirements when an entity has "full" or "substantial" control through its ownership and management of the asset, as compared when an entity has "minimal" control, as seen when leasing an asset from a vendor. We think that this clarification would aid entities in ensuring compliance with CIP-010-2.
Yes
Yes
Yes
Yes
SCE strongly supports the EEI comments relating to CIP-010-2.
Individual
Chris Scanlon
Exelon Companies
No
Exelon supports the revised structure of CIP-003 and the extensive revisions made to the requirement language. Below are comments for SDT consideration. Exelon voted negative on CIP-003, though it feels the standard is very close to acceptable. While most of the comments point to refinements in the language rather than “deal breaker” concerns, the length of the list suggested that the standard is not yet ready for final approval. Exelon called out the most concerning issues below and feels that addressing all the points below will provide greater clarity for entities when the standard is implemented and audited. General Concerns 1.

Potential for Multiple violations: Exelon supports the use of CIP-003 for the requirements applicable to lows and appreciates the revised language that allows entities with multiple impact levels the option to incorporate low into related programs applicable to highs and mediums. This flexibility is important to accommodate the diverse circumstances that exist across the industry. However, Exelon has some concern that in a multi-impact rated program (high, medium and low), any failure to fulfill a requirement such as Attachment 1, Element 1 Cyber Security Awareness or Element 4 Cyber Security Incident Response, could result in violation of CIP-003-6, R2, CIP-004-5, R1 and CIP-008-5. Potential compliance and enforcement implications should not dictate the structure of the standards nor an entity's compliance program. An entity should be allowed to determine, in a form most efficient and effective to the entity, the best approach in fulfilling the security requirements. Please offer reassurance that the currently proposed structure with CIP-003-6, R2 does not create a potential situation for multiple violations. Confirmation from NERC Compliance will be important. This is a key concern that influenced a negative vote. 2.CIP-003-6, R2. Please directly discuss in the Guidelines the relevance of the "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." This note was important in the approval of V5 and Exelon supports inclusion of this note to help limit focus on a list of devices rather than emphasizing protections. However, many struggle to understand how to demonstrate compliance without having a list. Please discuss any potential alternatives to a list. As well, since the note does not preclude using a list if an entity determines this to be a desired tool to demonstrate compliance, please confirm that violations are not to accrue to the list, but only to failures to implement the plan Attachment 1 1.Element 1: To be consistent with CIP-004-5 and to match the discussion in the Guidelines, Element 1 should remove the word "its" to read: "Cyber security awareness: Each Responsible Entity shall reinforce, once every 15 calendar months, cyber security practices, using one or a combination of the following methods: …" 1a -The inclusion of "its" reads that the awareness program is to discuss the cyber security practices of the entity rather than the more general wording of CIP-004-5, R 1.1: "… reinforces cyber security practices (which may include associated physical security practices) …" Furthermore, addition of the parenthetical would be helpful to clarify that physical security practices are acceptable awareness topics under this requirement. These two adjustments are important to entities with multiple impact level BES Cyber Systems that may want to apply a single program to apply to high, medium and low impact levels. 1b - As well, the adjustment is needed to be consistent with the Guideline language: "The intent of the security awareness program is for entities to reinforce good cyber security practices … The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems." As stated, the intent does not limit the awareness topics to only those associated with internal cyber security policies and practices. 1c - This revision is important to Exelon and was a factor in the decision to vote negative. 2. Element 1: Please move the bullets under Attachment 1, Element 1 to Attachment 2, Element 2. Moving the bullets in the measures is consistent with CIP-004-5, R1.1. 3.Exelon supports the stand alone nature of the element 2 and 3 language. While the requirements in these elements are consistent with those in the corresponding requirements applicable to High and Medium impact BES Cyber Systems, it is

appropriate for those applicable to lows to be unique and appropriate to the risk presented by Low impact BES Cyber Systems. 4.Element 3: On electronic access controls, please offer more insight on “other electronic access controls that provide an equal or greater level of protection.” Exelon recognizes and appreciates that technology evolves and the requirement language should allow entities to use technology/methods that may prove useful in the future but not yet envisioned at the writing of the requirements. How does the drafting team envision that entities manage the comparison? 5.Element 4. Cyber Security Incident response: Please clarify the intent of “either by asset or group of assets…” Exelon pointed out in comments to the initial proposal that revision was needed to clarify that Cyber Security Incident response plans need not be site specific and that an enterprise-wide plan could fulfill the obligations for locations with low impact BES Cyber Systems. If this is the intent of the grouping language, Exelon supports the intent, but finds that the revision is not clear to that intent. If the intent is different, please explain and revise with clearer language. Consider the following revision: Cyber Security Incident response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s) covering either an individual asset or group of assets, which shall include: … Or just remove the comma after “plan(s)”. 6. Please justify the addition of 4.6 and 4.7 to the obligations of a Cyber Security Incident response plan. These elements were not required in the initial posting of the revisions and add an additional administrative burden to lows than was first proposed. Attachment 2 1.Exelon supports the use of Attachment 2 to provide added detail to the Measures. 2.See above for suggested move of Element 1 bullets from Attachment 1 to Attachment 2. 3.Element 1 – The wording can be clearer. Please consider the following revision (including the bullets from Attachment 1): “Element 1: An example of evidence for element 1 may include, but is not limited to documentation that cyber security practices have been reinforced once every 15 months through dated copies of the information used to emphasize security awareness via one or a combination of the following methods: Direct communications (for example, e-mails, memos, computer-based training); Indirect communications (for example, posters, intranet, or brochures); or Management support and reinforcement (for example, presentations or meetings).” Guidelines 1.Minor items: 1a - Page 33, Requirement R2 Attachment 1 – Physical Security, third paragraph, last sentence: Instead of “imply” consider require or obligate. 1b - Page 33, LEAP, third sentence, “LEAP” should be plural.
Yes
Yes
Exelon supports the proposed revisions to CIP-010-2. In our internal discussions, participants raised a couple questions. Exelon requests that the SDT consider incorporating responses to these questions either in a Q&A document or within the Guidelines. Below are the questions and draft responses from SDT outreach. Q and A Q1: Are contract obligations sufficient to fulfill the Element 2 requirements? A1: Yes, see Guidelines, in particular page 42: To facilitate these controls, Responsible Entities may choose to execute agreements with vendors and contractors to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department Of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. Elements

from the procurement language may unify vendor and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP Program elements may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the vendor's support. Entities should consider the elements of the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls. Q2: How often are entities required to scan Removable Media to fulfill element 3.2? A2: Frequency and timing of scanning was intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The Removable Media must be scanned before it is connected to the BES Cyber Asset and that timing as dictated by the entity's plan should reduce the risk of malicious code mitigation.
Yes
Yes
Exelon supports the currently proposed Implementation Plan. We understand that others in the industry prefer to sync up the deadlines for the physical and electronic access control requirements. While Exelon would accept synced deadlines, it would do so only if the physical access controls deadline moved out to September 1, 2018 to match the electronic access controls deadline. Exelon prefers the staggered approach over moving the electronic access control deadline up to April 1, 2018. In addition, Exelon requests that the SDT consider incorporating responses to a question on the implementation plan either in a Q&A document or within the Guidelines. Below is a question and draft response from SDT outreach. Q and A Q1: Under the Cyber Security Incident response plan required to be in place by April 1, 2017, would a physical access incident be an incident if the physical access controls are not required until April 1, 2018? Likewise for electronic access controls not required until September 1, 2018? A1: The April 1, 2017 deadline requires that entities have a response plan in place. Since lows are not required to have ESPs or PSPs, the operative trigger is whether an event occurred that "Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System" (per the second bullet). As written in the implementation plan, between April 1, 2017 and the respective implementation deadlines for access controls, the entity would be required to demonstrate response to incidents that meet the second bullet; however, would not have to demonstrate the implementation of access controls that may have been related to the incident.
Yes
Exelon supports the Version X package of revisions and understands the need to have these revisions approved should they need to go forward independent of the revisions for Low Impact and Transient Devices. However, Exelon strongly supports the SDT's efforts to complete revisions in all four issues areas by the Feb 2015 filing deadline and hopes for a break in the revisions to the CIP standards. CIP resources are currently devoted to implementation of CIP Version 5. The task is daunting and resource intensive. Exelon looks forward to a stretch of time in which CIP work can focus on implementation without revisions

in development. In addition, timely resolution of the Order 791 CIP-003 directive is important to enable entities to avoid an iterative implementation of V5 and V6 for the Low Impact assets.
Yes
Concerns remain with the implications of the CIP-003 requirements on dispersed generation. Exelon supports the progress of the Order 791 revisions, but would like to see continued collaboration with the Project 2014-01 Applicability for Dispersed Generation Resources Standards to better balance the demonstration of compliance burden with the risk of dispersed generation facilities. Exelon thanks the SDT for their hard work in revising the CIP standards.
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 for Low Impact Assets, as an Attachment to CIP-003-6, results in Standards language inconsistencies that creates confusion and is likely to cause additional compliance risks to entities having multiple impact levels. The following are some specific examples: A. The Low Cyber System requirements continue to be inconsistent with High / Medium requirements in other standards. These current inconsistencies have been attributed to deficiencies in the Quality Assurance process used prior to the release of this new draft, however, this only validates concerns that there will ‘always’ be inconsistencies of this type when the controls are split between the Standards as was done in this case. B. 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 that are part of any impact category. This could also lead to the following: 1. If a BES asset contains Low and Medium or High Cyber Systems, it would be possible to violate multiple requirements in multiple Standards. This would be clearly be possible for some of the requirements in CIP-004, CIP-006 and CIP-008 (or any Standard with a facility impact), since having some ‘Low’s along with any other impact level Cyber Assets would apply to all Cyber Assets in that facility. 2. This further complicates the new policy and procedure structures that an entity needs to meet CIP version 5 compliance. The NIST-like structure outlined in CIP-003, R1, is likely the most common direction that most entities will choose to ‘clearly’ meet CIP Version compliance. Having the ‘Low’ impact Cyber Systems hanging ‘out on a limb’ in a CIP-003 Attachment will reduce the clarity of addressing the required controls for those assets in a ‘mixed’-impact environment. The end of result of having Low Impact Asset controls contained only in CIP-003

is that going forward, as the CIP requirements are changed, the likelihood of creating additional inconsistencies is high. 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 and/or becoming inconsistent. These new set of CIP standards are already very complex, and any added confusion caused by this structural problem will result in difficult (and costly) compliance implementations. This will likely negate the goals of improving overall reliability.
No
We agree with the NPCC cpmments on this question.
No
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Yes
We agree with the NPCC cpmments on this question.
Group
PJM Interconnection LLC
Stephanie Monzon
Yes
Yes
Yes
Yes
Yes
Yes
No

Individual
Sonya Green-Sumpter
South Carolina Electric & Gas
Individual
Kalem Long
The Empire District Electric Company
Agree
EEI
Individual
Christina Conway
Oncor Electric Delivery Company LLC
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions. Additional comments below: CIP-010-2 R4 Attachment 1: Oncor utilizes embedded device platforms, such as Substation relays and RTUs, which are not as vulnerable to malicious code/Malware as computer systems. It is Oncor's interpretation that Substation embedded device platforms are afforded security features provided by nature of embedded controls. However, these embedded devices do not have access control or logging capabilities, therefore incapable to log users and/or generate logs. Therefore, it is not technically feasible to demonstrate that a specific Transient Device, such as a laptop, is connecting or was connected to such embedded device platform. CIP-010-2 R4 Attachment 1 Element 1.2.2: The Guidelines and Technical Basis page 44 Element 1.2.2 states: To meet this requirement part, the entity is to document the following: 1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations. As previously mentioned, it is not technically feasible to authorize locations for Transient Devices, such as laptops, to access substation cyber assets. There are controls in place to restrict access such

as perimeter fence with locked gates, locked control house doors, and unique passwords to the assets. Oncor is seeking clarity on the following: Does the section on page 43 “Per Cyber Asset Capability” exclude the aforementioned Medium Impact BES Cyber Assets without ERC substation assets based on capabilities? Recommendation: Rewrite the Requirement, Attachment(s) and/or Guideline and Technical Basis to clarify and articulate that embedded device platforms, such as substation relays and RTUs, which are not vulnerable and incapable of control accessing or logging, are excluded from CIP-010-2. Alternatively, Limit applicability to Medium Impact BES Cyber Assets with ERC, or vulnerable to malicious code.
Yes
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
Yes
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
Yes
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
Group
Duke Energy
Michael Lowman
Yes
No
Duke Energy suggest the following revision to Low Impact BES Cyber System Electronic Access Point: “Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that permits Low Impact External Routable Connectivity. The Cyber Asset may reside at a location external to the asset or assets containing low impact BES Cyber Systems. The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System except when the LEAP is on the same Cyber Asset as an Electronic Access Control or Monitoring System.” We believe the use of the word “allows” is too broad whereas the word “permits” better reflects the SDT’s intent. The addition of “except when the LEAP is on the same Cyber Asset as an Electronic Access Control or Monitoring System” is needed for those instances when a LEAP is on the same Cyber Asset as an Electronic Access Control or Monitoring System.
No
Duke Energy suggests adding a time requirement in Attachment 2, section 1 similar to the one found in Attachment 1 section 1. As currently written, there does not appear to be a time requirement for the frequency with which an entity should review Transient Cyber Assets owned or managed by Vendors or Contractors. Is an entity required to review the items listed in section 2.1 every time a vendor logs on/ patches into the Cyber Asset?

Yes
We ask the SDT to provide an example of a device the is not capable of transmitting executable code. We are unclear as to an example of a Transient Cyber Asset that is not capable of transmitting executable code.
No
Duke Energy suggests revising the Compliance Date for CIP-003-6, Attachment 1, element 2 to coincide with the Compliance Date of CIP-003-6, Attachment 1, element 3. As currently written, it appears that the elements are circular in nature. Essentially, an entity would need to be compliant with element 3 before becoming compliant with element 2 and could be physically protecting a device that does not exist.
Yes
No
Group
Southern Company: Southern Company Services, Inc.; Alabama Power Company, Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Pamela Hunter
No
Southern appreciates the substantial revisions to the requirements language in CIP-003 and Attachment 1 and offers several items for SDT consideration below. The new structure and overall content are a great improvement. The negative vote on CIP-003 is only to address these couple of issues but overall the newly drafted standard reflects the appropriate level of detail for requirements applicable to Low Impacts assets. Comment 1: CIP-003-6 – Attachment 1: CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation: Change Attachment 1, Element 2 to “Physical security controls” to be consistent with the language of the standard. Please edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs) to CIP-003-6 R1 for consistency. Comment 2: CIP-003-6 Requirement R2 ends with “include the elements in Attachment 1”, although the first sentence in Element 1 says “include each of the elements provided below” the actual “elements” are not labelled “elements” as in Attachment 2, which references the elements in Attachment 1. Recommendation: Add “Element” before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses. This would also be helpful for Attachment 1 in CIP-010-2. Comment 3: The “(LERC)” and “(LEAP)” acronyms are missing in Element 2, 3, and 3.1, which makes it harder to identify the use defined phrases in these elements. Recommendation: Add the “(LERC)” and “(LEAP)” to elements 2, 3, and 3.1 to make it easier to identify the acronym. Comment 4: CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation: Add “,

if needed,” after “180 calendar days.” Comment 5: CIP-003-6 Attachment 2 and Guidelines and Technical Basis for element 2: Attachment 2 (examples of evidence) for element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for element 2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation: Include “perimeter controls” under element 2, Attachment 2 in the example: “(e.g., card key, special locks, perimeter controls). Comment 6: CIP-003-6 Guidelines and Technical Basis for Requirement R2 Attachment 1 and the LERC definition – Electronic Access Controls: The following scenario is unclear: {Low impact BES Cyber System (e.g., control system) ---- |1| ---- Cyber Asset (e.g., data historian) ---- |2|} ---- Location X Where: {} represents the asset/site boundary, |1| represents a firewall or electronic access point (in this case firewall 1), and ---- represents a bi-directional routable communication Based on the language of the definition and CIP-003-6 it is unclear whether there is a LERC and LEAP in this scenario and if there is LERC, which firewall is the LEAP. The Guidelines and Technical Basis for CIP-003-6 say “the electronic access controls should address the risk of using the asset’s LERC to gain access to the low impact BES Cyber Systems.” However, this scenario would require an adversary to gain access to not one but two access points, the firewalls on either side of the Cyber Asset (firewall 2 and then firewall 1) to get access to the low impact BES Cyber System. Whereas, the examples provided all show one access point, the LEAP, which requires controls. Recommendation: Add this scenario to the CIP-003-6 Guidelines and Technical Basis, clarify that there is a LERC and allow the Responsible Entity to have the flexibility choose the LEAP, either firewall 1 or firewall 2. Comment 7: The Guidance on LEAP has the phrase “However the LERC between assets “behind” the LEAP and another asset containing a low impact BES Cyber System must also pass through the single LEAP”. LERC between assets behind the LEAP” could imply connectivity between them is allowed without passing through the LEAP first – regardless of their communications with another asset containing a low impact BES Cyber System (which by definition would have to be behind a LEAP as well, but maybe not the same one). Southern Recommendation: Consider rephrasing to: However the LERC between assets “behind” the LEAP must pass through the single LEAP. Comment 8: The Guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation: In the Guidelines and Technical Basis for CIP-003-6, where LEAP is described, move the sentence “LEAP are not to be considered EACMS…” to create a second paragraph and add “However a LEAP can be implemented within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself.”

No

Southern appreciates the new terms to help clarify the requirements language in CIP-003. The negative vote on CIP-003 is only to address these couple of issues. Comment 1: Use of “allows” in the LEAP definition does not allow for the use of an unmanaged hub. An unmanaged hub, which does not support access controls and may be acting as a central connecting point, could be considered an interface that “allows” Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs. Recommendation: Change “allows” to “controls” to allow for the use of unmanaged hubs as appropriate. Please also make sure this is changed in the Guidelines and Technical Basis and anywhere else the LEAP definition is provided. Comment 2: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation: Change the exclusion sentence to: “Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).” Alternatively, clarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to include point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions.
No
Southern appreciates the revisions and overall direction that SDT made to the structure of CIP-010-2, R4 but offers the comments for consideration below to help with clarity. Comment 1: CIP-010-2 Attachment 1: The use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and 2) it is implied by the language of 1.2 and 1.3. The language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization. The redundancy creates uncertainty in the interpretation of the standard. It could be interpreted to imply a second step in addition to the R4 plan. In other words, in addition to the R4 plan for Transient Cyber Assets and Removable Media, which includes the 1.2 and 3.1 authorization elements, the Responsible Entity must also have a separate, formal approval process to identify authorized users, authorized locations, and authorized uses for Transient Cyber Assets and a separate formal approval process to identify who is authorized to use and where they are authorized to use Removable Media. We believe the intent of the Standards Drafting Team is that the plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address these authorization elements. This flexibility will allow the Responsible Entity to either write a plan that specifically defines who is authorized to use the Transient Cyber Asset(s) for which uses and locations or include a separate authorization process, which may include a formal approval process, in the plan that identifies the users, locations, and uses authorized for the Transient Cyber Asset(s). It will also give the Responsible Entity the same flexibility for Removable Media authorizations. This flexibility is particularly needed for

Responsible Entities that rely on contractor use of Responsible Entity managed Transient Cyber Assets and Removable Media who have less control over the contractor, i.e., the control is defined by a service agreement or contract. Giving the Responsible Entity flexibility on how to define the authorization process will allow them to align these requirements with their vendor contracts. Recommendation: Remove “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. Alternatively, clarify in the Guidelines and Technical Basis under Element 1.2 and 3.1 that the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 does not require a formal approval process for each user, location, and use of the Transient Cyber Asset (or Removable Media), but gives the Responsible Entity the flexibility to develop an authorization plan that either directly defines authorization or requires a specific authorization process. This allows Responsible Entities to align their Transient Cyber Asset and Removable Media authorizations with their vendor contracts for use of Responsible Entity managed Transient Cyber Assets. Comment 2: CIP-010-2- Attachment 1 Elements 1 and 2 are grouped by whether a Transient Cyber Asset is owned or managed by the Responsible Entity or by a vendor or contractor. The intent of this grouping is good because it considers the level of control by the Responsible Entity. However, the actual groupings could result in a Transient Cyber Asset that falls under both element 1 and 2. For example, if a Responsible Entity owns the Transient Cyber Asset, but a contractor manages its use under a service management contract. Another scenario is that the vendor owns the Transient Cyber Asset, but the Responsible Entity manages it. For these scenarios, it is unclear whether the Responsible Entity should include element 1 or 2 or both elements in their R4 plan(s). Recommendation: Remove “Owned or” from elements 1 and 2. Comment 3: CIP-010-2 Attachment 1, section 1.5: Currently drafted as: Transient Cyber Asset resides within a location with restricted physical access; Recommendation: Consider rephrasing to say: The Transient Cyber Asset must reside within a location with restricted physical access; Comment 4: CIP-010-2 - Attachment 1, Element 2.3: “Responsible Entities shall determine whether additional mitigation actions are necessary…” requires a statement that says no additional mitigation measures were identified as necessary, which creates an unnecessary administrative burden. Also, Element 2.3 is an element that should be addressed by the R4 plan for Transient Cyber Assets and Removable Media, the way Element 2.3 is written makes it look like a requirement rather than a plan element, which also causes confusion as to the frequency of review for elements 2.1 and 2.2. Element 2.3 as written suggests that a Responsible Entity must use the 2.3 and 2.4 mitigation methods prior to each connection of a vendor-owned Transient Cyber Asset in order to determine whether additional mitigation measures will be needed. This can be overly burdensome and unnecessary when a vendor is moving from system to system in a single day. Also, a Transient Cyber Asset may be owned by the Responsible Entity and managed by a vendor or owned by the vendor/contractor and managed by the Responsible Entity. The use of “vendor- or contractor-owned” in 2.3 is not consistent with these scenarios (see comment 3.3 above). Recommendation: Add “necessary” before “such actions.” Also, clarify in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how to manage vulnerability and malicious code reviews of their vendors or contractors and require additional mitigation actions. For example, one entity may require a vendor to plug a Transient Cyber Asset into a kiosk to scan for vulnerabilities and malicious code before each

connection. However, this approach may not be feasible for all entities, so defining a process to initially and periodically check and audit vendor/contractor processes for vulnerability and malicious code mitigation. Specifically, “prior to connecting the vendor- or contactor-owned Transient Cyber Asset” does not require that 2.1, 2.2, and 2.3 before each connection, but that the Responsible Entity should define a process to manage the use of vendor- or contractor- managed Transient Cyber Assets to mitigate vulnerabilities and malicious code. Also, change “owned” in 2.3 to “managed.” Comment 5: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped. Recommendation: Make it clear in the Guidelines and Technical Basis that “mitigate” and “mitigation” does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system that the Transient Cyber Asset or Removable Media is used on. Also, it may be impossible to detect every piece of malicious code. Mitigation is meant to reduce security risks, but elimination of all risk is impossible. Comment 6: CIP-010-2 – Attachment 2, Element 3.2: This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. Recommendation: Change “scan Removable Media outside of the BES Cyber System” to “use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code.” Comment7: Guidelines and Technical Basis for R4, Attachment 1, Element 1.1: inventories of Transient Cyber Assets is allowed by individual or group – individually or by asset type, therefore language under Element 1.1 should be consistent, allowing inventory of devices or device type. Recommendation: Add “or device types” to the second sentence: “pre-authorize and inventory of devices or device types or authorize devices or device types at the time of connection or use a combination of these methods.”
No
Comment 1: Transient Cyber Asset Definition: The “and” in the parenthesis after “A Cyber Asset,” is confusing and appears to be misplaced. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. It refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, “directly connected” may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Recommendation: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) 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.” Also, if the intent is for the Transient Cyber Asset definition to apply to both routable and non-routable communications, clarify this in the Guidelines and Technical Basis for CIP-010-2.
No
Southern appreciates the revised schedule and supports the increased timeframe for implementation. The only reason for the negative vote is the disconnect between the dates as noted below. Comment 1: CIP-003-6, Attachment 1, Element 2 compliance date of April 1, 2018: According to the Implementation Plan, the Element 2 physical access controls must be applied to LEAPs by April 1, 2018; however, the LEAPs are identified under Element 3, which must be applied by September 1, 2018. Recommendation: The compliance date for LEAPs is after the compliance date for physical, but the two are tied together since LEAPs have to be physically secured. These two dates should be the same or please add clarity on how best to implement the requirements based on disconnect between the two timeframes.
Yes
Southern supports the Version X package of revisions.
Yes
Southern would like to commend the SDT for all the hard work and effort that has gone into revising the CIP Standards.
Individual
Muhammed Ali
Hydro One
Agree
Task Force on Infrastructure Security & Technology - TFIST
Individual
Bob Thomas
Illinois Municipal Electric Agency
Agree
Florida Municipal Power Agency
Individual
John Merrell
Tacoma Power
Agree
Sacramento Municipal Utility District
Individual
David Burkey
Puget Sound Energy
Agree
Edison Electric Institute

Individual
David Thorne
Pepco Holdings Inc
Yes
PHI supports EEI Comments for this question.
Yes
Further clarification and description of the time sensitivety associated with LERC should be included in the Guidelins and Technical Basis section.
Yes
PHI supports EEI Comments for this question.
Yes
PHI supports EEI Comments for this question.
Yes
Yes
Yes
PHI supports EEI Comments for this question.
Individual
Roger Dufresne
Hydro-Quebec Production
No
Incoherence with CIP-002-5 are observed. Elements of CIP003-6 R2 are base on new definitions that applies to elements explicitely excluded from CIP-002-5. CIP-005 need to be ajusted to reflect the real intentions of the SDT. Incoherence are observed for the implementation dates: CIP-003-6, Attachement 1,element 1 until the later of April 1, 2017 CIP-003-6, Attachment 1, element 2 until the later of April 1, 2018 CIP-003-6, Attachment 1, element 3 until the later of September 1, 2018 CIP-003-6, Attachment 1, element 4 until the later of April 1, 2017 Physical requirement (element 2) goes in effect before the electronic ones (element 3). Requirement 2 demands to restric acces point of low BCS while low BCS a covered 5 months later.
Yes
No
Impacts are major for the utilities
Yes

No
See answer to question 1
Yes
No
Individual
Brett Holland
Kansas City Power and Light
No
No, we do not agree. The protections suggested for low impact assets still represent too large a pool of assets that do not have a substantive impact to the BES, the reference to electronic and physical controls language required for low impact assets is vague and open to much interpretation, and the requirement for issues to be reported to the ES-ISAC does not support measured improvement for reliability and security of the BES.
No
The new definitions do not add clarity, but rather confusion and complexity. Entities will be better served by describing the connectivity to their assets and how the entity manages security and reliability of those assets. Entities should explain how they mitigate risk and manage assets in support of BES reliability.
No
KCP&L, in agreement with SPP, offers the following comments. Item 1.2 in Attachment 1 contains requirements already covered in other standards. An authorized user will be on the entity’s list required by CIP-004-6 Requirement 4. Thus, Item 1.2 is not needed. Also, this standard does not define when actions should take place. Clarification is needed and should be placed for industry vote on requirements addressing a Vendor’s Transient Cyber Assets.
Yes
No
KCP&L, in agreement with SPP comments, offers the following comments. While additional time to complete tasks resulting from changes in the standard is welcome, the number of dates to manage is not. There should be one date for High and Medium Impact BES Cyber Assets and their accompanying devices and one for Low Impact BES Cyber Assets and associated devices. We would recommend that the latest date for each grouping be chosen as a new effective date for all requirements.
Yes
No

Group
Florida Municipal Power Agency
Carol Chinn
Yes
SMUD does suggest an important edit to Attachment 1, Element 1 to clarify the obligation. The posted language requires “Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:…” Literal reading of this obligation means that entities are required to perform security awareness on a specific 15 month cycle. To align this obligation with that of CIP-004-5, R1, Part 1.1, SMUD requests the following edit: “Each Responsible Entity shall reinforce, AT LEAST ONCE every 15 calendar months, its cyber security practices, using one or a combination of the following methods.” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle.
Yes
FMPA supports EEI’s comment regarding the definition of a LEAP: The definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation: In the Guidelines and Technical Basis for CIP-003-6, on page 42 of 49 where LEAP is described, move the sentence “LEAP are not to be considered EACMS…” to create a second paragraph and add “However a LEAP can be implemented within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself.”
No
FMPA supports EEI’s comment regarding Attachment 2 of CIP-010-2: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped.
Yes
FMPA supports SMUDs comments regarding Transient Cyber Assets and Removable Media: SMUD agree with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. However, SMUD is concerned with starting the definition of Removable Media with the capitalized “Media” considering that “Media” is itself not a defined term. SMUD recommends an edit to resolve this concern: Removable Media: One or more media directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, or access data. Removable

Media are not Cyber Assets. 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.
Yes
FMPA supports SMUDs comments for CIP-006-6: SMUD agrees and supports the proposed implementation plan deadlines for CIP-003-6, R2. SMUD appreciates that the SDT has provided a tiered approach to the implementation of physical security and electronic access controls. SMUD believes that even with the tiered approach to the implementation plan, entities are not restricted from implementing both controls in parallel. Considering the diverse nature of the facilities and systems, SMUD believes the additional compliance time as well as the tiered approach provides entities the needed flexibility to evaluate their physical security and system capabilities to effectively apply the new requirements. There are possibilities that physical modifications will need to be made to facilities to deploy the necessary controls to restrict physical access. Additionally, to deploy a Low Impact Electronic Access Point, it is possible that certain systems or computer network architectures may need to be modified to accommodate the additional of an access point.
No
The SDT has done an excellent job of addressing the IAC language along with their outreach and addressing stakeholder comments. FMPA can agree with the removal of the IAC language, but unfortunately, the current RSAWs do not provide enough clarity and guidance on compliance expectations to understand if “zero tolerance” concerns have been addressed. There is substantive work that needs to be done on the RSAWs, especially in light of the removal of the IAC language and the fact that RAI program documents have just been recently released and RAI is in early implementation stages. It’s not clear that RAI will address the “zero tolerance” concerns since there is processing and reporting required for 100% of non-compliance. More clarity around the RAI program may address this but it’s not clear at this point. The RSAWs are also a tool to address this matter.
Yes
FMPA’s negative votes are due to the current condition of the RSAWs and the status of RAI implementation. We expect that affirmative votes can be cast if : a. Compliance staff collaborates with the SDT on the RSAW revisions for the next posting that will significantly improve the RSAWs and b. if more clarity is communicated around how RAI addresses “zero tolerance”. FMPA also supports EEI’s comments regarding CIP-007-5: CIP-007-6 R2: Can you violate 2.3 while you meet 2.4? If you identify a patch within 35 days of evaluation and create a dated mitigation plan that says 8 months, but then 2 months later, the implementation of the patch is delayed a month because you can’t take the system down, the plan under 2.3 is no longer valid and you cannot revise it under 2.3 since 35 days have passed; however, under 2.4 you can revise the plan so 2.4 is not violated. Is 2.3 violated in this case?
Individual
Cliff Johnson
Consumers Energy Company

No
We agree with all except the two items below: Not as written specific to CIP-003-6 Attachment 1 numbers 3 and 4.7. Number 3 has the potential to create significant undue burden on entities. This language begins to treat Low Impact assets as if they could have some sort of significant impact on the BES and begins to approach the compliance activities that are applicable to more significant Medium and High Impact assets. Many entities own a significant number of geographically dispersed Low Impact assets with a multitude of cyber asset types making compliance with this language very time and resource intensive. If this level of compliance activities is mandated, the associated implementation deadline would need to be significantly delayed. This also increases the risk of losing focus on the Medium and High Impact assets. Number 4.7 requires updating the plan within 180 days after a test or actual incident without mention of a need for a change being identified that would drive the update. What update is an entity expected to make if the plan is well designed and the test or response to an actual incident was completely successful? We suggest modifying 4.7 to require the update of the plan when corrections or improvements are identified during a test or response to an actual incident.
Yes
Yes
Yes
No
Not as written specific to CIP-003-6 Attachment 1 number 3, it needs to be adjusted according to entity feedback.
Yes
No
Individual
Rich Salgo
NV Energy
No
The SDT made significant improvements to the language and the structure of these Requirements. There remain a few inconsistencies and clarification items that are potential trouble spots which necessitate a negative ballot. These are listed below: Attachment 1: The language in Element 1 “using one or a combination of the following” is inconsistent with the Element 2 language “through one or more of the following.” We recommend the SDT change the language in Element 1 to “through one or more of the following.” CIP-003-6 Requirement

R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” We recommend the SDT change Attachment 1, Element 2 to “Physical security controls” to be consistent with the language of the standard. This would extend to all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs). Attachment 1, Element 4.7 assumes the response plan will always need updates, which may not be the case. We recommend to add the important clarifier “if needed,” after the words “180 calendar days.” Beyond the changes outlined above, we note that the nature of the changes for CIP-003-6 to accommodate the Commission’s directive on Low Impact cyber assets hinge on the new terms introduced in this posting (LERC and LEAP). As noted in the following question response, we are advising several important changes to these terms. Without some assurance that these changes will be adopted, we cannot determine the suitability of CIP-003-6 and therefore cannot cast an affirmative ballot amid the uncertainty of the resolution on these definitions.
No
LEAP: The use of the word “allows” in the LEAP definition is not compatible with the use of an unmanaged hub. Such an unmanaged hub, which does not support any access controls and may be merely acting as a central connecting point, would be considered an interface that “allows” Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs and would therefore be problematic for compliance with this requirement. We recommend the SDT change the word “allows” to “controls”, which will therefore exclude unmanaged hubs from any requirements involving LEAPs. LERC: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. We recommend to change the exclusion sentence to: “Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).”
No
In Attachment 1, the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and (2) it is already implied by the language of 1.2 and 1.3. The language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which amounts to an “authorization.” The redundancy creates uncertainty in the interpretation of the standard, and could call into question whether a second step of authorization is prescribed. We recommend the removal of the word “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 as well as appropriate clarification in the Guidelines and Technical Basis. In Attachment 2, Element 3.2 is too restrictive and does not serve to mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. We recommend that the SDT change “scan

Removable Media outside of the BES Cyber System” to “use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code.”
Yes
Yes
We generally support the implementation plan as a whole; however, there appears to be a conflict between the date for which LEAPs are to be identified under Element 3 and the date that physical access controls are to be applied to these LEAPs (Sept 1, 2018 for the former; April 1, 2018 for the latter).
Yes
Individual
Kara Douglas
NRG Energy
Yes
Yes
Yes
Yes
Yes
Yes
suggest the SDT remove all “shalls” in the Attachment and refer to it as a list of items to include in a program.
Yes
For Version-X proposed changes: suggest the SDT remove all “shalls” in the Attachment and refer to it as a list of items to include in a program.
Group
SPP and specific Members
Lesley Bingham
Yes

No
The new definitions do not add clarity, but rather confusion and complexity. There is audit risk for an entity if their interpretation of these terms differs from that of their Compliance Enforcement Authority. Most entities will be better served by describing the connectivity to their assets through a policy statement which can be crafted to address a specific location.
No
Item 1.2 in Attachment 1 contains requirements already covered in other standards. An authorized user will be on the entity’s list required by CIP-004-6 Requirement 4. Thus, Item 1.2 is not needed. Also, this standard does not define when actions should take place. Should a Vendor’s Transient Cyber Asset and processes be reviewed every time the Vendor touches and entity’s systems? Annually? Once and then not again? Clarification is needed on this point.
Yes
No
While additional time to complete tasks resulting from changes in the standard is welcome, the number of dates to manage is not. There should be one date for High and Medium Impact BES Cyber Assets and their accompanying devices and one for Low Impact BES Cyber Assets and theirs. We would recommend that the latest date for each grouping be chosen as a new effective date for all requirements.
No
The removal of the IAC language has been closely tied to the proposed Reliability Assurance Initiative (RAI). While that program can, ideally, allow for auditors to review an entity’s controls which will identify, assess, and correct issues, the RAI program is not complete and has not been used in the audit and enforcement process. Simply put, this requires a significant amount of trust. The IAC language provides a more clear path and boundaries for auditors.
No
Individual
Brenda Hampton
Luminant Energy Company, LLC
Agree
Luminant Generation Company, LLC
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No

MMWEC respectfully submits the following suggestions for clarifying and improving the CIP-003-6 Attachments 1 and 2. Attachment 1, Element 1: change "once every 15 calendar months" to "at least once every 15 calendar months." In Attachment 2, Element 1 - change "once every 15 calendar months" to "at least once every 15 calendar months" or delete "once every 15 months. Attachment 1, Element 2: It is not clear whether the phrase "based on need" refers to the need to restrict physical access or the need to allow certain physical access. Does it mean that entities are required to restrict access by default and justify any allowed access? The Attachment 2 example for Element 2 indicates that an entity must describe the operational need for physical access, but also contains the confusing phrase "restrictions cited above are based on need" implying that it is the "restriction" that must be justified and documented. Please clarify. Attachment 1, Element 4.1: Change "Identification, classification, and response to Cyber Security Incidents" to "Identification and classification of Cyber Security Incidents." Delete “response” because "response" is a sub-set of "incident handling" which is required by Element 4.4. Attachment 1, Element 4.3: Since testing of the Cyber Security Incident Response Plan is required only every 36 months, entities should be required to ensure that individuals are aware of their response roles through more frequent training or review of their responsibilities. Consider modifying Element 4.3 to require those groups and individuals to review their roles and responsibilities for Cyber Security Incident response at least once every 15 months. Attachment 2, Element 3: Change "(e.g. IP addresses, ports, services)" to "(e.g., by restricting IP addresses, ports and/or services)" and move this phrase to follow "deems necessary" later in the same sentence. It is not clear from the current wording whether an entity must restrict using all of the example attributes.
No
MMWEC is concerned with the use of the phrase “low impact BES Cyber System.” Shouldn’t this be “BES Cyber Systems associated with Low Impact assets?” For the definition of LERC, consider changing “Communication protocols created…” to “Communication using protocols created…”
No
MMWEC respectfully submits the following suggestions for improving the CIP-010-2 Attachment 1. CIP-010-2, Attachment 1 should be limited to requiring control objectives not specific controls. Bullets are example controls and should not be include in Attachment 1 requirements. These examples should be moved to Attachment 2 or to guidance. CIP-010, Attachment 1, Element 1.1 is a method of compliance rather than a control objective. It is unnecessary and should be deleted from Attachment 1 and moved to guidance. The following is recommended wording for control objectives for Attachment 1 Elements 1.3, 1.4, 1.5, 2.1 and 2.2: "1.3 - Each Responsible Entity shall mitigate security vulnerabilities on Transient Cyber Assets." “1.4 Each Responsible Entity shall mitigate the risk of introduction of malicious code (per Transient Cyber Asset capability.)” “1.5 Each Responsible Entity shall mitigate the risk of unauthorized use of Transient Cyber Assets.” “2.1 Each Responsible Entity shall mitigate the risk of security vulnerabilities (per Transient Cyber Asset capability.)” “2.2 Each Responsible Entity shall mitigate the risk of introduction of malicious code (per Transient Cyber Asset capability.)” Using control objectives for elements 2.1 and 2.2, element 2.3 is redundant and should be deleted from Attachment 1. CIP-010, Attachment 1, Element 3.2 –

Change entire element to "Each Responsible Entity shall mitigate the risk of introduction of malicious code associated with the use of Removable Media." The examples of how to do this (i.e., scanning) could be included in Attachment 2 or guidance.
No
It not clear whether a Cyber Asset that meets the definition of BES Cyber Asset could be categorized as a Transient Cyber Asset (and require only the controls for Transient Cyber Assets) if it is connected for less than 30 days. To clarify that it cannot be classified as a Transient Cyber Asset, MMWEC recommends adding the following sentence to the end of the definition of Transient Cyber Asset,: "A Cyber Asset that meets the definition of BES Cyber Asset shall not be categorized as a Transient Cyber Asset." Another approach to this issue would be to restrict application of the Transient Cyber Asset category by changing the last sentence to “Transient Cyber Assets are limited to Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.”
Yes
Yes
No
Group
Edison Electric Institute (EEI)
Melanie Seader
No
EEI appreciates the efforts of the Standard Drafting Team (SDT) in revising CIP-003-6 to meet stakeholder concerns. We believe CIP-003-6 is close, but not yet ready for final ballot due to the following comments. We encourage the SDT to consider all of these comments carefully as our members have worked hard to explain their concerns in these comments as well as provide specific recommendations to help the SDT. Comment 1.1: CIP-003-6 Rationale for Requirement R2: “Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised.” Aggregating low impact BES Cyber Systems across multiple assets does not reflect a true risk-based assessment and therefore this sentence is not accurate. Recommendation 1.1: Delete this sentence. Comment 1.2: CIP-003-6 – Attachment 1: The language in Element 1 “using one or a combination of the following” is inconsistent with the Element 2 language “through one or more of the following.” Recommendation 1.2: Change the language in Element 1 to “through one or more of the following.” Comment 1.3: CIP-003-6 – Attachment 1: CIP-003-6 Requirement R1, Part 1.2, Subpart 1.2.2 “Physical security controls” is inconsistent with Attachment 1, which uses “Physical access controls.” Recommendation 1.3: Change Attachment 1, Element 2 to “Physical security controls” to be

consistent with the language of the standard. Please edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, RSAWs) to make them consistent with the CIP-003-6 R1 language. Comment 1.4: CIP-003-6 Requirement R2 ends with “include the elements in Attachment 1,” although the first sentence in Element 1 says “include each of the elements provided below” the actual “elements” are not labelled “elements” as in Attachment 2, which references the elements in Attachment 1. Recommendation 1.4: Add “Element” before each numbered bullet in Attachment 1, using the same format as Attachment 2 uses. This would also be helpful for Attachment 1 in CIP-010-2. Comment 1.5: The “(LERC)” and “(LEAP)” acronyms are missing in Element 2, 3, and 3.1, which makes it harder to identify the use of these defined terms in these elements. Recommendation 1.5: Add the “(LERC)” and “(LEAP)” to elements 2, 3, and 3.1 to make it easier to identify the terms. Comment 1.6: CIP-003-6 Attachment 1, Element 4.7 assumes the response plan will need updates, which may not always be the case. Recommendation 1.6: Add “, if needed,” after “180 calendar days.” Comment 1.7: CIP-003-6 Attachment 2 and Guidelines and Technical Basis for Element 2: Attachment 2 (examples of evidence) for Element 2 provides card key and special locks as examples of access controls; however, the Guidelines and Technical Basis for Element 2 states “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” These inconsistencies make the language of the standard in Attachment 1 vague and unclear. Recommendation 1.7: Include “perimeter controls” under Element 2, Attachment 2 in the example: “(e.g., card key, special locks, perimeter controls). Comment 1.8: CIP-003-6 Guidelines and Technical Basis, Requirement R2 Attachment 1 bold text subtitles on page 32: The subtitles are inconsistent with the element language in Attachment 1. Recommendation 1.8: Change the subtitle language to “Requirement R2 Attachment 1 – Cyber Security Awareness” and “Requirement R2 Attachment 1 – Physical Security Controls” (see Comment and Recommendation 1.3 above).
No
Comment 2.1: Use of “allows” in the LEAP definition does not allow for the use of an unmanaged hub. An unmanaged hub, which does not support access controls and may be merely acting as a central connecting point, could be considered an interface that “allows” Low Impact External Routable Connectivity and therefore would be improperly characterized as a LEAP. Element 3.1 of Attachment 1 CIP-003-6 requires inbound and outbound access control for LEAPs, which are not supported by unmanaged hubs. Recommendation 2.1: Change “allows” to “controls” to allow for the use of unmanaged hubs as appropriate. Please also make sure this is changed in the Guidelines and Technical Basis and anywhere else the LEAP definition is provided. Comment 2.2: Because the acronyms LEAP and LERC are used to help simplify the terms defined and used in the standard, it would help to include the acronyms each time the terms are spelled out in full in the definitions and in the standards and related guidance. Recommendation 2.2: Insert the acronyms “(LERC)” and “(LEAP)” as they are spelled out in the definitions. Comment 2.3: In the LERC definition, example exclusions are listed. The need for the exclusions provided in the examples is unclear. Recommendation 2.3: Change the exclusion sentence to: “Point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication

<table>
<tr><td>protocols for time sensitive protection and/or control functions are excluded (example protocols include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).” Also, clarify in the Guidelines and Technical Basis for CIP-003-6 that the exclusion is intended to include point-to-point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time sensitive protection and/or control functions. Comment 2.4: The definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the Low Impact BES Cyber System Electronic Access Point (LEAP) rather than the device containing the NIC. Therefore it is possible to have a NIC port inside a High or Medium Impact BES Cyber System Electronic Access Perimeter (ESP) in an Electronic Access Control or Monitoring System (EACMS). The LEAP does not need to be in an EACMS, but it can be. Recommendation 2.4: In the Guidelines and Technical Basis for CIP-003-6, where LEAP is described, move the sentence “LEAP are not to be considered EACMS…” to create a second paragraph and add “However a LEAP can be implemented within the same cyber asset that is serving the function of EACMS or EAP for a Medium or High BES Cyber System. This is possible because a LEAP is the interface on the controlling cyber asset (e.g., a firewall or router) and not the cyber asset itself.” Comment 2.5: Based on the LERC definition and the CIP-003-6 Guidelines and Technical Basis for Requirement R2 Attachment 1 – Electronic Access Controls, the following scenario is unclear: {Low impact BES Cyber System (e.g., control system) ---- |1| ---- Cyber Asset (e.g., data historian) ---- |2|} ---- Location X Where: {} represents the asset/site boundary, |1| represents a firewall or electronic access point (in this case firewall 1), and ---- represents a bi-directional routable communication Based on the language of the definition and CIP-003-6 it is unclear whether there is a LERC and LEAP in this scenario and if there is LERC, which firewall is the LEAP. The Guidelines and Technical Basis for CIP-003-6 say “the electronic access controls should address the risk of using the asset’s LERC to gain access to the low impact BES Cyber Systems.” However, this scenario would require an adversary to gain access to not one but two access points, the firewalls on either side of the Cyber Asset (firewall 2 and then firewall 1) to get access to the low impact BES Cyber System. Whereas, the examples provided all show one access point, the LEAP, which requires controls. Recommendation 2.5: Add this scenario to the CIP-003-6 Guidelines and Technical Basis, clarify that there is a LERC and allow the Responsible Entity to have the flexibility choose the LEAP, either firewall 1 or firewall 2.</td></tr>
<tr><td>No</td></tr>
<tr><td>EEI appreciates the efforts of the Standard Drafting Team (SDT) in revising CIP-010-2 to meet stakeholder concerns. We believe CIP-010-2 is close, but not yet ready for final ballot due to the following comments. We encourage the SDT to consider all of these comments carefully as our members have worked hard to explain their concerns in these comments as well as provide specific recommendations to help the SDT. Comment 3.1: CIP-010-2 R4: The placement of “under CIP Exceptional Circumstances,” is awkward. Recommendation 3.1: Move “under CIP Exceptional Circumstances” up in the sentence, such that it reads “…shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s)…” Comment 3.2: CIP-010-2 Attachment 1: The use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary because (1) it already appears in the underscored text for 1.2 and 3.1, and 2) it is implied by the language of 1.2 and 1.3. The language of 1.2</td></tr>
</table>

and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization. The redundancy creates uncertainty in the interpretation of the standard. It could be interpreted to imply a second step in addition to the R4 plan. In other words, in addition to the R4 plan for Transient Cyber Assets and Removable Media, which includes the 1.2 and 3.1 authorization elements, the Responsible Entity must also have a separate, formal approval process to identify authorized users, authorized locations, and authorized uses for Transient Cyber Assets and a separate formal approval process to identify who is authorized to use and where they are authorized to use Removable Media. We believe the intent of the Standards Drafting Team is that the plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address these authorization elements. This flexibility will allow the Responsible Entity to either write a plan that specifically defines who is authorized to use the Transient Cyber Asset(s) for which uses and locations or include a separate authorization process, which may include a formal approval process, in the plan that identifies the users, locations, and uses authorized for the Transient Cyber Asset(s). It will also give the Responsible Entity the same flexibility for Removable Media authorizations. This flexibility is particularly needed for Responsible Entities that rely on contractor use of Responsible Entity managed Transient Cyber Assets and Removable Media who have less control over the contractor, i.e., the control is defined by a service agreement or contract. Giving the Responsible Entity flexibility on how to define the authorization process will allow them to align these requirements with their vendor contracts. Recommendation 3.2: Remove “Authorized” from 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2. Also, clarify in the Guidelines and Technical Basis under Element 1.2 and 3.1 that the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 does not require a formal approval process for each user, location, and use of the Transient Cyber Asset (or Removable Media), but gives the Responsible Entity the flexibility to develop an authorization plan that either directly defines authorization or requires a specific authorization process. This allows Responsible Entities to align their Transient Cyber Asset and Removable Media authorizations with their vendor contracts for use of Responsible Entity managed Transient Cyber Assets. Comment 3.3: CIP-010-2- Attachment 1 Elements 1 and 2 are grouped by whether a Transient Cyber Asset is owned or managed by the Responsible Entity or by a vendor or contractor. The intent of this grouping is good because it considers the level of control by the Responsible Entity. However, the actual groupings could result in a Transient Cyber Asset that falls under both element 1 and 2. For example, if a Responsible Entity owns the Transient Cyber Asset, but a contractor manages its use under a service management contract. Another scenario is that the vendor owns the Transient Cyber Asset, but the Responsible Entity manages it. For these scenarios, it is unclear whether the Responsible Entity should include element 1 or 2 or both elements in their R4 plan(s). Recommendation 3.3: Remove “Owned or” from elements 1 and 2. Comment 3.4: CIP-010-2 - Attachment 1, Element 2.3: “Responsible Entities shall determine whether additional mitigation actions are necessary…” requires a statement that says no additional mitigation measures were identified as necessary, which creates an unnecessary administrative burden. Also, Element 2.3 is an element that should be addressed by the R4 plan for Transient Cyber Assets and Removable Media, the way Element 2.3 is written makes it look like a requirement rather than a plan element, which also causes confusion as to the frequency of review for elements 2.1 and 2.2. Element 2.3 as written suggests that a Responsible Entity must use the 2.1 and 2.2 mitigation methods prior to each connection of a vendor-owned Transient Cyber Asset in order to determine whether additional mitigation measures will be needed. This can be overly burdensome and unnecessary when a vendor is moving from system to system in a single day. Recommendation 3.4: Add “necessary” before “such actions.” Also, clarify in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how to manage vulnerability and malicious code reviews of their vendors or contractors and require additional mitigation actions. For example, one entity may require a vendor to plug a Transient Cyber Asset into a kiosk to scan for vulnerabilities and malicious code before each connection. However, this approach may not be feasible for all entities, so defining a process to initially and periodically check and audit vendor/contractor processes for vulnerability and malicious code mitigation. Specifically, “prior to connecting the vendor- or contactor-owned Transient Cyber Asset” does not require that 2.1, 2.2, and 2.3 before each connection, but that the Responsible Entity should define a process to manage the use of vendor- or contractor- managed Transient Cyber Assets to mitigate vulnerabilities and malicious code. Comment 3.5: CIP-010-2 – Attachment 1, Element 2.3 : A Transient Cyber Asset may be owned by the Responsible Entity and managed by a vendor or owned by the vendor/contractor and managed by the Responsible Entity. Therefore the use of “vendor- or contractor-owned” in 2.3 is not consistent with these scenarios (see Comment and Recommendation 3.3 above). Recommendation 3.5: Change “owned” in 2.3 to “managed.” Comment 3.6: CIP-010-2 – Attachment 2, elements 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, and 3.2: The use of “mitigate” and “mitigation” should be explained to make it clear to auditors that mitigate/mitigation means to reduce risk and does not mean that every vulnerability must be addressed and every piece of malicious code detected and stopped. Recommendation 3.6: Make it clear in the Guidelines and Technical Basis that “mitigate” and “mitigation” does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system that the Transient Cyber Asset or Removable Media is used on. Also, it may be impossible to detect every piece of malicious code. Mitigation is meant to reduce security risks, but elimination of all risk is impossible. Comment 3.7: CIP-010-2 – Attachment 2, Element 3.2: This requirement is too restrictive and does not mitigate risks. Capabilities exist for embedded, real-time virus scanning and encryption on USB drives, but Element 3.2 prevents their use. Also, 3.2 does not require the Responsible Entity to take any action other than scanning Removable Media at some point in time. Recommendation 3.7: Change “scan Removable Media outside of the BES Cyber System” to “use a method to scan Removable Media for malicious code and a procedure to respond to detected malicious code.” Comment 3.8: CIP-010-2 – Attachment 2, Element 1.2: The second sentence under Element 1.2 is a restatement of Attachment 1, Element 1.2 and is not an example of evidence. Recommendation 3.8: Remove the second sentence under Attachment 2, Element 1.2: “The documentation must…” to keep the text in Attachment 2 focused on examples of evidence and not include requirements. Comment 3.9: Guidelines and Technical Basis for R4,

Attachment 1, Element 1.1: Inventories of Transient Cyber Assets is allowed by individual or group – individually or by asset type, therefore language under Element 1.1 should be consistent, allowing inventory of devices or device type. Recommendation 3.9: Add “or device types” to the second sentence: “pre-authorize and inventory of devices or device types or authorize devices or device types at the time of connection or use a combination of these methods.”
No
Comment 4.1: Transient Cyber Asset Definition: The “and” in the parenthesis after “A Cyber Asset,” is confusing. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. Also, the parenthetical for the examples is misplaced; it refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and, therefore, unclear as to which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, “directly connected” may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Recommendation 4.1: Change the definition for Transient Cyber Asset to: “A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) 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.” Also, if the intent is for the Transient Cyber Asset definition to apply to both routable and non-routable communications, clarify this in the Guidelines and Technical Basis for CIP-010-2.
Yes
The timeframes in the implementation plan are reasonable and appropriate; however, we have the following comment to help clarify a source of confusion among Responsible Entities: Comment 5.1: CIP-003-6, Attachment 1, Element 2 compliance date of April 1, 2018: According to the Implementation Plan, the Element 2 physical access controls must be applied to LEAPs by April 1, 2018; however, the LEAPs are identified under Element 3, which must be applied by September 1, 2018. This requires Responsible Entities to identify LEAPs before April 1, 2018, which may be unclear under the Implementation Plan. Recommendation: Clarify in the Implementation Plan that the LEAPs must be identified before April 1, 2018 in order to apply physical access controls to them by April 1, 2018.
Yes
No
Individual

Thomas Foltz
American Electric Power
No
The modification of CIP-003-6 R1 exceeds FERC's order to add "objective security controls" to R2 in the existing approved standard. The inclusion of item 1.2 in requirement R1 to create a cybersecurity policy adds an additional burden on Entities that have facilities with low impact BES Cyber Systems. The previous draft only required the documentation and implementation of cyber security plans under R2 that addressed the defined items. The additional compliance burden of creating and maintaining another policy document under R1 will not provide an appreciable increase in cyber security to the BES. The documentation and implementation of cyber security plans that include “objective criteria” to evaluate the sufficiency of an entity’s protections as ordered by FERC should be sufficient. AEP suggests the SDT revert to the original wording of R1 and add the "objective criteria" to R2. In CIP-003-6, Attachment 1 Item #2, the language is more prescriptive than the wording for Medium Impact BES Cyber Systems without External Routable Connectivity. AEP suggests the wording be modified to provide a level of flexibility for low impact BES Cyber Systems that is commensurate with their potential impact to the BES. For example, regarding physical security, it may be difficult to prove compliance with this section given the options provided. This may necessitate installing card readers on over 1,000 substations. AEP suggests removing the prescriptive bullet points, “Access controls; Monitoring controls; or Other operational, procedural, or technical physical security controls,” and similar prescriptive language. Separating the security controls into Attachment 1 and what appears to be a combination of examples, measures, and evidence into Attachment 2 in CIP-003-6 is confusing and a deviation from the formatting of the other CIP standards. AEP suggests that the wording be transferred to a table similar to the rest of the CIP standards. Regarding the CIP-003-6 R2 rationale “Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised,” aggregating Low Impact BES Cyber Systems across multiple assets does not reflect a true risk-based assessment. Rather, the existing Standard focuses on individual Assets that contain Low Impact BES Cyber Systems. FERC did not order a change in this philosophy. AEP suggests deleting this sentence.
No
The definitions create confusion where they refer to "asset" when it appears the term should be "facility." AEP suggests changing the second lowercase use of the word "asset" in each definition to be "facility."
No
Separating the security controls into Attachment 1 and what appears to be a combination of examples, measures, and evidence into Attachment 2 in CIP-010-2 is confusing and a deviation from the formatting of the other CIP standards. AEP suggests that the wording be transferred to a table similar to the rest of the CIP standards. AEP is concerned with the use of the term “security vulnerabilities,” which AEP believes is a broader term than, e.g., security

patch management or malicious code prevention utilized in CIP-007. AEP disagrees with the implication that a Responsible Entity would be required to mitigate “security vulnerabilities,” which may require Responsible Entities to monitor the National Vulnerability Database and address all vulnerabilities published over a day, week, month, or year where there are currently 65,268 security vulnerabilities. Large corporate networks are not able to address all security vulnerabilities in real time. How can this be expected on Transient Cyber Assets that may or may not have External Routable Connectivity? AEP suggests reverting to, e.g., security patch management or malicious code prevention rather than “security vulnerability mitigation.” This would align with the CIP-007 requirements and would be a more reasonable and manageable requirement. The existence of External Routable Connectivity should also be taken into consideration when revising this requirement to ensure the CIP standards treat devices commensurate with their risk profile. Element 3.2 of Attachment 1 is too restrictive. This presumes the scanning takes place on another system. The capabilities exist today to have embedded virus scan and encryption on USB drives. This should not require the scanning of the USB drive on a system outside the BES Cyber System as the scanning is taking place in real time by the applications running on the USB drive itself. Consider how this requirement relates to CIP-007 R3, where a Responsible Entity is required to “deploy method(s) to deter, detect, or prevent malicious code.” The methods deployed on a BES Cyber System would cover the threat of malicious code introduced via Removable Media. There is more than one layer of security controls that protects a BES Cyber System from the threat of malicious code introduced via Removable Media. Physical security, user account management, BES Cyber System software patch management, and BES Cyber System malicious code prevention, for example, are all required and would provide significant threat mitigation against the introduction of malicious code via Removable Media. The technology to prove compliance with the scanning requirement prior to connecting Removable Media to a BES Cyber System is not readily available. Systems are not equipped to provide the granularity as to what USB drive, CD/DVD, memory card, or floppy disk has been plugged into it. AEP suggests revising the requirement to allow the use of more advanced Removable Media with the ability to scan for malicious code during use without the burden of additional scanning requirements on external systems. Regarding Element 1.2 of Attachment 1, authorization and verification of users on Transient Cyber Assets is not practical when the Transient Cyber Assets do not have External Routable Connectivity or are not connected to a BES Cyber System with External Routable Connectivity. The authorization and verification of users, locations, and uses of Transient Cyber Assets without External Routable Connectivity would be a paper exercise with no technical means of enforcement or logging. As a result, without External Routable Connectivity, it is not possible to verify that the risks of Transient Cyber Assets were properly mitigated. This authentication would be a significant administrative burden with negligible reliability benefit (similar to those Requirements removed during the Paragraph 81 effort) when considering the significant number of BES Cyber Systems and Assets that will be in scope. AEP suggests that the element be modified to only require the authorization of users and approved transient hardware for the ESP accessible via a network to high or medium impact BES Cyber Systems with External Routable Connectivity. Regarding Element 2 of Attachment 1, vendors and contractors are not subject to CIP requirements themselves. A

Responsible Entity cannot force a vendor or contractor to adhere to the requirements of this element. Use of specialized vendor expertise and tools may be limited such that BES reliability would be impacted. Imposing this requirement on vendors and contractors is in fact more restrictive than medium impact BES Cyber Systems with External Routable Connectivity. AEP suggests removing Element 2 in its entirety.
No
Regarding Transient Cyber Assets, the 30 day timeframe prevents a Responsible Entity from being able to consider a device that is temporarily connected to the BES Cyber System as part of the BES Cyber System, and it is arbitrarily beyond what was ordered by FERC. AEP suggests removing the 30 day timeframe to reduce the amount of tracking Responsible Entities must do with respect to these devices.
No
AEP is concerned that the tiered approach to effective dates is overly complicated and will create confusion, especially for large entities. AEP suggests streamlining the implementation date to the latest date proposed in the Version X and Version 6 implementation plans.
Yes
While AEP supports this approach, AEP is also expecting that NERC and the regions will continue to implement the Reliability Assurance Initiative to embody the spirit of the "IAC" language. For example, AEP expects to continue to see self-logging privileges granted for lower risk items pursuant to the criteria set forth by the RAI.
Yes
AEP recommends that the drafting team not include a prescriptive approach in the proposed attachments in CIP-003 and CIP-010. Such prescriptive approaches unreasonably restrict the Responsible Entities from defining their own programs. For those items where the drafting team has proposed prescriptive approaches, AEP recommends removing them from an "Attachment" format and including them in tabular format as requirements similar to the remainder of the CIP Requirements without the prescriptive elements of the steps Responsible Entities are required to take. While AEP understands that this approach creates a baseline for cybersecurity in the industry, it is also concerned about the security of prescribing one approach for all companies within a critical infrastructure sector which could increase the likelihood of a successful attack across a broad front. AEP recommends including the exclusion from the defined term “Low Impact External Routable Connectivity” for transfer trip communications into the defined term “External Routable Connectivity.” Exclusion wording from LERC definition: “Communication protocols created for Intelligent Electronic Device (IED) to IED communication for protection and/or control functions from assets containing low impact BES Cyber Systems are excluded (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).” There is no mandated timeframe to address the low impact and transient cyber device directives. AEP urges the SDT to take the time necessary to ensure that the requirements achieve the necessary reliability benefit and that there is broad-based industry support.
Individual
Barry Lawson

National Rural Electric Cooperative Association (NRECA)
In CIP-003-6, R2, it states “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.” NRECA strongly supports this statement. In order to help registered entities to better understand how this “Note” can be used in demonstrating compliance, NRECA requests that the SDT explain and provide examples on how registered entities can comply with this standard without providing a list for audit purposes. NRECA requests that the SDT provide a detailed justification for the most recent additions of 4.6 and 4.7 to CIP-003-6, Attachment 1. These elements were not included in the first posting of the CIP V5 revisions and they have been added without adequate justification. These two new requirements add additional compliance and administrative burdens compared to the first posting without a demonstration of why they are needed for BES reliability. While NRECA will be voting in the affirmative, we expect the SDT will fully address why these requirements are needed for BES reliability. If this cannot be done, then 4.6 and 4.7 should be removed from Attachment 1.
Yes
Yes
Yes
While NRECA supports the proposed Implementation Plan, we request that the SDT consider syncing up deadlines for the physical and electronic access control requirements so that both are required by September 1, 2018.
Yes
NRECA supports the Version X package of revisions. However, we are very hopeful that the SDT can successfully complete revisions to CIP V5 that address FERC’s four directives by the Feb 2015 filing deadline. Having the four directives addressed by the filing deadline is critical to achieving a steady state for the CIP standards.
Yes
NRECA appreciates the efforts of the CIP V5 Revisions SDT in addressing this challenging project under very tight time constraints.
Individual
Nathan Mitchell
American Public Power Association
Agree
Scott Saunders - SMUD
Group
Iberdrola USA
John Allen

No
Support EEI comments And The revised structure of CIP-003-6 has made it more cumbersome, and confusing to use. The use of the table in the previous version was effective. Attachment 1 is a list of requirements and should be treated as such within the main body of the standard.
No
Support EEI comments
No
Support EEI comments AND As written, Attachment 2.3 requires each Entity to review each vendor’s policies/procedures. Recommend changing from “Responsible Entities shall determine whether additional mitigation actions are necessary” to “Responsible Entities may determine whether additional mitigation actions are necessary”
Yes
Support EEI comments
Yes
Yes
No
Group
BC Hydro
Patricia Robertson
No
The cyber security plan elements defined within Attachment 1 are deemed to be too detailed and excessive for Low Impact BES Cyber Assets.
Yes
No
a) BC Hydro recommends a revision to the detailed expectations on the Responsible Entity in relation to Attachment 1, 2 Transient Cyber Asset(s) owned or managed by Vendors or Contractors. It is anticipated that it will not be feasible to actively review and monitor the measures on devices not owned by the Responsible Entity as detailed in Attachment 1, 2. b) BC Hydro recommends a revision to the expectations with regard to Attachment 1, 3 Removable Media. The revision would provide clarity on authorized users (ie is this applicable for vendors as well as the Responsible Entity).
No

BC Hydro requests clarification regarding the language "… directly connected for 30 calendar days or less …" Does this mean if a Responsible Entity has a USB drive plugged in to a BES Cyber Asset continuously for 32 days, that device no longer represents Removable Media?
N/A
Yes
Although BC Hydro overall supports the removal of the IAC language, it will create a zero-tolerance with regards to items of non-compliance. For high risk items this is appropriate however for low risk items the IAC language would be appropriate.
Yes
BC Hydro recommends a definition or guidance be developed with regards to the term "cyber security plan"
Individual
Andrew Ginter
Waterfall Security Solutions Ltd.
No
Almost all USB flash drives, mice, keyboards and other devices contain CPUs and software. Attackers can physically modified such devices to attack the computers to which the devices are connected - see http://www.theregister.co.uk/2011/06/27/mission_impossible_mouse_attack/ for an example. Worse, a malware-infected computer can compromise the software running in some kinds of connected USB devices - see http://www.wired.com/2014/10/code-published-for-unfixable-usb-attack/ for an example. Thus, a USB flash stick or other device whose firmware is compromised while connected to an external computer can cause BES Cyber Assets to malfunction when the USB drive is connected to those assets, either by loading malware on to the BES Cyber Asset, or by issuing incorrect mouse or keyboard commands to the asset. This suggests that USB devices generally should be considered BES Cyber Assets or Transient Cyber Assets, but the Removable Media definition gives USB flash drives as an example of Removable Media. The definitions and examples should make it clearer whether USB keyboards, mice, flash drives and other CPU & software-containing USB devices are BES Cyber Assets, Transient Cyber Assets, or Removable Media, and why those types of USB devices should be classified in this manner.
Group
PacifiCorp

Sandra Shaffer
No
o Need definition modifications completed before voting YES. PacifiCorp also supports the comments of MidAmerican Energy Company regarding dispersed generation resources.
No
o LERC definition: The second sentence uses undefined terms that cause confusion and refers to specific technologies which over time will make the definition obsolete as technologies change. This exception also seems to remove protections indiscriminately rather than addressing the importance of the assets to be protected and finding ways to provide meaningful controls around them without impacting the effectiveness of the protocols in question.
No
o Attachment 1, Element 1.2: Recommend removing ‘Authorized’ because it adds requiring someone to approve/authorize these items. Entities would still be required to “specify” users, locations and use (individually or by group) for each part in Element 1.2. It also should be noted that the physical location that the Transient Device is approved for may not be as relevant as the logical network or cyber system that the Transient Device is used with (i.e. there may be multiple networks available at a particular location and which network it’s used on is more impactful to the Transient Device than the physical location itself). Consider changing element 1.2.2 to specify “network zones or cyber systems, either individually or by group, that the Transient Device may be used with.” o Attachment 1, Element 3.1: Recommend removing ‘Authorized’ because it adds requiring someone to approve/authorize these items. Entities would still be required to “specify” users and locations (individually or by group) for each part in Element 3.1.
Yes
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
Yes
TSGT feels that the “topics” of R1 should reflect the “elements” of Attachment 1 referenced in R2 unless there is a different meaning intended with the different wording. If so, please clarify the difference. One way to do this would be to simply refer to Attachment 1 under R1.2 and remove all the sub-requirements under R1.2.
Yes

Yes
No
TSGT believes that the recent revisions made to the Removable Media and Transient Cyber Asset definitions introduced some unintended ambiguity. Revisions should be made to make it clear what the assets/devices must be connected to, in order to clarify this qualifier of the definition. It is our understanding that the intent of the drafting team was to state "…directly connected… [clause]… to…", where the items after the "to" is what the "Cyber Asset" or "Media" is connected to. One simple solution is to add a comma after the [clause] and before the word "to". Another option is to state the [clause] part after the list of what the "Cyber Asset" or "Media" is connected to. Here is a suggested revision to how the definition for Removable Media might read: A Cyber Asset, directly connected to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field and Bluetooth communication) ; and connected for 30 consecutive calendar days or less, capable of transmitting executable code. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Yes
The timelines are fine, but written in a very convoluted way. It would be helpful to state them more succinctly.
Yes
No
Group
Bonneville Power Administration
Andrea Jessup
BPA supports SMUD's comments with the exception of Questions 2 and 5.
Yes
BPA supports SMUD's comments.
Yes
BPA believes that reusing the term Access Point within the new definition of Low Impact BES Cyber System Electronic Access Point leads to confusion with existing medium and high definitions.
Yes
BPA supports SMUD's comments.
Yes
BPA supports SMUD's comments.
Yes

BPA disagrees with the tiered implementation timeline as currently proposed. BPA believes more time is required to create practices and procedures to implement the policy effectively. BPA suggests that policy (CIP-003-6, R1, part 1.2) be implemented prior to other requirements (CIP-003-6, R2 and CIP-003-6, R2 Attachment 1, items 1-4).
Yes
BPA supports SMUD's comments.
Yes
BPA disagrees with the CIP-007-6 R1.2 expansion of scope to non-programmable communication components and proposes re-alignment to R1.1. To increase the potential for managing compliance to this requirement, BPA requests additional guidance defining the specific nonprogrammable communication components located inside both a PSP and an ESP. This clarification is requested in addition to what has already been added via the Guidelines illustration and Technical Basis section.
Individual
Randi Nyholm
Minnesota Power
Agree
Minnesota Power supports comments submitted by EEI related to CIP-003-6, CIP-010-2 and the implementation plan.
Individual
Joe Tarantino
Sacramento Municipal Utility District
Yes
SMUD agrees and supports the changes that were made to CIP-003-6, R2 including the use of Attachment 1 and Attachment 2. SMUD does suggest the following changes: The posted language in Attachment 1, Element 1 requires “Each Responsible Entity shall reinforce, once every 15 calendar months, its cyber security practices, using one or a combination of the following methods:…” Literal reading of this obligation means that entities are required to perform security awareness on a specific 15 month cycle. To align this obligation with that of CIP-004-5, R1, Part 1.1, SMUD requests the following edit: “Each Responsible Entity shall reinforce, at least once every 15 calendar months, its cyber security practices, using one or a combination of the following methods.” This establishes that the obligation of security awareness just needs to occur at least once over a 15 calendar month cycle. The posted language in CIP-003-6, R1, Part 1.2, Subpart 1.2.2 uses “Physical Security Controls” to define the policy obligation. However, in Attachment 1, Element 2, “Physical access controls” is used. SMUD recommends Attachment 1, Element 2 be changed to “Physical security controls” to be consistent with the language in CIP-003-6, R1. Additionally, edit all other references (e.g., CIP-003-6 Attachment 2, Guidelines and Technical Basis, and RSAWs). The posted language in Attachment 1, Elements 2, 4, and 3.1 do not use the acronyms for Low Impact BES Cyber System Electronic Access Point or for Low Impact External Routable Connectivity. SMUD

recommends that the acronyms “LEAP” and “LERC” be used after each of their defined terms. The posted language in Attachment 1, Element 4, Part 4.7 requires that the Cyber Security Incident Response Plan be updated “within 180 days” of a test or actual incident. SMUD recommends add “if necessary” after “within 180 days.” It is possible that no updates are actually needed to the plan following either event and it should not be necessary for entities to update a document unless there is a need to make improvements. The posted language in Attachment 2, Examples of Evidence for Element 2 provides card key and special locks as examples of physical security controls; however, the Guidelines and Technical Basis for Element 2 states, “entities may utilize perimeter controls (e.g., fences with locked gates, guards, site access policies, etc.) and/or more granular areas of physical access control.” SMUD recommends including “perimeter controls” under Attachment 2, Element 2 as an example “(e.g. card key, special locks, perimeter controls)” for consistency. The posted language in Attachment 1, Element 3, requires the use of a Low Impact BES Cyber System Electronic Access Point (LEAP) if there is Low Impact External Routable Connectivity (LERC). The definition of a LEAP is the “interface” of the device that “allows” the LERC. SMUD recommends that the Guidelines and Technical Basis for Attachment 1 where LEAP is described be updated to include statements that the LEAP can be implemented within the same Cyber Asset that is serving the function of an EACMS or EAP designated for a high impact or medium impact BES Cyber System. This is acceptable because regardless of the impact rating, it is the “interface” that is in scope. It is not the intent to require entity’s to have two separate physical Cyber Assets for either access point implementation. Potential for Multiple violations: SMUD has some concern that in a multi-impact rated program (high, medium and low), any failure to fulfill a requirement, such as Attachment 1, Element 1 Cyber Security Awareness or Element 4 Cyber Security Incident Response could result in violation of CIP-003-6, R2 as well as CIP-004-5, R1 and CIP-008-5. Potential compliance and enforcement implications should not dictate the structure of the standards nor an entity’s compliance program. An entity should be allowed to determine, in a form most efficient and effective to the entity, the best approach in fulfilling the security requirements. Please offer reassurance that the currently proposed structure with CIP-003-6, R2 does not create a potential situation for multiple violations. Confirmation from NERC Compliance will be important to reassure industry. Can NERC Compliance explain how this issue would be addressed under the Reliability Assurance Initiative?
Yes
SMUD supports the new definitions for Low Impact External Routable Connectivity and Low Impact BES Cyber Systems Electronic Access Point. SMUD appreciates the development of new definitions to simplify the language in the requirement. SMUD does suggest the following minor changes to the definitions for clarity: The posted language for the Low Impact BES Cyber System Electronic Access Point (LEAP) definition uses “allow” in regards to Low Impact External Routable Connectivity (LERC), SMUD recommends using the word “controls” to be specific that it is the intent of the interface of the LEAP to control the communication inbound and outbound for the asset(s) containing the low impact BES Cyber System.
Yes

SMUD agrees and supports the changes that were made to CIP-010-2, R4; including the use of Attachment 1 and Attachment 2. SMUD does recommend a few edits for clarity: The posted language for Attachment 1, Element 2.3 requires, “Responsible Entities shall determine whether additional mitigation measures are necessary…” which is intended to ensure that entity’s make an affirmative decision to allow the device to connect. SMUD recommends adding “if necessary” after “additional mitigation actions” for clarity to ensure that entities can accept the device without requiring modifications. The posted language for the Transient Cyber Assets in Attachment 1, Element 1 allows for authorization to be done individually or by asset type; however the Guidelines and Technical Basis for Element 1 does not discuss the ability to authorize based on a group of assets. SMUD recommends language be added to allow “authorization individually or by groups of assets” to the Guidelines and Technical Basis for Element 1.1.
Yes
SMUD agree with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. However, SMUD is concerned with starting the definition of Removable Media with the capitalized “Media” considering that “Media” is itself not a defined term. SMUD recommends an edit to resolve this concern: “Removable Media: One or more media”, directly connected for 30 consecutive calendar days or less, capable of transmitting executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset that can be used to store, copy, move, or access data. Removable Media are not Cyber Assets. 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.
Yes
Comments: SMUD agrees and supports the proposed implementation plan deadlines for CIP-003-6, R2. SMUD appreciates that the SDT has provided a tiered approach to the implementation of physical security and electronic access controls. SMUD believes that even with the tiered approach to the implementation plan, entities are not restricted from implementing both controls in parallel. Considering the diverse nature of the facilities and systems, SMUD believes the additional compliance time as well as the tiered approach provides entities the needed flexibility to evaluate their physical security and system capabilities to effectively apply the new requirements. There are possibilities that physical modifications will need to be made to facilities to deploy the necessary controls to restrict physical access. Additionally, to deploy a Low Impact Electronic Access Point, it is possible that certain systems or computer network architectures may need to be modified to accommodate the addition of an access point.
Yes
SMUD supports the removal of the IAC language from the 17 requirements and the continued work by NERC to develop the Reliability Assurance Initiative.
Yes
SMUD appreciates NERC's work on the development of the RSAWs related to CIP Version 5 and Revisions. SMUD is concerned that the RSAWs have not sufficiently incorporated the

specific language of the standards or the measures. It is unclear from reading the currently posted RSAWs how auditors will use the measures to inform the Compliance Assessment Approach.
Group
Arizona Public Service Company
Raymond Myford
Yes
Yes
Yes
Yes
Yes
Yes
No
Individual
Judy VanDeWoestyne
MidAmerican Energy Company
No
The revised structure of the CIP-003-6 is an improvement for the low requirements. However, some concerns remain. We find the new LERC definition needs clarification. Therefore we must vote no on the requirements that reference the definition. //Attachment 1, Element 2 - The placement of the phrase “based on need” with the commas in the statement may cause differences in interpretation. **Recommendation - Remove “based on need” from the requirement and the guidelines and technical basis because it is creating a more restrictive requirement for lows than for medium BES Cyber Assets that don’t have external routable connectivity. For those medium impact BES Cyber Assets, CIP-006-5 R1.1 requires entities to “restrict physical access,” without requiring ‘authorization’ or ‘based on need.’ // Attachment 1, Element 4 - Cyber incident response – 4.6 record retention was added with draft 2. It is unclear why. This is a ‘documentation only’ requirement and is duplicative to the record retention in Compliance Monitoring section C of every standard. **Recommendation – Remove this requirement. // Att. 1 – Element 4 Cyber incident response – 4.7 plan update. We find no support for the 180 day limit. Given the scale of lows, there could be multiple 180-

day clocks to track. While it’s important to keep plans current, triggering updates for lows for discrete incidents is administratively burdensome compared to the risk. **Recommendation - At least once every 15 calendar months, review the Cyber Security Incident response plan(s) (unless the plan(s) have already been reviewed under CIP-008) and update, if needed. Note: We’re concerned about double jeopardy for entities that leverage their COP-008 plan(s). // As with MidAmerican Energy Company’s draft one comments, we recommend addressing dispersed generation with respect to the CIP-003-5 R2 requirements for low impact BES Cyber Systems. The dispersed generation SAR scope is to make it clear “what, if any, requirements should apply to dispersed generation … Unless this clarity is provided applicability at a finer level of granularity related to dispersed generation may be seen as required and such granularity will result in activities that have no benefit to reliable operation of the BES. Furthermore applicability at a finer level of granularity will result in unneeded and ineffective collection, analysis, and reporting activities that may result in a detriment to reliability.” Standards under revision “should be examined and revised, as needed, to ensure it is clear that these activities and reporting are conducted at the point of aggregation to 75 MVA, and not at an individual turbine, inverter or unit level for dispersed generation.” ** We recommend the CIP and dispersed generation drafting teams continue to collaborate to clarify the applicability of CIP-003-5 R2 for low impact BES Cyber Systems for dispersed generation. Where a Registered Entity can demonstrate that a dispersed generation low BES Cyber System cannot adversely impact 75MVA or more within 15 minutes, the R2 requirements should not apply to the dispersed generation low impact BES Cyber System. The burden of proof is on the Registered Entity. The requirements apply if the Registered Entity cannot meet the burden of proof. Appropriate text could be added to the R2 requirement.
No
The LERC definition is not clear. The second sentence uses undefined terms and refers to specific technologies, which over the time will make the definition obsolete as technologies change. The use of capital letters for Intelligent Electronic Device creates confusion by suggesting it is a glossary term. The exclusion is not present for medium or high impact. Explain the difference. // ‘Background’ in the ‘Applicability’ section for CIP version 5 of standards 004 through 007, includes the following: “This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.” Is this relevant for low impact BES Cyber Systems? If so, should it be included in CIP-003-6?
No
The revised structure of the CIP-010-2 and many of the revisions are an improvement for the transient devices requirements. However, some concerns remain. As with draft 1, use of the word ‘Authorized’ requires an additional level of documentation, which is more burdensome given the scale of low impact BES Cyber Systems. **Recommendation - Remove ‘Authorized.’ Entities would still be required to “specify” users, locations and use (individually or by group) for each part in Element 1.2 and 3.1 to meet the FERC directive. // Att. 1 – Element 2 Vendor/contractor owned or managed – 2.3 - The intent of this requirement is clear in the guidelines and technical basis, but not in the words of the requirement. The requirement could be interpreted such that Responsible Entities shall determine whether additional mitigation actions are necessary for any (and all) of the methods specified (listed) in 2.1 and

2.2, not just the ones that were selected. Clarification is needed in the requirement, not just in the guidelines and technical basis. // Guidelines and Technical Basis for R4 Att. 1 Element 1.1 - Insert “type” with references to devices. For example, “…pre-authorize an inventory of devices or device types; or authorize devices or device types at the time….”
Yes
No
The implementation plan requires physical access controls for lows by April 1, 2018. These controls are to be applied to LEAPs, which based on the implementation plan, aren’t required to be identified until September 1, 2018, with the electronic access controls. We propose making them both the same date – September 1, 2018, to minimize confusion. However, we would prefer to keep the dates staggered if synchronizing the dates would make the implementation date April 1, 2018, for both of them.
Yes
We support removal of the IAC language with the understanding that compliance exceptions and other elements of the Reliability Assurance Initiative will be implemented in all regions in January 2015.
Yes
MidAmerican Energy Company thanks the Standard Drafting Team for commitment of their time and expertise to the development of these CIP version 5 revisions.

Additional Comments

SPP RE
Bob Reynolds

1. For the requirements applicable to Low Impact assets, the Standard Drafting Team (SDT) changed the structure of CIP-003-6, Requirements R1 and R2 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-003-6 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: (1) The wording of element 2 (physical controls) has an issue – the phrase “based on need…” is misplaced and should be modified to appear earlier in the sentence. The SPP RE recommends the sentence be modified to read as follows: “Physical access controls: Each Responsible Entity shall, based on need as determined by the Responsible

Entity, implement controls to restrict physical access to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Low Impact BES Cyber System Electronic Access Point, if any, through one or more of the following:" (2) Element 4.6, which requires record retention related to Reportable Cyber Security Incidents, is nonsensical as written. The requirement should establish a minimum expectation; otherwise the Responsible Entity could declare a one-second retention period and the auditor would have no option except to find compliance. (3) Element 4.7, allowing 180 calendar days to update an incident response plan, is excessive and unreasonable. Updating the plan in the same time frame as that for High and Medium impact BES Cyber Systems is not unreasonable given the importance and the anticipated very broad application of the requirement. (4) The Guidelines and Technical Basis for Requirement R2 states that monitoring does not imply logging. At issue is how the Responsible Entity can demonstrate an effective monitoring process if unauthorized attempted or actual access is not recorded in some fashion.

2. The SDT proposed new definitions **Low Impact External Routable Connectivity** and **Low Impact BES Cyber System Electronic Access Point** to clarify the requirement language in CIP-003-6. Do you agree with the proposed new definitions? If not, please offer suggested revisions.

   Yes:

   No: X

   Comments: The SPP RE agrees with the definition of Low Impact External Routable Connectivity (LERC). SPP RE does not agree with the definition of Low Impact BES Cyber System Electronic Access Point (LEAP) with respect to the statement that allows the LEAP to be placed at an external location. This might not be an issue if the communication circuits between the LEAP and the protected BES Cyber Systems are private and managed by the Responsible Entity. When the communication circuits are over public Wide Area Networks using third-party service providers, placing the LEAP on the other side of the public network circuits provides minimal protection and exposes the protected assets to the risk of unauthorized access.

3. For the requirements applicable to transient devices, the SDT changed the structure of CIP-010-2, Requirement R4 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-010-2 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: (1) Element 1.4 should also include a requirement to ensure any removable media, such as a USB flash drive, is also externally scanned for malware before use with the Transient device. Element 3.2 implies such scanning is only necessary if the removable media is to be used with the BES Cyber System. (2) Any dependence upon the review of a vendor policy or process, as permitted by Elements 2.1 and 2.2, needs to include a step to confirm the policy or process has been implemented for the transient device.

4. The SDT revised the proposed new definitions for Transient Cyber Assets and Removable Media to address issues raised in stakeholder comments. Do you agree with the proposed definitions? If not, please offer suggested revisions.

   Yes:

   No: X

   Comments: (1) The SPP RE again urges the Standards Drafting Team to eliminate the less than 30 day usage period found in the definition of Transient Cyber Asset, and require instead that the transient device be disconnected from the BES Cyber System or network immediately when its intended temporary use is complete and to remain disconnected until the next temporary use is required. Otherwise, a Responsible Entity could essentially maintain a routine, long-term network connection with only momentary connection breaks and thus bypass the security controls imposed on BES Cyber Assets that are normally connected for the long term. (2) The 30-days or less qualification in the Removable Media definition is unnecessary and may preclude the use of removable media containing authentication (e.g., digital certificates) or license (e.g., PSS/E dongle) information.

5. In response to stakeholder comments, the SDT revised the implementation deadlines. The implementation plan now includes tiered deadlines for the aspects of CIP-003-6. The CIP-007-6 timeframe is now consistent with CIP-006-6. Are these timeframes reasonable and appropriate? If not please explain specifically which implementation plan item needs adjusting and include the rationale for the suggested change.

   Yes: X

   No:

   Comments:

6. The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.

   In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

Yes: X

No:

Comments:

7. Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.

   Yes:

   No: X

   Comments:

Calpine Energy
Hamid Zakery

Calpine agrees with removing " identify, access, and correct" from the standards for High and Medium impact categories but recommend keeping " identify, access, and correct" for Low impact category.

Austin Energy
Thomas Standifur

1. For the requirements applicable to Low Impact assets, the Standard Drafting Team (SDT) changed the structure of CIP-003-6, Requirements R1 and R2 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-003-6 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: Recommend the requirements for physical security of low assets be deleted. This requirement is repetitive of safety requirements in the National Electrical Safety Code (NESC), Section 11 - Protective arrangements in electric supply stations, paragraph 110

General requirements. The NESC includes requirements to protect the public from high voltages. The safety aspects of the NESC are more stringent than the requirements in the proposed NERC standard and public safety is a higher concern than the less likely occurrence of security concerns at a low impact asset. Specifically the proposed CIP-003-6 requires:

The proposed NERC requirement allows technical physical security controls to restrict physical access to both. A fence with a locked gate, which is required by the NESC appears to meet the proposed NERC requirement to restrict physical access to both the asset and the cyber asset. The other suggestions in the draft standard could be provided in a best practices document. The requirement for physical security of low assets should be deleted.

2. The SDT proposed new definitions **Low Impact External Routable Connectivity** and **Low Impact BES Cyber System Electronic Access Point** to clarify the requirement language in CIP-003-6. Do you agree with the proposed new definitions? If not, please offer suggested revisions.

   Yes:

   No: X

   Comments: The LERC should specifically exclude communications aided relaying used for pilot relaying protection. Also, there is a high risk of confusion when using technical jargon in NERC definitions. Both of these definitions fall within this high level of confusion. If a national reliability standard requires too much technical jargon, it is written at the wrong level for its purpose. The reliability standard should be written to avoid the use of these definitions.

3. For the requirements applicable to transient devices, the SDT changed the structure of CIP-010-2, Requirement R4 and revised the language in response to stakeholder comments. Do you agree with the proposed requirements including CIP-010-2 Attachment 1? If not, please explain your objections and offer suggested revisions.

   Yes:

   No: X

   Comments: While the language in the proposed requirements is a good practice, it creates significant compliance burden for entities to maintain documentation to prove compliance; plus, additional resources will be required to implement compliance controls that yield minimal risk reduction for the reliability of the BES. Transient devices will be a source of possible violations in future internal compliance reviews for self reports and also compliance audits. Section 1.2 of Attachment 1 is not needed and should be removed. Requirements already exist for anyone having access to protected cyber systems. Section 1.2 puts an entity in double jeopardy of violating multiple requirements for one action. The same comments apply to section 3.1 of attachment 1 and this requirement should be removed.

4. The SDT revised the proposed new definitions for Transient Cyber Assets and Removable Media to address issues raised in stakeholder comments. Do you agree with the proposed definitions? If not, please offer suggested revisions.

   Yes:

   No:

   Comments:

5. In response to stakeholder comments, the SDT revised the implementation deadlines. The implementation plan now includes tiered deadlines for the aspects of CIP-003-6. The CIP-007-6 timeframe is now consistent with CIP-006-6. Are these timeframes reasonable and appropriate? If not please explain specifically which implementation plan item needs adjusting and include the rationale for the suggested change.

   Yes:

   No:

   Comments:

6. The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.

   In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

   Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

   Yes:

   No: X

Comments: As stated in previous comments, we do not support the removal of the IAC language. Removal of the IAC language is a return to zero tolerance and RAI does not magically make a violation disappear. Our suggestion is to delete any requirement from the standard that contains IAC language. This is our opportunity as an industry to remove the sections, develop better language as FERC allowed, or face multiple violations of these zero tolerance requirements for many years. We've rushed through all the previous versions to meet a deadline. This is the time to work on a solution and get a better standard. We are working to meet compliance deadlines for version five standards while making changes to the standards – this can't be a good practice. FERC approved the version five standards; they didn't remand them back. We have an official compliance date to meet for version five. Worse case, let's use the IAC language as currently approved.

7. Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.

   Yes: X

   No:

   Comments: The NERC CIP standards have resulted in numerous violations to registered entities and have been difficult to implement. These standards must get to a steady state and changes to the standards should be limited to an absolute minimum.