Individual or group. (66 Responses)
Name (51 Responses)
Organization (51 Responses)
Group Name (15 Responses)
Lead Contact (15 Responses)
Question 1 (46 Responses)
Question 1 Comments (53 Responses)
Question 2 (46 Responses)
Question 2 Comments (53 Responses)
Question 3 (44 Responses)
Question 3 Comments (53 Responses)
Question 4 (45 Responses)
Question 4 Comments (53 Responses)
Question 5 (46 Responses)
Question 5 Comments (53 Responses)
Question 6 (48 Responses)
Question 6 Comments (53 Responses)

Group
Tennessee Valley Authority
Brian Millard
No
The Registered Entity objects to the placement of controls for BES Cyber Systems at low impact assets within Attachment 1 of the CIP-003 standard. The Registered Entity suggests consider placing these controls within the existing CIP standards framework and applicability model for consistency and clarity. The Registered Entity suggests revising requirement R2, Attachment 1, Section 3 – Electronic Access Controls, paragraph 3: replace “from or to” with “to or from” in the last sentence. The Registered Entity suggests revising Requirement R2, Attachment 1, Section 3 – Electronic Access Controls, paragraph 4 : remove the word “all” in the last sentence.
Yes
No
The Registered Entity suggests revising Attachment 1, Section 1.5 to retain theft recovery tools as a valid method of mitigating the risk of unauthorized use of a transient cyber asset Mobile threat management platforms are a mature technology designed to address this issue, and are already used by many utilities today.
Yes
Yes
No
Individual
Scott Bos
Corn Belt Power Cooperative
Yes
No
The language used to define Low Impact External Routable Connectivity and Low Impact BES Cyber System Electronic Access Point in CIP-003-7 is excessively confusing and consists of many undefined terms. The language used in the currently approved CIP-003-5 for electronic access controls for external routable protocol connections is sufficient and meets the requirements in FERC Order 791.

Yes
Yes
Yes
No
Individual
Barry Lawson
NRECA
Yes
NRECA supports the revision that aligns the the compliance dates for these two sections.
Yes
1. NRECA requests that the SDT consider adding further clarity to the CIP V5 Revisions Implementation Plan (IP). With the numerous versions of the standards that have been revised and the CIP V5 standards that have not been revised, NRECA requests that an IP be included in the final ballot that clearly shows the compliance dates for all cyber security-related CIP standards. This will be very helpful to industry. 2. NRECA continues to support the SDT's efforts to address all of FERC's directives at one time. We are hopeful that affirmative ballot results are achieved for all of the revised standards so that NERC will only have to submit one filing to FERC on Feb. 3, 2015. 3. Related, NRECA believes a single filing by NERC will help to more quickly reach a much needed steady-state for the CIP standards. The industry needs several years of the CIP standards not being revised in order to implement CIP V5 and the revisions this SDT is working on. The continuous revisions and the moving target of compliance dates/requirements must end to give industry the opportunity to successfully implement these important standards. 4. NRECA wishes to thank the SDT (and their companies) and the NERC staff coordinators for their time, dedication and expertise on this challenging and important project.
Group
Northeast Power Coordinating Council
Guy Zito
No
1. Agree with the updated Rationales for R1 and R2. 2. Agree with the change from "element" to "section" in Attachments 1 and 2. 3. Agree that the newer consistency is easier to understand. 4. Request clarification on Section 2 of Attachment 1. There is a possible misinterpretation of what "need" in "…control physical access, based on need as determined by the Responsible Entity…" means. Does it mean a need to control access via a security program, or control access based on a person, employee or contractor need to access? Suggest that this be made consistent with the rest of the CIP Standards, based on a person's, employee's, or contractor's job requirements. 5. We request NERC resolve the inconsistency between the LERC definition and the application of the definition (CIP-003-7 Reference Model-4 on page 42). The Reference Model-4 illustrating that a LERC configuration is present is inconsistent with the LERC definition. Specifically, the LERC definition states: Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

According to the above definition, where an IP/Serial converter is utilized, the end-to-end session is not entirely bi-directional routable protocol. In this case LERC is not present (as illustrated in Reference Model 4) and a LEAP is not required. In this Reference Model, the session ends at the media converter. 6. Agree with Attachment 2, sections 1 and 2.
Yes
No comment on the definitions of LERC and LEAP.
Yes
No comment on CIP-010-3.
No
There appears to be a gap between how the three definitions for BES Cyber Asset (BCA), Protected Cyber Assets (PCA), and Transient Cyber Asset (TCA) might be interpreted and clarification will help ensure all entities and regions apply the use of the definition. Use Case: The example of a laptop used for vulnerability assessments, network sniffing or maintenance might be required to be a Protected Cyber Asset(s) because it first meets the Protected Cyber Assets requirements using a routable protocol verses a Transient Cyber Asset. However, the Transient Cyber Asset definition allows the device to be a Transient Cyber Asset if connected for less than 30 days and has a purpose as defined in the Transient Cyber Asset definition examples. Please ensure the standard allows the entity to define the Transient Cyber Asset ensuring it would not be interpreted by auditors as a Protected Cyber Asset(s) or BES Cyber Asset. The concern is that there is potential for inconsistency categorizing the Cyber Asset that is connected within the Electronic Security Perimeter using a routable protocol for less than 30 days as the Protected Cyber Asset(s) definition could also be applied to the use case, vulnerability laptop, if an entity's CIP-002-x methodology was applied using precedent order 1. Critical Asset, 2. BES Cyber Asset, 3. Protected Cyber Asset and then 4. Transient Cyber Asset.
Yes
No comment on the Implementation Plan, with respect to including CIP-003-7, Attachment 1, Section 3.
Yes
In the Guidelines and Technical Basis Section for CIP-003-7, the data flows presented in Reference Model-1, Reference Model-2, Reference Model-3, Reference Model-4, Reference Model-5, and Reference Model-6 would be easier to understand if the models depicted the actual data path. The models as shown in this posting do not make it easy to tell how the outside asset is logically connecting to the device within, without reading the description.
Individual
Leonard Kula
Independent Electricity System Operator
Yes
Yes
Yes
Yes
Yes
No
Group
ACES Standards Collaborators
Warren Cross
Yes

We support the changes from v6 with additional wording changes in Attachments 1 and 2, most of which is in the Guidance and Technical Basis Section. We support the clarification of 'Using the list of assets containing low impact BES Cyber Systems' to reduce any concerns regarding a list of Low Impact BES Cyber Asset inventory.
Yes
We agree with the defined terms of Low Impact External Routable Connectivity (LERC) and Low Impact Cyber System Electronic Access Point (LEAP) to be used to avoid confusion with the similar terms such as External Routable Connectivity (ERC) used for high and medium impact BES Cyber Systems.
Yes
In R4 the requirement states to implement one or a combination of both of activities to mitigate the task of vulnerabilities. In the list of examples and also in the RSAW, it lists 'System Hardening'. What specific System Hardening requirements are needed outside of those that are already listed? That term cannot be consistently audited against and is too vague to interpret. The SDT revised the proposed definitions for Transient Cyber Assets and Removable Media based on stakeholder comment. Do you agree with these proposed revisions? If not, please explain your objections and offer suggested revisions.
Yes
We support the clarification in the definition of a Removable Media (RM) that storage media is not a Cyber Asset in CIP-010-3. We support the SDT's inclusion in Transient Cyber Asset (TCA) definition that adds that a TCA is not included in a BES Cyber System and is not a Protect Cyber Asset. These changes will assist entities moving forward to better understand what are and what are not Removable Media and TCA.
Yes
We support the proposed Implementation Plan with substantive changes for CIP-003-7 Attachment 1 Section 2 (physical access controls for Low impact assets) being pushed back from April 1, 2018 to Sept. 1, 2018.
Yes
1. Regarding CIP-003-7 Attachment 1 Sections 1-4, we support this type of communication from the Standard Drafting Team (SDT) in terms of or providing the industry the objectives and intentions of the standards and requirements. While the sections in the Guidelines and Technical Basis Sections' provide additional guidance and direction to the responsible entities, the SDT should make it clear that the guidance and comments made in these sections are not enforceable and will not be audited against. 2. In CIP-010-3 please provide additional guidance as to what is required to document the review of antivirus, malicious code, and system hardening practices required in Section 2.1 and which entity is responsible for any security failure for a vendor Transient Cyber Asset that went through the documented protocol and still had security flaws after review(s). 3. The implementation plan does cause some concern. There are going to be as many as three different versions of individual standards that responsible entities will have to manage as part of that implementation. Will that be consolidated at the FERC submission? Are all Version 5 and Version 6 effective dates be removed and consolidated to Version 7? 4. Further explanation as to what constitutes an "unplanned change" in the implementation and after which effective date of which version of the standards, does the 12 calendar months begins. The implementation plan, states, "For unplanned changes resulting in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization, the Responsible Entity shall comply with all Requirements applicable to low impact BES Cyber Systems within 12 calendar months following the identification and categorization of the affected BES Cyber System." 5. In the Mapping Document on Page 8, Section CIP-007-5 R1.2, change "The protection again" to "The protection against. ' 6. The VSL for CIP-003 R2 is inconsistent with Attachment 1. The VSL does not use the defined term Cyber Security Incident while Attachment 1 uses the term exclusively. 7. Why response is capitalized in attachment 1 section 4 but lower case it in R1? 8. In CIP-002 Guideline and Technical Basis section on page 34 of the red-line, the statement "A Responsible Entity using this technology is not expected to implement a LEAP even though there technically is LERC" should be struck as it is inconsistent with the definition of LERC. The definition specifically excludes the technology referenced and, therefore, is not technically a LERC. 9. In CIP-002 Guideline and Technical Basis section on page 35 of the red-line, the statement "The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber

System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session" should be struck or revised as it is inconsistent with the definition of LERC. The proposed modified definition of LERC is very specific and only includes access or connection "from a Cyber Asset outside the asset containing those low impact BES Cyber System(s)". Thus, it cannot include access from the low impact BES Cyber System to a device outside the asset containing the low impact BES Cyber System. The Guidelines and Technical Basis section should be reviewed very closely to ensure additional inconsistencies are not contained in the document. 10. SPS should be removed from the standard. At the November Board of Trustees (BOT) meeting, the BOT approved the new definition of RAS along with the retirement of SPS. 11. Thank you for the opportunity to comment.
Group
FirstEnergy Corp.
Mark Koziel
No
Although FirstEnergy (FE) generally agrees with the proposed revisions to the CIP-003 Standard, FE believes the SDT has included a Reference Model with the proposed standard language that directly conflicts with its proposed definition of LERC and the approved definition of External Routable Connectivity (ERC). Reference Model 4 incorrectly indicates that a serial connected BES Cyber Asset is capable of having ERC and that the serial, non-routable connection to the low impact BES Cyber Asset provides the depicted device with LERC. Per the proposed LERC definition, a cyber asset outside a low impact asset must be connected to the low impact BES Cyber System with a bi-directional routable protocol connection for LERC to exist. The serial cable is not a bi-directional routable protocol connection. Reference Model 4 also conflicts with the ERC definition. If the BES Cyber Asset shown in the Reference Model was designated as Medium Impact, it would have no ERC because a single BES Cyber Asset with no routable connections has no associated electronic security perimeter (ESP), and the definition of ERC requires that the BES Cyber Asset have an associated ESP for ERC to exist. The SDT introduced the terms LERC and LEAP to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems (e.g., External Routable Connectivity (ERC) or Electronic Access Point (EAP)). An obvious conflict with a key provision of the ERC definition would undermine that objective and create considerable confusion. For instance, a single substation with multiple voltage lines could have serial connected relays associated with low voltage lines (low impact BES Cyber Systems) and serial connected relays associated with the higher voltage lines (medium impact BES Cyber Systems), which are connected per Reference Model 4. Per the proposed language, the low impact relays would have ERC and the medium impact relays would not have ERC per the existing standard language even if both sets of relays utilized the exact same external connection path. FE recommends the SDT remove Reference Model 4 and all references to Reference Model 4.
No
Although FE generally agrees with the definitions of LERC and LEAP, FE believes the definition of LERC needs to be revised to clarify the fact that only devices with routable connections can have External Routable Connectivity (ERC). In FE's opinion, the current definition already makes this clear by including the phrase "via a bi-directional routable protocol connection" at the end of the first sentence in the definition. Obviously, this is not sufficient since the SDT, itself, construed the LERC definition to allow a BES Cyber Asset with no bi-directional routable connections to possess LERC. Specifically, the SDT provided Reference Model 4 with their standard language, which incorrectly indicates that a serial connected BES Cyber Asset is capable of having both ERC and that the serial, non-routable connection to the low impact BES Cyber Asset provides the depicted device with LERC and ERC. FE recommends the following change to the first sentence of the LERC definition, "Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) entirely through a bi-directional routable protocol link between the BES Cyber System and the external Cyber Asset."
No
FirstEnergy believes the proposed standard language does not appropriately establish the scope of devices that should be classified as Transient Cyber Assets. Refer to Question 4 for comments and

recommendations related to the CIP-010-3 Standard language. FE agrees with the proposed structure of the standard.

No

FirstEnergy believes the proposed definitions do not appropriately establish the scope of devices that can be classified as Transient Cyber Assets. The proposed Transient Cyber Asset definition specifically excludes BES Cyber Assets (BCAs) and Protected Cyber Assets (PCAs) that are connected less than 30 days. This directly conflicts with the original FERC Mandate to develop requirements for BES Cyber Assets and Protected Cyber Assets (PCAs) that are connected less than 30 days. Instead of developing requirements for BCAs and PCAs that are connected less than 30 days, the SDT has chosen to eliminate this 30-day exemption entirely. Now, these devices have to meet the full suite of applicable CIP Standards regardless of how short the connection time period is. This conflicts with NERC's position as documented in FERC Order 791, "NERC and other commenters state that the 30-day exemption is necessary because removing the language would require responsible entities to implement the full set of CIP version 5 requirements on transient systems,156 which they assert would be impractical and costly.157" It also conflicts with FERC's position as documented in the order, "We are persuaded by commenters' explanations that it would be unduly burdensome to protect transient devices in the same manner as BES Cyber Assets because transient devices are portable and frequently connected and disconnected from systems." Also, the Transient Cyber Asset definition should limit the scope of cyber assets to those used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. FirstEnergy recommends revisions to three definitions that will address the above concerns: Transient Cyber Asset: A Cyber Asset that if, for 30 consecutive calendar days or less, is directly connected to a network within an ESP, a Cyber Asset within an ESP, or a BES Cyber Asset; and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. BES Cyber Asset (BCA): A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. A Cyber Asset is not a BES Cyber Asset if it meets the Transient Cyber Asset definition. Protected Cyber Assets (PCA): One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if it meets the Transient Cyber Asset definition.

Yes

No

Individual

Alshare Hughes

Luminant Generation Company, LLC

Suggested Revisions. Page references are from the "Clean" draft standard. (1) Page 31-32 (Guidelines & Technical Basis), "Examples of sufficient access controls," 3rd bullet ("As shown in Reference Model 5,…"). There is NO LERC in this example, so there is no access control requirement, at all. Should move this paragraph elsewhere. Suggestion: Make it non-bulleted and locate just ahead of the later paragraph that begins, "Some examples of situations,..." Also suggest replacing 1st sentence with: "Reference Model 5, below, provides an example where there is no LERC and therefore no electronic access control requirement. A non-BES Cyber Asset has been placed between the low impact BES Cyber System on the substation network and the Cyber Asset in the business network. The expectation is that..." (2) Page 35, Reference Model 3. Explanatory paragraph should say that low impact BES Cyber Systems at the asset are "…are externally accessible using a routable protocol from,…" (3) Page 38, Reference Model 6. The "Cyber Asset" within the BES asset should be labeled "Non-BES Cyber Asset" for consistency with Reference Model 5. This Cyber Asset doesn't "stop" direct access. Suggest changing the explanatory paragraph to: "Although direct, bi-directional routable connectivity is possible between the business network and the non-BES Cyber Asset, the

low impact BES Cyber System (s) cannot be directly accessed from outside the BES asset. A business network user or device trying to communicate with the BES Cyber Asset must first establish a network connection to the non-BES Cyber Asset, then establish a second connection from that system to the BES Cyber Asset. There is no LERC in this example." (4) Page 32 (Guidelines and Technical Basis), “Some examples of situations that would lack sufficient access controls,” 3rd bullet (“In Reference Model 5,…”) and Page 38, Reference Model 6 explanatory paragraph both seem to suggests that a non-BES Cyber Asset within a BES asset containing low impact BES Cyber Systems must/can/does play a role in protecting those BES Cyber Systems. This language should be removed to remove the potential interpretation of how such a non-BES Cyber Asset should be “controlling inbound and outbound electronic access.” (5) Page 36, Reference Model 4. This model incorrectly identifies LERC as being present. If LERC is not present, then LEAP is not required. This reference should be removed or modified. Minor Wording Change Suggestions are included for clarification. Page references are from the “Clean” draft standard. (1) Page24 (Attachment 2), Section 2, Item b: Change, “The Cyber Asset, if any, containing the LEAP” to The Cyber Asset, if any, containing a LEAP” (2) Page 24 (Attachment 2), Section 3, 1st paragraph: Change “Documentation showing that inbound and outbound connections for any LEAP are confined,…” to “Documentation showing that inbound and outbound connections for any LEAPs are confined,…” (3) Page 29-30 (Guidelines & Technical Basis), Requirement R2, 2nd paragraph: (3A) Change, “The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems or the low impact BES Cyber System itself or LEAPs, if any.” to “The Responsible Entity has the flexibility in the selection of the methods used to meet the objective to control physical access to the asset(s) containing low impact BES Cyber Systems, the low impact BES Cyber Systems themselves, or LEAPs, if any.” (3B) Change, “User authorization programs and lists of authorized users for physical access are not required although would help meet the security objective.” to, “User authorization programs and lists of authorized users for physical access are not required although they would help meet the security objective.” (4) Page 30 (Guidelines & Technical Basis), Requirement R2, 1st paragraph: Change, “In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of the communication within its low impact cyber security plan.” to “In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of such communication in its low impact cyber security plan(s). (5) Page 32 (Guidelines & Technical Basis), last paragraph “(The following diagrams,…” to Suggest changing to “The following diagrams provide reference examples intended to illustrate how to determine whether there is LERC and options for implementing a LEAP, if necessary. While these diagrams identify several possible configurations, Responsible Entities may have additional configurations not identified below.”
Yes
Yes
No
(1) Consider a revision of the Removable Media definition to allow for direct connection to a Transient Cyber Asset. Revised definition in part would read “…directly connected for 30 consecutive days or less to a BES Cyber Asset, a network within an ESP, a Protected Cyber Asset, or a Transient Cyber Asset….” (2) Consider a revision to the Transient Cyber Asset definition part (iii) to read “is not categorized by the entity as a Protected Cyber Asset (PCA)”
Yes
No
Individual
Maryclaire Yatsko
Seminole Electric Cooperative, Inc.
Yes

While Seminole accepts the proposed approach, we believe that since there is no difference in the requirement for CIP-004 R1 and the Security Awareness Requirement in CIP-003, the issue would be best addressed by adding additional applicability to the CIP-004-7 R1 Applicable Systems in the table of requirements.
No
The use of the word "location" is ambiguous and may be interpreted in multiple ways as used in the phrase “Low Impact BES Cyber System Electronic Access Point (LEAP)”
No
The use of the word "location" is ambiguous and may be interpreted in multiple ways. Business function authorization is excessive as there is no direct relationship between business function and cyber security in this environment. In general, the authorization requirements as provided are excessive. The activity will occur on a Cyber Asset inside an ESP. Authorization of Electronic Access and Unescorted Physical Access should be adequate for use of removable media on Cyber Assets within the ESP.
Yes
Yes
No
Individual
Amy Casuscelli
Xcel Energy
No
Xcel Energy has concerns about the requirements applicable to Low Impact assets. The revised language states that an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required and that lists of authorized users are not required. Yet, the Guidelines and Technical Basis section states that user authorization programs and lists of authorized users for physical access are not required although would help meet the security objective - which is misleading. We agree with the requirement to not maintain a list of low impact BES cyber systems but if the intent of the Guidelines and Technical Basis is to document controls and access, this seems to lead entities to track (list) low impact BES Cyber Systems and incorporate additional CIP program controls. Xcel Energy feels that by stating that an access point (LEAP) is required for these network-connected low impact assets, the actual scope of CIP controls must increase to ensure the access point is secure. These additional CIP controls include the need to manage change control for the LEAP, maintain an inventory of the connected devices (PCAs), and to perform occasional cyber vulnerability assessments to ensure the access point controls are effective. This ambiguity and the actual increase in scope, even though not stated directly in Requirement language, is concerning to Xcel Energy since the number of low impact subs will be over 600 substations which is more than 10 times the current Critical Asset Substations. Xcel Energy expects that the investment to implement LEAP at these low impact substations to cost at least $18 million. There is a single requirement for Low Impact Assets yet the Guidelines and Technical Basis section, along with the attachments, adds many more requirements which concerns Xcel Energy. The large number of assets in scope, as indicated above, along with the additional requirements set forth by attachments and Guidelines would require Xcel Energy to focus heavily upon assets classified as “low impact” to the BES which will detract from the overall protection of the BES by removing focus from High and Medium impact BES Cyber Systems. This significant increase in scope including the controls needed to be implemented and the cost and time to implement does not seem commensurate with the minimal additional protection to the BES. While Xcel Energy does support the staggered implementation timeline which will assist in compliance monitoring, Xcel Energy also recommends moving the Low Impact BES Cyber System requirements from the Attachments as well as the Guidelines and Technical Basis sections to their own Standard as done with CIP-014-1.

Group
Arizona Public Service Company
Kristie Cocco
Yes
No
The current definition contains both a definition as well as exclusions. The exclusions are very specific in nature, not all encompassing and apply only to transmission. The definition becomes confusing with this extra information. The glossary should contain a universally applicable simple definition of the term. Exclusions, ancillary explanations, and additional detail should be placed into a guidance document. If specific examples are used in the guidance document then additional examples should be included to cover both generation and transmission applications. APS suggests that the definition be simplified as follows: Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection, via routable protocol, to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s).
Yes
Yes
Yes
No
Individual
EricRuskamp
Lincoln Electric System
Yes
No
The proposed definitions do not take into account the exclusion for communication networks in Section 4. (Exemptions: Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters). The examples provided introduce a new “parameter” of BES Asset Boundary (definition?) for determination of LEAP and LERC. Based on the examples and explanations, utilities will be expected to document the entire communication path originating from, or terminating at, the BES Asset. Telecommunication companies are moving away from leased serial lines and moving the circuits to IP-based. If the phone company installs an IP/Serial converter, does that mean the utility has a LERC even though they have no control over this (or knowledge of the conversion)? Reference Model 3 appears to defeat the purpose of LERC, when the LEAP could be physically located at a remote location. Additionally in some instances, the SCADA system CFE communicates over IP to a terminal server inside the Control Center for serial-based protocols. Based on the guidance provided, this IP to Serial conversion in the terminal server at the Control Center would qualify all Low Impact substations using serial protocols to have LERC and the terminal server could be considered the LEAP. Recommendation: The determination for LERC should be determined by the protocol being used by the low impact BES Cyber Assets. If the BES Cyber assets do not have configuration settings for communicating on a routable system, the BES Cyber assets should be considered to have no external routable connectivity. The standards should not require utilities to track down every cyber asset (including cyber assets owned by others) along the communication path to confirm there is not routable connectivity. The Low Impact Cyber Assets should have password protection enabled (and

other measures based on the utility's risk tolerance) and this should be an acceptable level of risk mitigation for the assets protected
No
Many of the sections in the R4 referenced Attachment 1 include the ability to use a "other method to mitigate". Even though we agree with the need for flexibility in these areas there is concern about which "methods" will be accepted by the auditors. For example: Section 1.4 "…process to restrict communication, or other methods to mitigate the introduction of malicious code." Does disabling all unused communication ports go far enough to meet this requirement? Does scanning the USB drives that transfer files to and from these devices go far enough to meet this requirement? and Section 1.5 "…methods to restrict physical access.." If the laptop is being used at a technician's desk is the card reader access on the front door of the building reasonable (which restricts unescorted physical access to only company employees and a handful of contractors go far enough to meet this requirement? Else is their an expectation that there be an additional security layer within the secured building with access reduced to those that have a "business need" for access to the space. ========== On page 40 of 46 it states: "Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code." Many in the industry have relay test equipment that injects voltages and currents into protective relays to simulate faults and test the protective relay functions. This testing is done on the intervals described in PRC-005. This test equipment injects 60Hz voltage signals and does not transmit executable code to the protective relay. However, as with any modern test equipment it is "capable" of transmitting executable code. Most test equipment these days have one or two Ethernet ports that can communicate with a laptop for monitoring and control. Our request would be to change this to something like the following "and transmits executable code to the BES Cyber Systems." By making this this change it would be more clear that the requirements do not apply to the described relay test equipment as this test equipment does not transmit executable code to the protective relay or BES Cyber Systems.
Yes
Yes
No
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes
In CIP-003-7 - Attachment 1 - Section 1, it does not specify who is to receive the reinforcement of cyber security practices. We can assume it is the personnel who have access to the low impact BES Cyber Systems, but it is not clearly stated in the standard. Recommend adding a similar statement that is in CIP-004-7 R1.1 for medium impact BES Cyber Systems, "personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems". In CIP-010-3 - Attachment 1 - Section 1.5, listed is "Full-disk encryption with authentication" and is also described as "full-disk encryption solution along with the authentication protocol" in the standard. We are not sure what the authentication or authentication protocol is and would like to have it clarified in the standard. Does it mean full-disk encryption with pre-boot authentication?
Individual
Debra Horvath

Portland General Electric
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
Yes
No
Like the previous inclusion of "The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System." language better.
Yes
No
same comment as on the CIP-003-7 definition, prefer the language "The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System."
No
I appreciate the drafting team efforts. Thank you.
Individual
Dan Bamber
ATCO Electric Ltd
Yes
Yes
Yes
Yes
Yes
No
Group
Seattle City Light
Paul Haase
Individual
Sergio Banuelos

Tri-State Generation and Transmission Association, Inc.
Yes
There is a typo in the new draft in the Background section (p. 5, last paragraph). How does a “cyber security awareness program” address training requirements? Training (R2) and awareness (R1) are distinct items per CIP-004-7 as are their respective programs. This oversight is so blatant (and contradicted in the requirements) that it is not felt that it will change entity interpretations of the requirements and therefore is not significant enough to call for a negative vote on this draft. However, it is expected that future versions of CIP-003 will have this error corrected.
Yes
Yes
Yes
Yes
No
Individual
Joe O'Brien on behalf of Jerry Freese-NIPSCO
NIPSCO
No
Reference model 4 incorrectly identifies LERC as being present. LERC requires the use of bidirectional routable protocol for the entire end-to-end session. Where an IP/Serial converter is utilized the end-to-end session is not entirely bi-directional routable protocol. In this case LERC is not present and a LEAP is not required. Since these are Low impact devices and a serial device would not respond to a Shodan type query and identify itself this is not an inappropriate outcome of application of the definition. We propose that reference model 4 should be retained without designating the LEAP and LERC and updating the comment associated with the diagram.
Yes
No
CIP-010-3 Guidelines & Technical Basis Edit the language of subpart 3.2.1 to: “Use method(s) to detect malicious code on Removable Media using a Cyber Asset that is not a Protected Cyber Asset or part of a BES Cyber System; and”
No
We believe that the definition of Transient Cyber Asset requires an asset not to be a Protected Cyber Asset or a Bes Cyber Asset. This does not align with our understanding that a Cyber Asset connected within an ESP using a routable protocol for less than 30 days was to fall into the TCA category. As written any cyber asset connected within an ESP with a routable protocol would be required to be categorized as a PCA regardless of duration of connection. In the definition item iii should be changed to … is not categorized by the entity as a PCA. And then add to the Guideline a statement that clarifies when an entity anticipates connecting a cyber asset using a routable protocol within an ESP for 30 days or less the entity chooses whether to protect the cyber asset as a TCA, PCA or BCA; If the device is connected for more than 30 days it must be treated as either a PCA or BCA. Finally, the wording of the Transient Cyber Asset definition does not appear to meet the intent of the SDT as expressed during the Webinar. It was stated that a PCA that is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes can meet the Transient Cyber Asset requirements and NOT the PCA requirements. However, the words of the definition clearly state that a PCA can never be a Transient Cyber Asset regardless of the PCA’s function. Revised Definition to address concern Transient Cyber Asset: A Cyber Asset that is capable of transmitting or transferring executable code and is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, and wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to

a BES Cyber Asset, a network within an ESP, or a PCA. 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 or simultaneously classified as a CIP Cyber Asset (e.g., PCA).
No
Considering the aforementioned concerns with CIP-003 we voted Negative on the related Implementation Plan and non-binding ballot.
Yes
Additional comments to consider: The SDT may have strayed off course regarding Transient Cyber Asset revisions. The original FERC Mandate was essentially to develop requirements for BES Cyber Assets and PCAs that are connected less than 30 days: 132. Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems. 133. As explained by NERC, the 30-day exemption is intended to remove transient devices from the scope of the CIP version 5 Standards. We recognize that including transient devices in the definition of BES Cyber Asset would subject transient devices to the full suite of cyber security protections in the CIP version 5 Standards. We are persuaded by commenters' explanations that it would be unduly burdensome to protect transient devices in the same manner as BES Cyber Assets because transient devices are portable and frequently connected and disconnected from systems. Instead of developing requirements for BES Cyber Assets and PCAs that are connected less than 30 days, the SDT has chosen to eliminate this 30-day exemption entirely. Now, these devices have to meet the full suite of CIP Standards regardless of how short the connection time period is. This is a heavy burden just from the standpoint of maintaining inventory lists, drawings, and other real time documents and databases and represents a complete flip from NERC's original position, "NERC and other commenters state that the 30-day exemption is necessary because removing the language would require responsible entities to implement the full set of CIP version 5 requirements on transient systems, which they assert would be impractical and costly." Additionally, it appears that the SDT has chosen to bring cyber assets into the scope of CIP Requirements that were previously NOT in the scope of the CIP requirements. By the current CIP Version 5 Standards, a Cyber Asset connected to an ESP or BES Cyber Asset with non-routable protocol is not subject to the CIP Standards unless the device, itself, meets the definition of a BES Cyber Asset. If these changes are approved, any device connected with non-routable protocol must meet new transient cyber asset requirements. Let me correct that; if it is connected more than 30 days, no requirements apply. These new protections may be a good security practice, but it was not in the FERC Mandate, and it is a significant increase in the scope of the CIP Standards.
Individual
James Gower
Entergy
No
Entergy recommends aligning the Electronic Access Controls language in Section 3 of Attachment 1 with the Physical Access Controls language in Section 2 to allow the Responsible Entity the latitude to design controls that are consistent with needs dictated by the Responsible Entity's configuration.
Yes
Yes
Yes
Yes

No
Group
Colorado Springs Utilities
Shannon Fair
Individual
Mike Smith
Manitoba Hydro
Yes
No comments.
Yes
No comments
Yes
No comments.
Yes
No comments.
Yes
No comments.
Yes
No comments.
Group
Bonneville Power Administration
Andrea Jessup
Yes
CIP-003-7 attachment 2 Section 3: BPA requests specific clarification of the new LEAP concept. All of the SDT's examples show the possibility of Business Network connections having some kind of connectivity to low impact BES cyber systems. Cyber assets and systems can also be located on a completely isolated network, such that the BES asset boundary has no penetrations from/to other network systems. BPA's interpretation suggests this architecture is evidence enough to meet the Electronic Access Controls requirement in CIP-003-7 attachment 2 Section 3. BPA requests validation of this approach and a new reference model drawing showing this approach.
Yes
The definition of LERC begins by addressing 'Direct user-initiated interactive access or a direct device-to-device connection'; these terms address the intended use of the communications and not its nature. Additionally this phrase broadly covers both user and system access making the distinction unnecessary. BPA believes the only difference between External Routable Connectivity and LERC is the impact rating of the system and that the definition should be written as such. BPA's proposed definition: The ability to access a Low Impact BES Cyber System from a Cyber Asset that is outside of its associated Asset via a bi-directional routable protocol connection. BPA agrees with the exclusion for Point-to-point IED communications.
Yes
BPA supports the current structure.
Yes
Yes
No
Individual
Phan, Si truc

Hydro-Quebec transEnergie
Individual
Candace Morakinyo
Wisconsin Electric Power Company
Individual
RoLynda Shumpert
South Carolina Electric and Gas
No
• Attachment 1, Section 2 - The word “control” implies that an entity must know who can and cannot enter the restricted space. This is contradictory to the note included in R2 which states, “Lists of authorized users are not required”. SCE&G suggests the following revision to Section 2: “Each Responsible Entity shall define the method(s) used to inhibit illegitimate physical access...” • Guidelines and Technical Basis, Reference Model 4 – SCE&G does not agree that the Low Impact BES Cyber System, as depicted in Reference Model 4, has LERC. In order for LERC to exist, all of the following criteria must be met according to the LERC definition: 1. Connection exists from a cyber asset outside of the asset where the Low Impact BES Cyber System resides; and 2. The connection is made “via a bi-directional routable protocol connection”. When read strictly, the Low Impact BES Cyber System in Reference model 4 does not meet criteria 2, because it does not have a routable protocol connection. Rather than contend that the Low Impact BES Cyber System meets the LERC definition because the IP/Serial converter extends the routing, the SDT should make the case that the IP/Serial converter must be included as part of the Low Impact BES Cyber System. The IP/Serial Converter would be considered a Low Impact BES Asset with ERC. The rest of the system would be considered Low Impact BES Cyber Asset(s) without ERC. By protecting the IP/Serial gateway, the entity would inherently be protecting the serially connected devices at a network level, thereby accomplishing the SDTs understood intent.
No
SCE&G believes the definitions for EAP and ERC should be written so that they can apply regardless of the cyber system’s impact classification. Page 30 of the Guidelines and Technical Basis states, “The defined terms LERC and LEAP are used to avoid confusion with the similar terms used for high and medium impact BES Cyber Systems”. The confusion the SDT is trying to avoid seems to be around the use of the term “Electronic Security Perimeter” which is used in the EAP and ERC definitions. Low Impact BES Cyber Systems do not have ESPs, so this creates a problem for the SDT with those definitions. SCE&G believes the SDT should consider revising the definitions for EAP and ERC to remove ESP rather than creating the new definitions for LERC and LEAP. Once properly revised, the SDT can use the applicability sections to create a distinction in requirements for Low Impact Electronic Access Points and Low Impact External Routable Connectivity. SCE&G believes taking this approach provides the best long-term solution and creates the less ambiguity by not having terms defined differently based on their impact classification.
No
In Section 1.1 of Attachment 1, the SDT needs to include a provision for on-demand transient device compliance testing to occur once upon initial use within an ESP, and then to allow the tested transient device to be used anywhere within that single ESP. If the transient device leaves the ESP, then it should be rescanned before being reintroduced. However, as long as it stays within the ESP, it should be considered “clean”. It would be unreasonable and unnecessary to ask a relay technician who is performing relay tests to scan his laptop each time he connects to a different relay at the substation.
Yes
No
An overall 1-year extension should be given on all Low Impact Requirements. Because of the vagueness of CIP V5’s Low Impact requirements, many companies have been tentative to begin implementation. There is great concern that these revisions will impact the implementation designs being developed for V5, as evidenced by the LERC and LEAP definitions. Many stakeholders are waiting on these revisions to be completed before beginning implementation at their Low Impact

sites to avoid “shooting at a moving target”. Essentially, this has taken 1-year out of the original 3-year implementation plan.
No
Group
Santee Cooper
S. Tom Abrams
No
• Attachment 1, Section 2 – Santee Cooper is concerned with the removal of “restrict” and replacing it with “control” in context of physical access. Requirement CIP006 R1.1 Medium Impact BES Cyber Systems without External Routable Connectivity requirement states “Define operational or procedural controls to restrict physical access.” When comparing this to the Attachment 1 language it appears that the requirement to control physical access to all Low Impact sites are greater than that of a Medium Impact BES Cyber Systems without External Routable Connectivity requirement. Additionally no guidance is giving to the Entity on determining the need to apply such controls. Santee Cooper suggests revising the requirement so that the requirements for a Low Impacts site are no greater than, or does not appear to be greater than, the requirement of that of Medium Impact sites. For example: Each Responsible Entity shall document the method(s) that are used to prohibit unauthorized physical access to Low Impact sites…. • Guidelines and Technical Basis, Reference Model 4-Santee Cooper is concerned with the reference model explanation. . Identifying LERC communications through the IP/Serial Converter adds confusion to understanding the application criteria within the LERC definition, as it calls for “bi-directional routable protocol connection”. This could additionally cause confusion when attempting to apply these reference models to other systems using serial communications. Santee Cooper suggests including the IP/Serial convertor as part of the Low Impact BES Cyber System. • Santee Cooper is concerned with the formatting provided for the Low Impact requirements whereby they are included as section attachments. All other CIP Standards are listed in a tabular format that includes the Applicable System, Requirement, and Measure. Deviation from this format adds complexity to the readability of the standard and creates unnecessary confusion. Santee Cooper recommends modifying the format of the requirements to match those of the other standards.
No
Santee Cooper is concerned with the vagueness within the definitions. We understand the intent of the SDT was not to confuse the impact ratings associated with these definitions. However, to help avoid additional confusion we recommend SDT consider revising the definition of EAP and ERC to in order for these to be applicable across all appropriate BES Cyber Systems.
No
• Santee Cooper is concerned with the formatting provided for the Low Impact requirements whereby they are included as section attachments. All other CIP Standards are listed in a tabular format that includes the Applicable System, Requirement, and Measure. Deviation from this format adds complexity to the readability of the standard and creates unnecessary confusion. Santee Cooper recommends modifying the format of the requirements to match those of the other standards. • Section1.1 of Attachment 1 , Santee Cooper understands this to mean every time a Transient Cyber Asset or Removable Media connects to a different BES Cyber System they must be reviewed before it is attached. Santee Cooper recommends that the requirement be changed to state that the system be reviewed before its initial connection to a High or Medium BES Cyber System or if the system had not had been continually used in the purpose in which it was approved for its connectivity. For instance, for a device requiring to attach to multiple BES Cyber Systems the Transient Cyber Asset will need to be reviewed on its initial introduction to the BES Cyber System Environment and if for any reason this asset is used for any other function outside of the BES Cyber System Environment than its initial introduction then it shall be reviewed again. This would allow a relay tech to go to multiple BES Cyber Systems of the same impact rating while avoiding excessive documentation and scanning of a known good system. Additionally, these assets would not require reviewing if they are used throughout multiple BES Cyber Systems, as long as the assets are maintained by the same approved user or role, and are not used for another function outside of the BES Cyber Systems of the same impact. Should they be utilized for another function at a site of a

different impact rating, then they will require reviewing prior to being introduced into another High or Medium impact BES Cyber System.
Yes
No
Santee Cooper recommends that an additional 1-year extension needs to be given on the Low Impact Requirements. Given the current status and uncertainty of the impact of the Low Impact requirements many entities are continually revising their implementation plan or have simply stopped and are waiting the final results. Adding a 1 year extension will give entities adequate time to implement the security controls in an effective manner.
No
Individual
Chris Scanlon
Exelon Companies: BGE, ComEd, PECO, Exelon Generation
Yes
Yes
Yes
Yes
Yes
Yes
Exelon strongly supports the SDT's efforts to complete revisions in all four issue areas by the February 2015 filing deadline. Entities are focusing their CIP resources to implement the CIP Version 5 Standards. The task is daunting and resource intensive. It's important to resolve all the Order 791 directives in a timely manner to provide entities with some stability in the CIP standard language as the standards are being implemented. Exelon looks forward to a stretch of time in which CIP work can focus on implementation without directed revisions in development. Dividing the attention of CIP resources among current compliance, CIP V5 implementation and standard development is undesirable. Exelon requests that NERC better define RSAW development. While Exelon appreciates the posting of draft RSAWs for comment alongside of standard revisions, the response to the comments is not clear. Greater transparency is needed to understand the RSAW development process in general and the reasoning behind specific RSAW revisions. The RSAW development process should be a publicly accessible document and RSAW comments should be posted publicly. For standard drafting teams, the RSAW development process should be discussed and planned as part of the initial drafting team meeting so that schedules and other details can be determined, and team members can understand their role in the process. This is important to enable SDT members to fulfill their obligations under the Standards Process Manual to "collaborate" with NERC on the RSAW development. Exelon greatly appreciates the diligent work of the CIP V5 Revisions SDT. Thank you for your knowledge, skill and commitment to the project.
Individual
Oliver Burke
Entergy Services, Inc.
Yes
Yes
Yes

Yes
Yes
Entergy recommends aligning the Electronic Access Controls language in Section 3 of Attachment 1 with the Physical Access Controls language in Section 2 of Attachment 1 to allow the Responsible Entity the latitude to design controls that are consistent with needs dictated by the Responsible Entity's configuration.
Yes
Individual
Duane Radzwion
Consumers Energy Company
No
In rev 7, the SDT has continued to increase the requirements, measures and documentation above that approved at the prior rev 5 level, plus further removed flexibility for implementation. These additions are unnecessary to mitigate the extremely low risk posed by the low impact assets. These additions create further increased burden on entities and will cause limited resources to be diverted away from higher impact (and risk) cyber assets. In addressing the FERC order, the SDT can still provide “objective criteria” without going to such prescriptive requirements and measures.
No
Rev 7 continues on with the recent new requirement to identify a “LEAP” for locations, assets and systems with external routable connectivity, yet the standard and guidelines still claim that the cyber assets behind the LEAP do not have to be identified. “An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” This creates substantial compliance uncertainty and audit vulnerability. The SDT should clearly guide on how LEAPs can be identified without identifying the cyber assets being protected. The diagrams included in the guidelines and technical basis document, although providing some direction and clarification, also create additional questions. It is not entirely clear when processes, methods and protections will eliminate LERC and when not, especially when serial devices are involved.
Yes
Yes
Yes
No
Individual
Kara Douglas
NRG Energy
Yes
Yes
Yes
Yes
Yes

No
Individual
Andrew Ginter
Waterfall Security Solutions
No
Comment: Waterfall personnel have heard NERC subject matter experts maintain that the word "bi-directional" in the LERC definition has no meaning - that the word simply "clarifies" the word routable. It was clear in the recent NERC webinar on these proposed changes that hardware-enforced unidirectional gateways are intended to be seen as "unidirectional" rather than "bi-directional" communications, and so the use of these gateways does not constitute LERC. Given this confusion, even among subject matter experts, the guidance should be extended to include a reference model for at least the most common unidirectional deployment model currently used in the BES - unidirectional protection of generating units. Proposed additional reference model: Unidirectional gateway - a Cyber Asset in the generating asset network uses routable communications to gather data from one or more Cyber Assets in the generating unit. This Cyber asset is connected to, and sends generating unit state information to, a "transmit" hardware module located inside the generating asset. This constitutes a layer 7 application protocol break. The transmit hardware module is connected to a "receive" hardware module outside the asset using a one-way fiber optic cable. The transmit module hardware is physically unable to receive any signal from that fiber, and the receive module is physically unable to send any signal to the fiber. The receive hardware module is connected to a Cyber Assets on the corporate network. That Cyber Asset is connected to one or more other Cyber Assets on the corporate network through a variety of routable protocols, again constituting a layer 7 application protocol break. This communications is unidirectional, and therefore not LERC. Comment: The proposed guidelines do not document best practices for high-risk central monitoring of many low-impact generation assets. Proposed addition: In the bulleted list starting "Examples of sufficient access controls may include:" add a bullet: "As shown in reference model 7 <or whatever the unidirectional reference model above is called> many generating units, whose aggregate net Real Power capability exceeds 1500MW in a single interconnection, all communicate with one or more Cyber Assets on a corporate network. To prevent the corporate Cyber Asset(s) from constituting a single point of compromise for the entire set of generating units, each generating unit network contains a unidirectional security gateway. The gateway communicates generating unit status information to the corporate Cyber Asset(s), and is physically unable to send any attack, or any information at all, back into the protected generating assets.
Yes
Yes
No
Re: the definition of Removable Media. Nearly all "USB flash drives, external hard drives and other flash memory cards/drives" contain CPUs and firmware. In many of these units, the firmware can be compromised, and the compromised firmware can in turn compromise Cyber Assets to which the USB components are connected. See: https://github.com/adamcaudill/Psychson for details. Thus, all USB equipment are Cyber Assets. The last sentence of the definition of Removable Media should be changed to read "Examples include but are not limited to floppy disks and compact disks." Re: the definition of Transient Cyber Assets: Nearly all "USB flash drives, external hard drives and other flash memory cards/drives" contain CPUs and firmware. In many of these units, the firmware can be compromised, and the compromised firmware can in turn compromise Cyber Assets to which the USB components are connected. See: https://github.com/adamcaudill/Psychson for details. Thus, all USB equipment are Cyber Assets, transient or not. The last sentence of the definition of Transient Cyber Asset should be changed to read "Examples include, but are not limited to, USB flash drives, external hard drives and other flash memory cards / drives that contain nonvolatile memory, as well as Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."

Yes
No
Individual
Brian Evans-Mongeon
Utility Services
No
On Attachment 1 to the proposed CIP-003-7, Utility Services is concerned on the phrase “Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to…”. From our perspective, the language suggests or could be interpreted to imply that the Responsible Entity shall perform a determination of need and have it be documented. In addition, we are concerned that a CEA could evaluate the determination of need and subjectively consider the determination of need to be incomplete or insufficient in its evaluation of need. This seemingly parallels treatment and risks under the older versions of CIP-002 and the requirements for the RBAM. Utility Services would like to see the language strengthened to ensure that the Responsible Entity has some protections against subjective considerations from others and the only provision for violation be that a needs determination was not performed. Utility Services can support the point of documentation but not exposure to someone outside of the organization coming in and saying that you performed your determination incorrectly. Utility Services encourages the SDT to consider supplementing the existing language to provide greater assurances that the entity’s determination is sufficient to meet the purpose of this obligation. Additionally, the SDT could set the VSLs associated with this requirement to be strictly tied to the need determination being made and not allow for inadequacies or subjective third party considerations of the need determination. The CIP-003-7 Guidelines and Technical Basis for Attachment 1, Section 2 (page 30) states: “The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems.” Attachment 1, Section 2 (page 22) lists the following “(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 Points (LEAPs).” Should the Guidelines include language “for access to site or systems” be replaced with “ “for access to locations, systems or LEAPs”?
Individual
David Jendras
Ameren
Group
Florida Municipal Power Agency
Carol Chinn
FMPA supports the comments submitted by SMUD. FMPA also strongly supports the SDT's position on the RSAWs.
FMPA supports the comments submitted by SMUD. FMPA also strongly supports the SDT's position on the RSAWs.
FMPA supports the comments submitted by SMUD. FMPA also strongly supports the SDT's position on the RSAWs.
FMPA supports the comments submitted by SMUD. FMPA also strongly supports the SDT's position on the RSAWs.
FMPA supports the comments submitted by SMUD. FMPA also strongly supports the SDT's position on the RSAWs.

FMPA supports the comments submitted by SMUD. FMPA also strongly supports the SDT's position on the RSAWs.
Group
Dominion NERC Compliance Policy
Randi Heise
No
CIP-003-7 Rationale Block, pg 8 0f 40 Third paragraph Balloted language: “Responsible Entities will use their list of assets containing low,….” Suggested language: Delete sentence. There is no basis in CIP-002 to develop a list, only identify. CIP-003-7 Attachment 1, Section 1 Cyber Security Awareness., pg 22 of 40 For whom? In the similar requirement CIP-004-7 Part 1.1 which specifies “for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems” requirement CIP-003-7 R2, Section 1 does not address the target audience as in CIP-004-7 Part 1.1 and therefore is ambiguous. Since there is no authorized electronic or physical access to low impact BES Cyber Systems and therefore, no list of those with electronic or physical access to define a target audience, the requirement section 1 should be removed. CIP-003-7 Attachment 1, Section 2 Physical Security Controls., pg 22 of 40 Regarding the language “based on need as determined by the Responsible Entity” the SDT responded to comment with “The SDT moved, but retained, the phrase “based on need” so that criteria are established by which to control access. The need for access is to be “determined by the Responsible Entity” to accommodate facts and circumstances relevant to the location.” There is no obligation to determine any need for access but rather to control physical access. The SDT comment is unresponsive to the concern. The language “based on need as determined by the Responsible Entity” is a criteria for “control physical access” and therefore not a criteria for determining a need for access. Thus, the revised placement of the “based on need” phrase is particularly troublesome. A lock on a gate provides access control, but there is no deterministic feature involved. If you have a key, you have access, whether or not you “need” access. In addition this would imply a authorization and approval process which is specifically not required as indicated in the Guidelines and Technical Basis pg 30 of 60, “User authorization programs and lists of authorized users for physical access are not required”. Still confusing is the next paragraph where it is stated “The objective is to control the physical access based on need as determined by the Responsible Entity. The need can be documented at the policy level for access to the site or systems. The requirement does not obligate an entity to specify a need for each access or authorization of a user for access.” Documenting the “need” at the policy level does not enhance reliability and it is strictly administrative in nature. Therefore this language should be removed from the proposed standard. CIP-003-7 Attachment 1, Section 2 Cyber Security Incident Response, pg 23 of 40 Section 4.6 What triggers an update to the Cyber Security Incident Response plan(s), if needed? As with CIP-008 where there is an obligation to maintain the plan(s) based on triggering events in Part 3.1, there is not similar obligation in CIP-003 Attachment 1 Section 4. Therefore recommend removing the obligation to update the plan(s). Basis, there is no criteria specified in the requirement on what triggers the update. The ambiguity in this section part is problematic and will introduce audit risk. CIP-003-7 Attachment 2, Section 1 Physical Security Controls, pg 24 of 40 If there is an obligation to determine need as specified in Attachment 1 Section 2, please provide examples of evidence in Attachment 2 for “examples of need” and “examples of methods to determine need”. For examples, the following three examples arise as possible interpretations of the intent of “based on need”: Ex. 1: The need for the controls: “Because Low Impact BES Cyber Assets can impact the reliability of the BES, they must be protected.” Ex. 2: The need to have the ability to access (e.g., have a key): “Keys to Facilities containing Low Impact BES Cyber Assets can be distributed based on roles and responsibilities.” Ex. 3: The need to access: “You may only access a Facility containing Low Impact BES Cyber Assets if you need to perform one of the following functions: …” Please explain which of the examples was intended, or provide an example of the true intention. Also, as discussed above, please indicate how Ex. 1 provides any enhanced reliability, how Ex. 2 does not create an obligation for an authorization process to determine roles and responsibilities and a monitoring process should these change, and how Ex. 3 would ever be enforced at a site with no active monitoring. And, if you cannot monitor and enforce these “needs” why would you put them in a policy? “Based on need” is confusing and adds nothing to the requirement. It should be removed. If the SDT insists on keeping it, an example of a policy statement should be included here in the Guidance section, along with how it provides additional benefit and does not contradict previous guidance of not requiring an authorization process and list

of authorized users. CIP-003-7 Guidelines and Technical Basis, pg 28 of 40 Section: Requirement R2 Balloted language: “Using the list of assets containing low impact BES Cyber Systems from CIP-002” Suggested language: Delete sentence. There is no basis in CIP-002 to develop a list, only identify. CIP-003-7 Guidelines and Technical Basis, pg 29 0f 40 Section: Requirement 2, Attachment 1, Section 1 – Cyber Security Awareness Balloted language: “was delivered”, “delivery” Suggested language: Delete “that was delivered according to the delivery method(s)”. There is no basis in the requirement part to substantiate delivery. Guidance even says “The Responsible Entity is not required to maintain lists of recipients and track the reception of awareness material by personnel.” CIP-003-7 Attachment 1, Section 2 Physical Security Controls., pg 22 of 40 Guidelines and Technical Basis, pg 29 of 40 Reference Model -3 pg 35 of 40 Regarding the LEAP located at a location outside the asset containing the low impact BES Cyber Systems. Is a LEAP not located at the asset containing the low impact BES Cyber Systems required to be compliant with Attachment 1 Section 2, (2)? The LEAP is not located at an asset containing low impact BES Cyber Systems and Attachment 1 specifies “Required Sections for Cyber Security Plan(s) for (emphasis added) Assets Containing Low Impact BES Cyber Systems”. The wording of Attachment 1 Section 2 (1) conflicts with the applicability statement associated with Attachment 1 in that it appears to require protection of an asset other than an asset containing low impact BES Cyber Systems. Recommend changing applicability statement to: “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems and LEAPs”
No
Recommend changing the language of LERC by adding the phrase “other than a LEAP”. The revised definition is provided… Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset other than a LEAP outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time -sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).
Yes
No
The definition lacks objectivity and clarity in addressing the parenthetical portion of the original definition of a BES Cyber Asset and FERC Order by including what was the 4 specific uses of Cyber Assets in a transient nature as only examples. This will create confusion and the possibility of misclassification of Cyber Asset. Recommend the following definition. A Transient Cyber Asset is a Cyber Asset that if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. (A Transient Cyber Asset is not a BES Cyber Asset or Protected Cyber Asset (PCA).)
Yes
No
Individual
Venona Greaff
Occidental Chemical Corproation
Yes
No
OEVC has concerns that unnecessary limitations have been added to the exception allowed in the definition of "Low Impact External Routable Connectiviey (LERC)". As newly written, LERC only excludes point-to-point "communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between a Transmission

station or substation". The previous exception had a broader scope - recognizing that protection and control functions outside the Transmission system may be equally appropriate exclusions.
Yes
Individual
David Thorne
Pepco Holdings Inc.
No
Attachment 1, Section 3 Concern - LEAP (as used) applies to BOTH LERC and Dial Up - in contrast to Attachment 1 Section 3.1 where it is applicable solely to LERC (to permit only necessary inbound and outbound bi-directional access) whereas dial up connectivity requires 'authentication'. Remediation - Capture the discreet difference between 'authentication only' as it applies to dial up APs, rather than commingle this within LEAPs applied to routable connectivity.
No
See answer to #1
No
Attachment 2, Section 1.2.1 p 41- Use of word “Caution.” Concern - Use of 'Caution' is inconsistent with standard style and confusing Remediation – Change the wording to what is intended. “Transient Cyber Asset users must also have authorized electronic access to BES Cyber Systems that Transient Cyber Assets connect with read/write intent.”
No
Guideline and Technical Basis, Requirement R2, p18 Concern - Since transient devices and removable media (by nature) are regularly removed from PSPs, the current wording may be interpreted as being required at the end of use within a PSP (including chain of custody requirements) Remediation - Suggest not using “custodian” but use “assignee as applies to TCA and RM.”
Yes
No
Individual
Michelle R D'Antuono
Ingleside Cogeneratioon LP
Group
SERC CIPC
Bill Peterson
Yes
Yes
Yes
Yes
Yes
No

The comments expressed herein represent a consensus of the views of the above-named members of the SERC CIPC only and should not be construed as the position of SERC Reliability Corporation, its board, or its officers.
Individual
Kenn Backholm
Public Utility District No.1 of Snohomish County
Individual
Bill Temple
Northeast Utilities
No
1 Northeast Utilities agrees with the updated approach from “element” to “section” in Attachments 1 and 2. The “sections” are now aligned and easier to follow and understand. 2 Northeast Utilities requests clarification on Section 2 of Attachment 1. The phrase “based on need” in the statement, “control physical access based on need as determined by the Registered Entity,” is ambiguous and has multiple interpretations. The phrase “based on need” is used in other CIP standards with the meaning of “based on a person, employee or contractor’s job requirements; however, the CIP-003-7 Guidelines and Technical Basis indicates “the need can be established at the policy level based on higher operational or business needs to access to the site or systems.” To ensure the meaning of “based on need,” it would be prudent to clearly define “based on need” within the actual section. 3 Northeast Utilities requests that the inconsistencies between the LERC definition, the Requirement R2, Attachment 1, Section 3 – Electronic Access ControlsGuidance and Technical Basis, and the application of the LERC definition in CIP-003-7 Reference Model 4 be resolved. The inconsistencies are highlighted by the intermingling of the terms “protocol” and “session.” For example, the Guidance and Technical Basis uses the phrases “single end-to-end protocol session” and “a single end-to-end bi-directional routable protocol session” but the definition states “via a bi-directional routable protocol.”The terms “protocol” and “session” are distinctly different. Please clarify if it is an end-to-end protocol or an end-to-end session. In addition, the term “via” can be interpreted as either a “portion of” or “as a whole.” The definition should clearly describe the intent of “via a bi-directional routable protocol connection.” The inconsistency continues in the Model 4 – Description. The model fits the definition but does not fit the Guidance and Technical Basis. According to the definition, where an IP/Serial converter is utilized, the end-to-end session is not entirely bi-directional routable protocol.The first sentence of the Model 4 – Description is missing the discussion of the bi-directional routable protocol as discussed in the LERC definition. References for above comment: LERC definition: Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols). Guidelines and Technical Basis: When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases “direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.” The intent of “direct” in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for “device-to-device connection,” LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication from or to the low impact BES Cyber System. Reference Model - 4 Description: "The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communicationbetween the

business network Cyber Asset and the low impact BER Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System."
Yes
Yes
No
Northeast Utilities agrees with the definition of Removable Media; however, we request further clarification on the definition of Transient Cyber Assets. There is perceived gap between how the three definitions for BCA, PCA, and TCA might be interpreted and clarification will help ensure all entities and regions apply the use of the definition. Use Case: The example of a laptop used for vulnerability assessments, network sniffing or maintenance might be required to be a PCA because it first meets the PCA requirements using a routable protocol verses a TCA. However the TCA definition allows the device to be a TCA if connected for less than 30 days and has a purpose as defined in the TCA definition examples. Please ensure the standard allows the entity to define the TCA ensuring it would not be interpreted by auditors as a PCA or BCA. The concern is there is potential for inconsistency categorizing the Cyber Asset that is connected within the ESP using a routable protocol for less than 30 days as the PCA definition could also be applied to the use case, vulnerability laptop, if an entities CIP-002-x methodology was applied using precedent order 1. Critical Asset, 2.BES Cyber Asset, 3.Protected Cyber Asset and then 4.Transient Cyber Asset.
Yes
Yes
Please note the comments submitted are consistent with the comments submitted by EEI and the NPCC Task Force for Infrastructure and Technology (TFIST). NU wants to also recognize the SDT for the commitment they have shown in working with industry and responding to all the comments received to date. We look forward to continuing to work on these standards as the development process moves forward.
Group
Southern Company: Southern Company Services, Inc; Alabama Power Company; Georgia Power Company; Mississippi Power Company; Gulf Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing
Pamela Hunter
Southern would like to thank the SDT for the revisions to the requirements language in CIP-003 to accommodate industry concerns. Southern offers two small revisions for consideration: Comment 1: CIP-003-7 Attachment 2, Section 4, #2: It currently states "..identification and documentation of the roles and responsibilities for Cyber Security Incident response by groups of individuals" Recommendation: Change "of" to "or" to state: "the identification and documentation of the roles and responsibilities for Cyber Security Incident response by groups or individuals…" Comment 2: CIP-003-7, Guidelines and Technical Basis, R2 Attachment 1, page 34: Currently states: Locating the LEAP at an external location with multiple BES assets containing low impact BES Cyber Systems "behind" it should not allow unfettered access from one BES asset to all other BES assets sharing the LEAP. Locating the LEAP at an external location with multiple BES assets containing low impact BES Cyber Systems "behind" it should not allow unfettered access "to any other asset(s) sharing the Cyber Asset with multiple LEAPs". It might not be accessing all but should control any access between multiple lows behind the Cyber Asset containing the LEAPs. Southern Recommendation: Consider the following small modification to the text: Locating the LEAP at an external location with multiple BES assets containing low impact BES Cyber Systems "behind" it should not allow unfettered access from one BES asset to all other BES assets sharing the Cyber Asset with multiple LEAPs .
Yes
No

Southern agrees with the EEI comments on the requirements for transient devices. We answered no to this question due to the issues with the TCA definition, although we are comfortable with the language of the standard, the Guidelines & Technical Basis needs to be updated to reflect any changes made to the TCA definition. Please see our comments for Question 4.
No
Southern agrees with the EEI comments on the requirements for transient devices. The posted definition of Transient Cyber Asset (TCA) requires that a TCA cannot be a Protected Cyber Asset (PCA) or a BES Cyber Asset (BCA). This makes sense with the original BCA and PCA definitions; however, the revised definitions for BCA and PCA no longer include the 30 day exemption (e.g., "A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."). The concern is particularly critical for PCAs. Under the posted definition, any cyber asset connected within an ESP with a routable protocol would be required to be categorized as a PCA regardless of the duration of the connection (e.g., a laptop used for one day for maintenance). As a result we do not understand what devices can be categorized as a TCA given the posted definitions of BCA, PCA, and TCA. The Standards Drafting Team should address this concern before NERC submits CIP-010-3 and the PCA and TCA definitions to the Commission for approval. It is our understanding that a Cyber Asset connected within an ESP using a routable protocol for less than 30 days was to fall into the TCA category. Our understanding is based on FERC Order 791, which requires NERC to "develop requirements that protect transient electronic devices (e.g., thumb drives and laptop computers) that fall outside of the BES Cyber Asset definition." The BES Cyber Asset definition provides that a "Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an [Electronic Security Perimeter], a Cyber Asset within an [Electronic Security Perimeter], or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." (See FERC Order No. 791, paragraph 6) Also, in Order 791, FERC agreed that "it would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets" despite potential concerns of abuse for such an exemption. The 30-day exemption "is intended to remove transient devices from the scope of the CIP version 5 Standards. (Order 791, paragraph 132-133) We recommend a revision to the TCA definition to address this concern, for example: "A Cyber Asset that if, for 30 consecutive calendar days or less, is directly connected to a network within an ESP, a Cyber Asset within an ESP, or a BES Cyber Asset; and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Transient Cyber Asset is not a BES Cyber Asset or a Protected Cyber Asset." If a definition like this used, the Standards Drafting Team should also clarify in the Guidelines and Technical Basis for CIP-010-3 that if a Cyber Asset meets the TCA definition, only the TCA requirements apply. For example, if a Cyber Asset meets the PCA and TCA definition, only the TCA requirements need to be met and not both the PCA and TCA requirements.
Yes
No
Individual
Craig Jones
Idaho Power Company
No
Idaho Power Company continues to object to the Section 2 & 3 of attachment 1 in that it will require entities to maintain lists of Low Impact BES Cyber Systems at Low Impact assets which continues to be in conflict with CIP-002.
Yes
Yes
Yes

It seems that (ii) should say is not an BES Cyber Asset instead of "is not included in a BES Cyber System" as our understanding is that BES Cyber Systems are a grouping of BES Cyber Assets. Therefore, if the device is not a BES Cyber Asset it likewise would not be included in a BES Cyber System.
Yes
No
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
Yes
Yes
Yes
Yes
Yes
ATC wants to thank the SDT for revising the implementation timeline in accordance with comments to extend Low Impact out and give entities the time they need to succeed. ATC also appreciates and thanks the SDT for addressing the unofficial comments provided regarding the LEAP definition by changing it from a device to a device interface.
Individual
Marc Donaldson
Tacoma Power
Individual
Scott Berry
Indiana Municipal Power Agency
Yes
IMPA appreciates the “Guidelines and Technical Basis” section of CIP-003-7. However, this section contains many important statements that should be included in the attachment 1 or 2 sections of the standard. By including them in the attachment sections, they can be used by entities during audits to show compliance to a requirement. Auditors will audit entities to the criteria included in the attachment sections of the standard and not statements contained within the “Guidelines and Technical Basis” section. For example on page 29 of 40, 4th paragraph, the last sentence states “The Responsible Entity is not required to maintain lists of recipients and track the reception of the awareness material by personnel”. This statement seems to be as important as the note in requirement R2 that addresses not having to have a list of low impact BES Cyber Systems or their BES Cyber Assets. IMPA recommends including this statement in Section 1 of attachment 1.
Individual
David Rivera
New York Power Authority

No
NYPA continues to recommend that the language added to CIP-003-6, table R2 (Low Impact Cyber Systems) 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 Cyber Systems, 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. Having shifted 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. The bottom line is that NYPA takes the position that all of the issues identified with this new version of the CIP Standards, are the result of NERC having placed the controls for the 'Low' impact Cyber Systems into a single requirement of CIP-003. Further, as long as the structural problems exist, there will be continued changes needed to these new requirements and associated controls.
No
See comment for Question 1
Yes
Yes
Yes
No
Group
Duke Energy
Michael Lowman
Yes
No

Duke Energy suggests the following rewrite of LERC: “Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection up until the devices at which the routable protocol connection terminates. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).” As it is currently written, it can be misinterpreted that LERC exists up to a serial device if that serial device protocol (i.e. Modbus) is at one point converted to a routable protocol (i.e. TCP/IP). The addition of “up until the devices at which the routable protocol connection terminates” helps to clarify that routable connectivity only exists up to the point where the IP connection terminates, even if the connection is then converted to another protocol and the communication path continues on.
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 that 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.
Yes
Yes
Duke Energy suggests adding the previous language in CIP-003-6 Attachment 1, Section 2 back into CIP-003-7, Attachment 1, Section 2 as follows: “Physical Security Controls: Each Responsible Entity shall implement controls to restrict physical access, based on need as determined by the Responsible Entity, 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 Points (LEAPs), if any, based on need as determined by the Responsible Entity, through one or more of the following: • Access controls; • Monitoring controls; or • Other operational, procedural, or technical physical security controls.” While the language in the Guidance suggests that “User authorization programs and lists of authorized users for physical access are not required”. However, as currently written, Section 2 could be interpreted to require an authorized users list. Duke Energy suggests modifying the language to more closely resemble the language in the Guidance Document. In addition, we believe that the examples provided for Section 2 of Attachment 2 do not align with the current language and are more in line with the language in the previous draft of CIP-003-6. Finally, Duke Energy has reviewed EEI’s comments related to this project and support said comments.
Individual
Megan Wagner
Westar Energy
Individual
Bob Thomas
Illinois Municipal Electric Agency
Individual
Thomas Foltz
American Electric Power
No
AEP has two objections to this standard. First, AEP recommends replacing the word "control" from Attachment 1, Section 2 with something less stringent such as "restrict" because "control" implies a program that demonstrates control over access such as a key control program rather than restricting

physical access through locked doors, etc. Such an access control program would place a large financial burden on entities for low impact BES Cyber Systems. Second, AEP continues to object to the inclusion of obligations that are truly requirements in "attachment" form because AEP is concerned that the structure is confusing and that many will read the body of the standard and not associate the attachment as the requirement.
Yes
In addition, the exclusion for point-to-point communications should be more generally applicable than just to Transmission assets. The exclusion should also be extended to medium impact BES Cyber Systems with point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions.
No
AEP objects to the continued inclusion of the bulleted list in the attachments to CIP-010-3 because the bulleted lists seem prescriptive. AEP supports the SDT's revision of CIP-003-7 to include the bulleted lists in the measures rather than as part of the attachment because it reduced the prescriptive nature of the attachment, and AEP believes that CIP-010-3 should be similarly revised to move the bulleted lists to the measures in Attachment 2.
Yes
Yes
Yes
The SDT and NERC have done a great job of walking the fine line between the regulator and industry. They have gone the extra mile to obtain broad-based industry support for the V5 revisions and meet the FERC Order. AEP's concern with these Version 7 requirements is that it and other entities are in a position of implementing Version 5 without clear interpretations from NERC and the regions, with Version 7 implementation on the horizon as well. As of this writing, there are 23 questions open in the lessons learned and FAQ areas, half of which relate to the foundational requirements of CIP-002 that impact all the CIP requirements. Recognizing that this is not the responsibility of the SDT, AEP recommends that NERC resume the interpretation process as soon as possible to ensure timely conclusions that can inform entities' implementation of Version 5 and all future versions. In addition, regarding the implementation plan, the SDT should consider providing additional implementation time for CIP-010 in consideration of entities with large numbers of transient assets.
Individual
Nathan Mitchell
American Public Power Association
Yes
Yes
Yes
Yes
Yes
Yes
APPA staff supports the efforts to align the CIP RSAW development with the draft standards under ballot. APPA encourages NERC staff to meet with the SDT to incorporate their subject matter expertise into the next RSAW draft. We also request that a separate review of the revised RSAWs be afforded the industry either in conjunction with the final CIP ballot or shortly thereafter.
Individual

Jonathan Appelbaum
The United Illuminating Company
No
Agree with EEI
No
Agree with EEI Comments and see comments at end. UI is voting negative for CIP-003 Standard and defintion because the interpretation, definition and reference model 4 are not consistent with each other and to unclear to hazard a positive vote.
No
Voted No because the definition will need to change.
No
NEED to be clear that we can identify a cyber asset as a TCA and it will not be found by an auditor to be a PCA. For example, a cyber asset used for maintenance and connected within an ESP for less than 30 days will meet both definitions PCA and TCA. The drafting team says that an entity would identify it as a TCA and that is correct. But an auditor could just as easily say it meets both definitions so both sets of controls need to apply. I think that the definition of TCA should include a stronger statement than A TCA is not a PCA or BCA, for example, Once an Entity properly identifies a cyber asset as a TCA then the cyber asset does not need to be assessed as a PCA or BCA.
Yes
Yes
There are inconsistencies between the LERC definition, the Technical Guide and reference Model 4. Whether further revisions are made or not are made I want to point out where there are inconsistencies so the SDT can review them. Inconsistencies between the definition of LERC, the Technical Guidance and the explanatory text of Reference Model 4 will create confusion among Entities attempting to identify and implement LERC and is less practical solution then what EEI proposed. The following discusses the inconsistencies with the draft standard. The definition of LERC identifies two inclusions and one exclusion. LERC is present when a remote user and establish direct connection or when there is a device to device connection via a bi-directional routable protocol. The technical guideline on page 30 and 31 in its attempt to clarify the definition actually adds confusion. The guideline states “The Responsible Entity is not required to establish LERC communication or a LEAP if there is no bi-directional routable protocol communication or Dial-up Connectivity present. In the case where there is no external bi-directional routable protocol communication or Dial-up Connectivity, the Responsible Entity can document the absence of the communication within its low impact cyber security plan”. This sentence seems to refute the diagram in reference model 4 because the test is whether there is external bi-directional routable protocol communication present at the asset. There is no discussion of the term via. It is clear go or no go. The guideline on page 31 attempts to define “direct” as the ability to establish an interactive session with the low BCS from a remote location using a bi-directional routable protocol within a single end-to-end protocol session. This sentence does not state that the remote access is via a bi-directional routable protocol session but that the Bi-directional protocol session is a single end-to-end session. Again, this appears to be inconsistent with reference model 4 that clearly shows a protocol change from IP to Serial. It’s possible that the word protocol is doing double duty, once defined with bi-directional routable and once as the entire communication path meaning no application breaks. But it isn’t clear. The guideline introduces another test for LERC presence by analyzing the ability of the Low BCS to establish any connection with a device outside the location using a single end-to-end bi-directional routable protocol session. Again the use of the phrase single end-to-end bi-directional routable protocol session seems to rule out the concept of via a bi-directional routable protocol. In this test case the need for the connection to be direct or interactive is also removed. The Guideline attempts to clarify device-to-device connections but it applies a new twist. LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication from or to the low impact BES Cyber System. The Guideline requires the entity to analyze the Cyber Asset outside the low bes Cyber asset to determine if LERC exists in the Low BCS. Again the concept of via a bi-directional routable protocol is removed. Reference Model 4 is deficient because it is difficult to ascertain if this is representing

“direct” access or device-to-device connection. The explanatory text introduces a further characteristic not present in either the definition or the guideline: direct addressability and that the communication path is extended. If the definitional use of the term via is meant to mean that any portion of the communication from a remote location to the Low BCS utilizes a bi-directional routable protocol session then the use of the characteristic direct addressability is irrelevant. The explanatory text should state that there is LERC because one portion of the path is via a bi-directional routable protocol session, or maybe the term direct addressable has some alternate meaning.
Individual
Gregory Campoli
New York Indepent System Operator (NYISO)
Yes
Yes
Yes
No
There appears to be a gap between how the three definitions for BES Cyber Asset (BCA), Protected Cyber Assets (PCA), and Transient Cyber Asset (TCA) might be interpreted and clarification will help ensure all entities and regions apply the use of the definition. Use Case: The example of a laptop used for vulnerability assessments, network sniffing or maintenance might be required to be a Protected Cyber Asset(s) because it first meets the Protected Cyber Assets requirements using a routable protocol verses a Transient Cyber Asset. However, the Transient Cyber Asset definition allows the device to be a Transient Cyber Asset if connected for less than 30 days and has a purpose as defined in the Transient Cyber Asset definition examples. Please ensure the standard allows the entity to define the Transient Cyber Asset ensuring it would not be interpreted by auditors as a Protected Cyber Asset(s) or BES Cyber Asset. The concern is that there is potential for inconsistency categorizing the Cyber Asset that is connected within the Electronic Security Perimeter using a routable protocol for less than 30 days as the Protected Cyber Asset(s) definition could also be applied to the use case, vulnerability laptop, if an entity’s CIP-002-x methodology was applied using precedent order 1. Critical Asset, 2. BES Cyber Asset, 3. Protected Cyber Asset and then 4. Transient Cyber Asset.
Yes
Yes
Group
Edison Electric Institute
Melanie Seader
No
Improvements made to the CIP-003-7 low impact requirements are appreciated; however, we answered no to this question because of specific inconsistencies (described below and in our response to question 2) between the language of the standard and the Guidelines and Technical Basis. This is a concern because our members have reported that at least one Region has communicated that they will only be using the language of the standard and will not use the Guidelines and Technical Basis for enforcement, which will result in multiple interpretations and requirements across the regions. For those of our members who fall under multiple regions, this is very problematic and therefore should be addressed by the Standards Drafting Team before NERC submits CIP-003-7 to the Commission for approval. The removal of monitoring controls from the language of the standard (CIP-003-7 Attachment 1, Section 2), which now requires Responsible Entities to “control physical access” may lead to interpretations that only physical access controls or perimeter controls can be used. However, the Guidelines and Technical Basis states “the Responsible Entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls.” The language of the standard is enforceable and

therefore should be clear as to what controlling physical access means, in this case operational, procedural, or technical physical security controls such as perimeter and/or monitoring controls. The Standards Drafting Team should address this concern before NERC submits CIP-003-7 to the Commission for approval. In addition to the above comment below, please see our comments for Question 2, which also apply to CIP-003-7.
No
The CIP-003-7 Guidelines and Technical Basis interpretation for Requirement R2, Attachment 1, Section 3 – Electronic Access Controls inappropriately exceeds the language of the standard. The standard requires an electronic access point to "permit only necessary inbound and outbound bi-directional routable protocol access" where a LERC is present. The language of the standard and the LERC definition both focus on routable protocol connections, and the language appears to exclude cyber assets with only non-routable protocol connections. However, Reference Model 4 appears to mandate that some cyber assets with only non-routable connections need to be treated as routable connected devices: "there is a LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System." Reference Model 4 contradicts the plain language of the LERC definition, which could bring many non-routable connected devices into the scope of this requirement. This is particularly concerning given that our members have reported that at least one Region has communicated that they will only be using the language of the standard and will not use the Guidelines and Technical Basis for enforcement, which will result in multiple interpretations and requirements across the regions. For those of our members who fall under multiple regions, this is very problematic and therefore should be addressed by the Standards Drafting Team before NERC submits CIP-003-7 to the Commission for approval. In addition, the CIP-003-7 Guidelines and Technical Basis interpretation of external routable connectivity for Low Impact BES Cyber Systems will also create confusion with the External Routable Connectivity (ERC) definition and could cause unintended consequences with implementation and enforcement of requirements on Medium Impact BES Cyber Systems with ERC. Despite the use of different terms (e.g., LERC instead of ERC), the similarity between the ERC and LERC definitions (copied below), specifically the use of access from a Cyber Asset either outside the asset containing the low impact BES Cyber Systems or outside the Electronic Security Perimeter "via a bi-directional routable protocol connection" could logically lead to interpretations that the Reference Model 4 concept would also apply to high and medium impact BES Cyber Systems, therefore bringing many non-routable devices into scope of additional CIP Standard requirements. The compliance cost to apply ERC related CIP Standard requirements to high and medium impact cyber assets with no routable connections is unduly burdensome. The Standards Drafting Team should address this concern before NERC submits CIP-003-7 to the Commission for approval. (ERC and LERC definitions referenced above): External Routable Connectivity (ERC) is defined as "the ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." Low Impact External Routable Connectivity (LERC) is defined as "Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection…."
No
We answered no to this question due to the issues with the TCA definition, as further described in our comments on Question 4. We are comfortable with the language of CIP-010-3, Requirement R4, with the caveat that the Guidelines & Technical Basis needs to be updated to reflect changes made to the TCA definition as described in our comments for Question 4.
No
The posted definition of Transient Cyber Asset (TCA) requires that a TCA cannot be a Protected Cyber Asset (PCA) or a BES Cyber Asset (BCA). This makes sense with the original BCA and PCA definitions; however, the revised definitions for BCA and PCA no longer include the 30 day exemption (e.g., "A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."). The concern is particularly critical for PCAs. Under the posted definition, any cyber asset connected within an ESP with a routable protocol would be required to be categorized as a PCA regardless of the duration of the connection (e.g., a laptop used for one day for maintenance). As a result we do not understand what devices can be categorized as a TCA given

the posted definitions of BCA, PCA, and TCA. The Standards Drafting Team should address this concern before NERC submits CIP-010-3 and the PCA and TCA definitions to the Commission for approval. It is our understanding that a Cyber Asset connected within an ESP using a routable protocol for less than 30 days was to fall into the TCA category. Our understanding is based on FERC Order 791, which requires NERC to "develop requirements that protect transient electronic devices (e.g., thumb drives and laptop computers) that fall outside of the BES Cyber Asset definition." The BES Cyber Asset definition provides that a "Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an [Electronic Security Perimeter], a Cyber Asset within an [Electronic Security Perimeter], or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." (See FERC Order No. 791, paragraph 6) Also, in Order 791, FERC agreed that "it would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets" despite potential concerns of abuse for such an exemption. The 30-day exemption "is intended to remove transient devices from the scope of the CIP version 5 Standards. (Order 791, paragraph 132-133) We recommend a revision to the TCA definition to address this concern, for example: "A Cyber Asset that if, for 30 consecutive calendar days or less, is directly connected to a network within an ESP, a Cyber Asset within an ESP, or a BES Cyber Asset; and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Transient Cyber Asset is not a BES Cyber Asset or a Protected Cyber Asset." If a definition like this used, the Standards Drafting Team should also clarify in the Guidelines and Technical Basis for CIP-010-3 that if a Cyber Asset meets the TCA definition, only the TCA requirements apply. For example, if a Cyber Asset meets the PCA and TCA definition, only the TCA requirements need to be met and not both the PCA and TCA requirements.
Yes
No
Individual
Christina Conway
Oncor Electric Delivery Company LLC
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions. Additional comments below: Recommendation: CIP-003-7 Attachment 1 Section 2, Oncor recommends the draft language revert back from "control" to "restrict" to eliminate ambiguity.
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 41 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 41 "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-010-3. Alternatively, Limit applicability to Medium Impact BES Cyber Assets with ERC, or vulnerable to malicious code.
No
Oncor supports EEI comments. Please reference EEI comments for suggested revisions.
Oncor has no comment.
Oncor has no comment.
Individual
Brett Holland
Kansas City Power and Light
No
Per the addition in "Section 1" of Attachment 1, there is no reason to include a statement such as "which may include associated physical security practices." It is not as clear with this clause as it was with the previous examples what is actually required. The most essential function of the requirements is to provide an outline of what needs to be accomplished, not provide statements regarding what you "may" want to do. Per the additions in "Section 2" of Attachment 1, removal of an implementation of controls and references to the "controlling of physical access " cause confusion when determining what is meant by a requirement to "control physical access." It appears that the requirements are trying to have it both ways, in implying entities must maintain absolute control of physical access, and then following up the requirement by stating that the entity can essentially do whatever they want “based on need.” This is not the type of requirements direction and guidance that is helpful when trying to establish a compliant program. A statement that includes "based on need as determined by the Responsible Entity" is a red flag for an overreaching guideline turned requirement that should not be included in a FERC-enforced order. The “Guidelines and Technical Basis” section has grown to overrule other sections. The section has been used to allow the “Requirements and Measures” sections to be written ambiguously under the guise that the “Guidelines and Technical Basis” section is only supplemental to the actual requirement. In reality, the “Guidelines and Technical Basis” will be the primary place an auditor or an entity will go to understand compliance with the requirements. The requirements section is akin to an outline of control objectives, whereas the guidelines section is akin to dozens and dozens of disorganized control activities, or internal controls, sprinkled into each paragraph.
No
The definition of LEAP does not specify what is meant by “controlling” LERC. If “control” includes access control, then devices that manage things such as two-factor LERC would be considered LEAPs, along with the device that actually allows for the electronic routable pass-through (firewall, switch, etc.). If any external application is used to “control” access via LERC, the device or series of devices hosting that application could be construed as LEAPs. KCP&L recommends amending the definition of LEAP to state “A Cyber Asset interface that controls traffic that is defined as Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.
Yes
Yes
Yes
No
Individual
Cheryl Moseley
Electric Reliability Council of Texas,, Inc.

Yes
While the current definition of Transient Cyber Asset (TCA) is effective, ERCOT offers the following suggestions to improve the definition. “Transient Cyber Asset: A Cyber Asset that, (i) is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes, and (ii) has a temporary direct connection either physically (e.g., Universal Serial Bus, etc.) or logically (e.g., using Ethernet, or wireless, including near field or Bluetooth communication) to a BES Cyber Asset, a network within an ESP, or a PCA. There has been much discussion regarding the length of connectivity of a Cyber Asset versus the purpose of the connectivity of the Cyber Asset. It is important to note that the purpose of the connectivity is the key to determining the classification of a Cyber Asset and, therefore, the controls to be applied. • How should Cyber Assets be properly categorized as TCA, Protected Cyber Asset (PCA), or BES Cyber Asset (BCA)? It is ERCOT’s contention that an asset commissioned to provide a reliability function would be a BCA, regardless of the duration of connectivity. Any asset connected to perform the functions noted in the definition of TCA would be a TCA, regardless of duration of connectivity. ERCOT contends it is incumbent on entities to properly note the purpose of the asset and categorize it accordingly. ERCOT recommends limiting the definition of a TCA to only those functions noted in the original definition, which were transitioned to this definition. • What happens when a prescribed task (i.e., data transfer, vulnerability assessment, maintenance, or troubleshooting purposes) takes longer than 30 days? In this instance, it appears that the asset would then become a PCA, at a minimum. Cyber Assets categorized as PCAs are to be compliant upon commissioning of the asset. This would pose a problem with a Cyber Asset that was not planned to be in place for more than 30 days (a TCA), but that has been in place for at least 30 days and may exceed the 30 day time period. ERCOT recommends removing the 30 day limitation on the definition of TCA to allow focus to be on the intended purpose of the Cyber Asset. • Should clarity be added to ensure proper delineation between direct connectivity to a Cyber Asset and direct control of a Cyber Asset? ERCOT recommends modification to address this concern. ERCOT is amenable to these concerns being addressed in the manner that the drafting team determines to be most appropriate. Suggestions are modification to the guidance, which may not be considered a substantive change to the standard requirements, or issuance of a lessons learned guidance document.
No
Individual
John Brockhan
CenterPoint Energy Houston Electric LLC.
No
Reference Model 4 – CenterPoint Energy agrees with EEI’s comments. Reference Model 4 contradicts the language of the LERC definition and incorrectly identifies a LERC being present. The existence of an External Routable Connectivity (ERC) should be applied in the same manner for Low Impact BES Cyber Systems as it is applied to Medium and High Impact Cyber Systems. Utilizing an IP/Serial converter in an end-to-end session is not considered a bi-directional routable protocol. CenterPoint Energy is concerned that the interpretation could unintentionally increase the scope Medium and High Impact BES Cyber Systems with ERC. Therefore, CenterPoint Energy recommends removing Reference Model 4 from the Guidelines and Technical Basis section.
No
CenterPoint Energy generally agrees with the definitions of LERC and LEAP. However, CenterPoint Energy is concerned with how the definitions will be applied for Low Impact BES Cyber Systems. See comments in Question 1.
No
CenterPoint Energy agrees with EEI’s comments. CenterPoint recommends that the STD update the Guidelines and Technical Basis section of the standard to address the concerns related to the Transient Cyber Asset definition. See comments in Question 4.
No
CenterPoint Energy agrees with EEI’s comments. CenterPoint Energy appreciates the STD’s attempt to revise the Transient Cyber Asset (TCA) definition to meet industry concerns; however, the

proposed definition introduces confusion for Cyber Asset categorization. As currently written, the definition of Protected Cyber Asset(PCA) excludes the 30 day exemption, which may unintentionally include Cyber Assets that are covered in the TCA definition. Therefore, a Cyber Asset connected within an ESP using a routable protocol for less than 30 days may be categorized as both a PCA and TCA under the current definitions. According to FERC Order 791, these Cyber Assets should fall into the TCA category. CenterPoint Energy recommends the following revisions to the TCA definition to better align with the intentions of FERC Order 791: “A Cyber Asset that if, for 30 consecutive calendar days or less, is directly connected to a network within an ESP, a Cyber Asset within an ESP, or a BES Cyber Asset; and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. A Transient Cyber Asset is not a BES Cyber Asset or simultaneously classified as a Protected Cyber Asset.” Additionally, the STD should add clarification in the Guidelines and Technical Basis section of CIP-010 to address this issue.
Yes
Yes
CenterPoint Energy is dissatisfied that the Standard Drafting Team has made significant changes to standards that have already passed. It is important that the CIP version 5 standards be at a steady state in order to implement the standards in a timely manner. CenterPoint Energy strongly encourages the STD to make timely and appropriate revisions to the standards so that they can be at a steady state for implementation.
Individual
Joe Tarantino
Sacramento Municipal Utility District
Yes
SMUD supports and appreciates the changes made by the drafting team and the extensive Guidelines and Technical Basis documentation.
Yes
SMUD supports and appreciates the changes made by the drafting team.
Yes
SMUD supports and appreciates the changes made by the drafting team and the extensive Guidelines and Technical Basis documentation.
Yes
SMUD supports and appreciates the changes made by the drafting team.
Yes
SMUD supports and appreciates the changes made by the drafting team.
Yes
With the amount of effort from the SDT to develop significant Guidelines and Technical Basis documentation, SMUD would like to understand from NERC how this information will be used to inform the regional audit approaches; including the RSAWs and the Reliability Assurance Initiative (RAI). In previous comments provided to the RSAW development team, SMUD and others have requested to have some of the salient points from the Guidelines and Technical Basis included in the “Note to Auditor” section; however, that has not been done. SMUD understands that the Guidelines and Technical Basis are not themselves standards and enforceable, yet the section explains rationale and implementation parameters that are used by many entities to demonstrate compliance. If there are other tools that NERC and regions are developing under the RAI program, SMUD encourages NERC to engage with the SDT and the industry.
Individual
Joel Gerber
Tri-County Electric Cooperative, Inc.
Individual
Nick Braden
Modesto Irrigation District
Individual

Brenda Hampton
Luminant Energy Company LLC
Individual
Ronald L Donahey
Tampa Electric Company
No
Tampa Electric Company (TEC) participated in the development of and supports the comments of the Edison Electric Institute. In addition, we have concerns that the functional models do not address/depict serial communications. TEC offers the following scenario for consideration. We are providing the scenario in text format to accommodate the limitations of the ballot system. If requested, TEC will provide a diagram. Scenario: a user on the corporate network accesses a relay at a substation. From the corporate network, the user accesses a jump host environment that requires two-factor authentication. If successful, the user will then access an application that stores credentials to the relay. This application resides on an EACM. Once the user selects the applicable relay, the application initiates a connection to the relay. For this to happen, the EACM first connects to a Cyber Asset that resides in a DMZ. This DMZ network is an interface off of an EAP. Up until this point, all communications has been over IP. From the Cyber Asset, a serial connection is initiated to another Cyber Asset that resides at an asset boundary (i.e., substation). From this point on, all communications to the relay is done via serial. TEC's question is whether a or b is applicable: A. This scenario requires an entity to comply with LERC requirements since the initial data flow started as IP. B: Since the communication path is over serial when it crosses the asset boundary, LERC does not apply.
No
Tampa Electric Company (TEC) participated in the development of and supports the comments of the Edison Electric Institute
No
Tampa Electric Company (TEC) participated in the development of and supports the comments of the Edison Electric Institute
Tampa Electric Company (TEC) participated in the development of and supports the comments of the Edison Electric Institute
Yes
No
Individual
Judy VanDeWoestyne
MidAmerican Energy Company
No
Improvements made to low impact requirements are appreciated. In Section 2 physical security controls, we support the inclusion of monitoring controls as part of the physical security controls. The monitoring concept must be included in (CIP-003-7 Attachment 1, Section 2). For example, revise it to “Each Responsible Entity shall control or monitor physical access, …” Accordingly, the first sentence in the Guidelines and Technical Basis paragraph about monitoring could be revised to “Monitoring can be used as a physical security control or can be used as a complement to physical access controls.” The result of removing all reference to monitoring controls from the language of the standard (CIP-003-7 Attachment 1, Section 2) creates inconsistency and confusion. This could create compliance auditing and enforcement issues because although Attachment 2, Section 2 evidence examples and Guidelines and Technical Basis include monitoring, the requirement in (CIP-003-7 Attachment 1, Section 2), which is enforceable, does not. The applicability of CIP-003-7 R2 to dispersed generation resources should be limited as follows: For dispersed power producing resources identified under inclusion I4 of the BES definition, those generation resources and their associated BES Cyber Assets that are part of a BES Cyber System that impacts an aggregate nameplate generation of less than or equal to 75 MVA are excluded from Requirement R2. This is in line with the FERC-approved threshold of 75 MVA and with what has been approved by industry for

multiple NERC operations and planning standards. This concept is based on the transformation of the ERO to making risk-based decisions weighing results with resources in addition to the desire to minimize administrative burden, see FERC Order 791 footnote 85 – “The Reliability Assurance Initiative program is a NERC initiative to transform the current compliance and enforcement program into one that focuses on high reliability risk areas and reduces the administrative burden on registered entities.” Paragraph 111 states, “Based on the comments, we are persuaded that it would be unduly burdensome to require responsible entities to create and maintain an inventory of Low Impact assets for audit purposes. Creating and maintaining such a list could also divert resources away from the protection of Medium and High Impact assets. Further, we note that NERC‘s approach is consistent with its move away from embedding documentation obligations in the substantive requirements of Reliability Standards.” This concept translates similarly to creating and maintaining evidence for each individual 1.0 to 3.0 MW wind turbine or 1 MW solar inverter as being unduly burdensome. There are about 40,000 (transmission level) wind turbines in the United States. Further support is found in this excerpt from the dispersed generation resource (DGR) SAR, which states, “…. to ensure it is clear that these activities are conducted at the point of aggregation at 75 MVA, and not an individual turbine, generating unit or panel level for 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.”

Yes

No

There is confusion with the definitions referenced in these requirements. See comments about the definitions in question 4.

No

With the current “standalone” definition of a Protected Cyber Asset (PCA), a Cyber Asset that is connected using routable protocol within or on an ESP is a Protected Cyber Asset regardless of how long it is connected and what functions it performs. The revisions to the Protected Cyber Asset in Draft 2 removed the original CIP version 5 exclusion for devices connected for less than 30 days used for those specific functions. FERC acknowledged this exclusion was reasonable in paragraph 133 of the Order. One part of the definition of a Transient Cyber Asset states that it is not a Protected Cyber Asset. Therefore, PCAs, including those that are connected for 30 days or less, are excluded from being a Transient Cyber Asset. Others interpret the Transient Cyber Asset definition as the 30-day exclusion from the PCA definition. There is conflict and confusion between the two definitions. Add back the exclusion to the PCA definition to make the two definitions mutually exclusive.

Yes

Yes

We support comments provided by the Edison Electric Institute. The efforts of the standard drafting team to address the FERC directives and entity comments are very much appreciated