NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2014-02
CIP Version 5 Revisions

Consideration of Comments
Additional Comment Period

November 25, 2014

RELIABILITY | ACCOUNTABILITY

Table of Contents

Consideration of Comments: Project 2014-02 CIP Version 5 Revisions

The Project 2014-02 Standard Drafting Team (SDT) thanks all commenters who submitted comments on the draft Critical Infrastructure Protection (CIP) Reliability Standards. These Reliability Standards were posted for a 45-day public comment period from September 3, 2014 through October 17, 2014. Stakeholders were asked to provide feedback on the Reliability Standards and associated documents through a special electronic comment form. There were 70 responses, including comments from approximately 164 different people from approximately 117 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

This consideration of comments is responding to the comments received on the standards and implementation plan balloted as CIP-003-6 and CIP-010-2 during the additional comment period and ballot. These standards included revisions to address the low impact and transient devices directives. There was a concurrent 45-day comment period and ballot of the Version X standards and implementation plan that addressed only the identify, assess, and correct (IAC) and communication networks directives. The SDT's responses to comments on those revisions are available here.

All comments submitted may be reviewed in their original format on the CIP Version 5 Revisions SDT project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, please contact Valerie Agnew, the Director of Standards, at 404-446-2566 or valerie.agnew@nerc.net. There is also a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process can be found in the Standard Processes Manual. http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Introduction

The SDT appreciates industry comments on the revisions to the CIP Reliability Standards. During the development of the revised standards prior to posting, the SDT made it a priority to conduct outreach as modifications were made to the standards. The SDT conducted three face-to-face meetings to revise the standards, Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs) in order to appropriately consider all comments received. The SDT continued its rigorous conference call schedule as it understands the importance of getting these standards to steady state.

Background

On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards and also directed that NERC make the following modifications to those standards:

1. Modify or remove the “identify, assess, and correct” (IAC) language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for to assets containing low impact BES Cyber Systems.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of “communication networks” and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the IAC language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the low impact and transient electronic devices directives. The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.

Question 1: CIP-003-6

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

Placement

Several stakeholders commented on the placement of the low impact requirements in the CIP suite of standards. Tennessee Valley Authority (TVA), New York Power Authority, and Iberdrola USA commented that they preferred the low impact requirements in the relevant CIP standard rather than as a plan in CIP-003. American Electric Power (AEP) and Independent Electricity System Operator (IESO) suggested the SDT place the requirements in a table format similar to other CIP standards. However, Exelon, Edison Electric Institute (EEI), Southern Companies, MidAmerican Energy Company, NV Energy, Consumers Energy Company, FirstEnergy, Colorado Springs Utilities, Occidental Chemical Corporation, Pepco Holdings, Sacramento Municipal Utility District (SMUD), Bonneville Power Administration (BPA), and ACES Standards Collaborators expressed support for the current CIP-003 plan structure for low impact requirements.

The SDT appreciates the comments regarding the placement of the low impact requirements and determined to retain the current CIP-003 plan structure due to a majority of stakeholder support.

Attachment 1

Several commenters suggested revisions to the sections included in Attachment 1 to CIP-003-6, Requirement R2. Please note that the SDT changed the term “element” to “section” in response to several comments so the remainder of this document will use “section” even if commenters referred to “element.”

For section 1, NIPSCO, EEI, Oncor Electric Delivery Company LLC, Iberdrola USA, NV Energy, FirstEnergy, and Pepco Holdings suggested that the SDT make Attachment 1 language consistent with Attachment 2 by using “through one or more of the following” and labeling Attachment 1 sections similar to Attachment 2. Dominion also commented that Attachment 1 should be consistent with Attachment 2. Exelon suggested that the SDT relocate the bullets from the requirement in Attachment 1 to the measures in Attachment 2. Exelon further commented that the SDT should remove “its” because it is more prescriptive than CIP-004-6, Requirement R1. Massachusetts Municipal Wholesale Electric Company (MMWEC), Colorado Springs Utilities, Indiana Municipal Power Agency (IMPA), SMUD, BPA, and Florida Municipal Power Agency (FMPA) recommended changing “once every 15 calendar months” to “at least once every 15 calendar months.” In response to these comments, the SDT changed the word “element” to “section” throughout the standard, moved the bullets from the requirements language to the measures, removed “its” as suggested, and revised the requirement to read “at least once every 15 calendar months.”

For section 2, Dominion, MMWEC, MidAmerican Energy Company, MRO NERC Standards Review Forum, and Luminant Generation Company commented that “based on need” should be removed. SPP-RE commented that the phrase “based on need” should be moved to earlier in the sentence. Dominion, NIPSCO, EEI, Oncor, Southern Companies, Iberdrola USA, NV Energy, FirstEnergy, Pepco Holdings, SMUD, BPA, and IMPA recommended that the SDT ensure that the terms for physical controls are consistent between attachments and suggested using the term “physical security controls.”

The SDT revised CIP-003-6, section 2 to clarify that the Responsible Entity is obligated to “control physical access” at the asset or location containing the low impact BES Cyber System. 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. This revision addresses the FERC Order No. 791 directive to add objective criteria or specificity to the requirement.

Note, in response to other comments, the SDT changed "access" to "security" and "to restrict" to "control" and made the suggested change to "physical security controls."

Dynegy suggested that the SDT use "or" rather than "and" in section 2 and commented that an inventory is required if the language used "and." The SDT appreciates the comment. The SDT used "and" to restrict access to both the asset/location of the BES Cyber System and the LEAP should it reside outside of the asset/location. Entities would need to physically protect two spots if they were separate. The graphics in the guidance shows this scenario for electronic access. If the LEAP is located within the asset containing the low impact BES Cyber System, the entity would need to show how the asset containing both the LEAP and the low impact BES Cyber System is protected. It is still one obligation to show how physical access controls are being applied to either item. The intent of the language is for an entity to have an inventory of the LEAPs, but not inventories of low impact BES Cyber System(s) and their individual Cyber Assets.

Nebraska Public Power District (NPPD) recommended that section 2 requirements for physical security be deleted and the vulnerabilities are covered by national Electrical Safety Code, Section 11. The SDT thanks you for the comments. CIP-003-5 incorporated physical security obligations for assets/locations with low impact BES Cyber Systems into the suite of requirements under the NERC purview. FERC approval of CIP V5 and the Order No. 791 directives obligate the drafting team to retain the physical security requirements.

AEP and Xcel Energy commented that section 2 is more prescriptive than medium impact without External Routable Connectivity and would be a compliance burden. The SDT revised CIP-003, section 2, and removed some of the specific list of physical security controls. Section 2 retains "based on need" as a qualifier to physical security controls, but it's used to make the section objective clear.

For section 3, TVA commented that establishing a LEAP assumes an ESP which is subject to CIP-005-5, Requirement R1 with inbound and outbound access subject to CIP-007-6, Requirement R1. The SDT thanks you for your comment. The requirements for low impact BES Cyber Systems are contained solely within CIP-003-6, R2. No other CIP standards related to high and medium impact BES Cyber Systems apply.

EEI, Oncor, Southern Companies, Iberdrola USA, FirstEnergy, Pepco Holdings, SMUD, BPA, IMPA, Entergy Services, and American Public Power Association (APPA) commented that the LERC and LEAP acronyms were missing from sections 2 and 3. The SDT added the acronyms where appropriate in the requirement.

For section 4, Dominion, CenterPoint Energy Houston Electric, EEI, NIPSCO, Oncor, Southern Companies, Iberdrola USA, NV Energy, Consumers Energy Company, Xcel Energy, MRO NERC Standards Review Forum, FirstEnergy, Pepco Holdings, and Luminant Generation Company suggested that the SDT add "if needed" to the requirement to update the Cyber Security Incident response plan(s). Exelon requested that the SDT clarify the intent of the phrase "either by asset or groups of assets" to confirm whether enterprise-wide plans could fulfill the obligations. Exelon, MidAmerican, and NRECA requested that the SDT justify the addition of 4.6 and 4.7 and the 180-day clock because it could cause entities to maintain multiple clocks for different impact levels. SPP-RE commented that the record retention requirement in Section 4.6 does not make sense and recommended that the requirement establish a minimum expectation. SPP-RE further commented that the updates for Section 4.7 take place at the same frequency as that of medium and high impact BES Cyber Systems.

The SDT confirms that the phrase "either by asset or by groups of assets" accommodates use of an enterprise-wide plan for multiple assets or locations to fulfill the obligation. The SDT added language to the guidelines to emphasize the point. The SDT removed 4.6; however, retained 4.7. The SDT finds the updating of the Cyber

Security Incident response plan following a test or actual Reportable Cyber Security Incident to be a valuable security step, if updates are needed. The SDT added "if needed" in recognition that updates may not always be needed. The SDT retained the "180 calendar days" time period for updates. This is a reasonable amount of time to make updates. Entities may make the updates sooner ("within 180 calendar days") if preferable for their program.

MMWEC suggested changing identification, classification, and response to Cyber Security Incidents to identification and classification because response is a subset of incident handling. In addition, MMWEC commented that because the testing is every 36 months, entities should be required to ensure individuals are aware of their response roles through more frequent training or review their responsibilities. Consider review roles at least once every 15 calendar months. The SDT thanks you for your comments. In the initial comments, stakeholders preferred a closer alignment between the CIP-008 and the CIP-003 elements to help accommodate entities that will have multiple impact levels. Given the risk, the SDT thinks 36 months is appropriate.

Northeast Power Coordinating Council (NPCC) requested clarification where dividing line is between section 4 and EOP-004. The SDT notes that EOP-004-2 does not cover the reporting of Cyber Security Incidents. Entities may choose to use the same plan used for EOP-004-2 for Reportable Cyber Security Incidents.

Lincoln Electric System and Consumers Energy Company commented that section 4 is virtually identical to CIP-008-5 for medium and high impact BES Cyber Systems and noted that the requirement would be burdensome for low impact without External Routable Connectivity. The SDT removed 4.6 to reduce the burden. The requirement allows Responsible Entities to use an enterprise Cyber Security Incident response plan and not develop individual by asset or device to also reduce the burden.

Texas Reliability Entity (TRE) recommended that additional elements be added to CIP-003 regarding low impact to reduce the risk to high and medium impact assets: information protection, recovery functions, system security functions, and configuration change management. The SDT thanks you for the comments. The SDT considers the controls for low impact BES Cyber Systems to be appropriate to their level of risk to the Bulk Electric System.

Entergy Services suggested that the SDT align the electronic access controls with the physical access controls to provide entities latitude. The SDT thanks you for the comments. The SDT considers the controls for low impact BES Cyber Systems to be appropriate to their level of risk to the Bulk Electric System.

Exelon expressed support of the standalone nature of the requirements in sections 2 and 3 and states they are consistent with medium and high impact requirements but tailored to lows. The SDT thanks you for the comment.

Kansas City Power and Light and BC Hydro commented that the protections are too detailed and excessive and represent too large a pool of assets that do not have a substantive impact to the Bulk Electric System. The SDT thanks you for the comments. The SDT considers the controls for low impact BES Cyber Systems to be appropriate to their level of risk on the Bulk Electric System.

Attachment 2

TVA commented that Attachment 2 does not offer much clarity beyond what is already documented in Attachment 1 and examples of evidence should be documented in table format. The SDT thanks you for your comments but notes that it received support of the details outlined in Attachment 2.

Dominion, NIPSCO, EEI, Oncor, Southern Companies, Iberdrola USA, Xcel Energy, SMUD, BPA, APPA, and IMPA commented that section 2 of Attachment 2 did not include "perimeter controls" like the guidelines and suggested section 2 include it. The SDT added "perimeter controls" to Attachment 2 as recommended.

MMWEC suggested that the SDT change "(e.g. IP addresses, ports, services) to "(e.g. by restricting IP addresses, ports, and/or services)" and to move the phrase following "deems necessary." The SDT added the text "(e.g. by restricting IP addresses, ports and/or services)" as recommended.

List of Assets

TVA commented that the CIP-003-6 Guidelines that say "using the list of assets from CIP-002" contradicts CIP-002-5.1, Requirement R1, Part 1.3 which states "a discrete list of low impact BES Cyber Systems is not required." Exelon Companies, Idaho Power, Xcel Energy, and NRECA requested the SDT to discuss how to demonstrate compliance without a list of Systems and suggested the SDT add guidance on the note in the requirement.

The SDT notes that the list of assets containing low impact BES Cyber Systems from CIP-002-5.1 ("Part 1.3 list") is different from a discrete inventory of low impact BES Cyber Systems and the Cyber Assets that make up the low impact BES Cyber System ("cyber list"). The Part 1.3 list of generation plants, substations, control centers, etc. must be maintained and provided at audit. The cyber list; however, is not required. A cyber list would encompass every Cyber Asset in every BES asset across the NERC region. The SDT determined and FERC supports in Order 791, the effort to flawlessly maintain the cyber list over the audit period at each BES asset does not match the level of risk.

The items in CIP-003-6 Attachment 1 were written to be assessed at a physical asset containing low impact BES Cyber System(s) site level. The cyber security policies, awareness program, and incident response plan can be assessed through the assessment of the documented processes. The physical security controls can be assessed at the site level. The electronic access controls were developed to focus protection on the presence of Low Impact External Routable Connectivity (LERC) and establishing boundary protection with LEAP(s), if any. It is intended that entities will have an inventory of LEAPs, if any, but not a cyber list of the individual low impact BES Cyber System(s) Cyber Assets. An assessment may spot-check an asset containing low impact BES Cyber System(s) site to determine whether the cyber security plan(s) meets the objectives of the physical security controls at the asset containing the low impact BES Cyber Systems and whether LERC exists and LEAPs are properly established. However, a Cyber List of the low impact BES Cyber System(s) or their associated Cyber Assets is not required to perform this assessment.

Other

TVA commented that the Violation Severity Levels (VSLs) for CIP-003, Requirement R2 are in the Severe category but apply to low impact systems. The SDT notes that VSLs do not measure risk but the level of violation of the requirement. The VSL construct indicates that a binary VSL would use the Severe column. In addition, the VRF assesses risk, and the requirement's VRF is Lower.

TRE recommended replacing "its" with "a Responsible Entity's" in the Rationale of Requirement R1. The SDT replaced "its" with "a Responsible Entity's" per the recommendation.

Lincoln Electric System recommended replacing the term Bulk-Power System with Bulk Electric System in the Rationale of Requirement R2. The SDT replaced Bulk-Power System with Bulk Electric System as recommended.

Dominion suggested revising the Requirement R2 guidance to state, "The SDT is balancing the fact that low impact BES Cyber Systems are indeed low impact to the BES, but they do still meet the definition of having a 15-minute adverse impact so some protections are needed." Dominion also suggested revising the guidance to state, "Low Impact BES Cyber System Electronic Access Point (LEAP) – a Cyber Asset interface that allows Low Impact External Routable Connectivity." The SDT revised the sentences but retained the concepts.

NIPSCO, EEI, Oncor, Iberdrola USA, AEP, and Pepco Holdings recommended removing the sentence that states, “Individually, these low impact BES Cyber Systems pose a relatively lower risk to the BES than other BES Cyber Systems, but in aggregate or through communication dependencies, they have the potential to create an adverse reliability impact if compromised” because aggregating low impact BES Cyber Systems across multiple sites does not reflect a true risk-based assessment and therefore this sentence is not accurate. The SDT removed the sentence form the Rationale for Requirement R2.

NIPSCO, EEI, Oncor, Iberdrola USA, and Pepco Holdings commented that the bold subtitles in the Guidelines are inconsistent with section language in Attachment 1 and recommended changing the titles for Cyber Security Awareness and Physical Security Controls. The SDT revised the titles accordingly.

Exelon suggested that the SDT consider using “require” or “obligate” rather than “imply” in the guidance on Requirement R1, Attachment 1 – Physical Security and suggested making LEAP plural in the same section. The SDT revised the language to say “require.” The SDT thanks the commenter for the suggestion to make LEAP plural but ultimately removed the language.

Southern Companies commented that the scenario for LERC and LEAP in the Attachment 2 Guidelines is unclear as to which firewall is the LEAP and suggested adding a scenario where there is LERC and an entity has flexibility to determine the LEAP. The SDT added additional scenarios to the Guidelines to clarify LERC and LEAP.

Southern Companies also suggested that the SDT rephrase the Guidelines to state, “However, the LERC between assets ‘behind’ the LEAP must pass through the single LEAP.” The SDT revised the language accordingly.

Southern Companies, SMUD, BPA, IMPA, and APPA commented that the SDT should revise the Guidelines regarding EACMS and LEAPs and suggested that the SDT create a paragraph stating, “However, a LEAP can be implemented within the same Cyber Asset that is serving the function of EACMS or EAP for a medium or high impact BES Cyber System. This is possible because a LEAP is the interface on the controlling Cyber Asset (e.g. firewall or router) and not the Cyber Asset itself.” The SDT addressed EACMS in the context of LEAPs in the Guidelines.

SPP-RE commented that the Guidelines for Requirement R2 states that monitoring does not imply logging and questioned how a Responsible Entity can demonstrate effective monitoring without recording unauthorized access or attempts at access. In response, the SDT notes that monitoring includes human observation or alerting mechanisms, and the retention of access logs is not required to implement monitoring controls.

Luminant Generation Company suggested several revisions to the Guidelines. For the Guidelines on Requirement R2, Attachment 1, Luminant commented that a discussion on LERC was not clear and recommended revisions to state, “SDT intends IED to IED communications be exempt from any requirement to use an LEAP even if there is LERC. Through this exemption, the SDT intends to not preclude the use of time-sensitive reliability enhancing data exchanges.” In response, the SDT revised the LERC definition for clarity. Luminant suggested that the SDT revise the sentence regarding LEAPs and EACMS to read, “A LEAP is not to be considered an EACMS. In response, the SDT developed additional guidance regarding LEAPs and EACMS. Luminant suggested that the SDT replace “interface” with “internal interface” in the Guidelines describing LEAP. The SDT appreciates the comment but retains the language to better convey the practical use of interface in the definition. Luminant also suggested revising the Guidelines on LEAP to state, “…must also pass through a LEAP” instead of “must also pass through the single LEAP.” Furthermore, Luminant suggested deleting “physically” from “unidirectional gateway that physically enforces outbound-only data flows.” For the sentence beginning “The electronic access controls,” Luminant suggested that the SDT replace shall with should. Finally, Luminant suggested that the SDT delete the sentence regarding assets without LERC and real-time monitoring. The SDT revised the language according to these suggestions but removed “unidirectional gateway.”

Hydro-Quebec commented that the compliance date for electronic access controls is after the date for physical security controls in the Implementation Plan. The SDT has modified the Implementation Plan to make the compliance date for electronic access and physical security controls consistent.

MidAmerican and PacifiCorp recommended that the SDT continue working with the drafting team regarding dispersed generation applicability to determine what, if any, requirements apply to dispersed generation. The CIP SDT will continue to collaborate with the DGR SDT to address concerns with CIP and DGR.

Exelon, NYPA, Seattle City Light, MidAmerican, SMUD, BPA, IMPA, and APPA expressed concern that in a multi-impact rated program any failure to fulfill a requirement such as those in Sections 1 and 4 in Attachment 1 could result in violation of CIP-004 and CIP-008 as well. The SDT collaborated with NERC Enforcement in response. Responsible Entities may choose to implement multi-impact rated programs to address low, medium, and high impact BES Cyber Systems. It is possible the same facts and circumstances may indicate noncompliance of both the requirements applicable to low impact BES Cyber Systems and the corresponding requirements applicable to high and medium impact BES Cyber Systems. That the same act or omission may result in two separate violations is not unique to the CIP V5 standards. For example, the same failure to act immediately could constitute a violation of both TOP-001-1a R2 and TOP-008-1 R1. NERC's *Sanction Guidelines* provide that one penalty may be assessed where there are multiple violations arising from a single act or common incidence of noncompliance. Therefore, if a penalty is assessed at all, it would not be duplicated. In addition, the disposition of any noncompliance is based on the level of risk posed to the reliability of the BPS. Therefore, in the event one or more of the instances of noncompliance poses a minimal risk, a number of streamlined options is available, including treatment as a compliance exception. As with any noncompliance, a determination of whether compliance exception treatment will be appropriate in a given case will depend on the facts and circumstances.

Question 2: Low Impact Definitions

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

LERC in DMZ

TVA, EEI, NIPSCO, Oncor, Iberdrola USA, and FirstEnergy requested clarity regarding the scenarios in the Guidelines, specifically where the LEAP is located in the diagram and when LERC exists. TVA commented that it is unclear whether LERC exists in a scenario where all external communication is through a jump host or historian in a demilitarized zone (DMZ). The SDT added additional diagrams to the Guidelines and modified the definition to provide more clarity regarding LERC. The new definition states LERC is "*direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s)….*"

In the Guidelines, it clearly demonstrates that if all communication from the low impact BES Cyber Systems is internal (e.g. the DMZ is implemented in such a way to restrict all external communication to the BES Cyber System), then LERC does not exist. In this case, the objective of protecting the low impact BES Cyber System is achieved.

Be aware, however, that if the low impact BES Cyber System has established bi-directional routable communication to an external Cyber Asset, then LERC does exist. This would be the case even if the low impact BES Cyber System communicates through a jump host DMZ using the same protocol session with an external Cyber Asset.

LEAP "Allows"

TVA, EEI, NIPSCO, NV Energy, Oncor, Southern Companies, Iberdrola USA, FirstEnergy, MRO NERC Standards Review Forum, and SMUD commented that the term "allows" in the definition is too broad and suggested that the SDT consider "controls" or "restricts." Duke Energy suggested using "permits." NPCC and NYPA commented that the guidance states "allows and controls" whereas the definition states "allows." The SDT agrees there is an inconsistency and changed "allows" to "controls" in both the definition and the guidance.

61850 Exclusion

Several stakeholders commented on the exclusion included in the LERC definition. Dominion, EEI, NIPSCO, NV Energy, Oncor, Southern Co, Iberdrola USA, and FirstEnergy requested clarification in the guidance that LERC excludes "point to point communications (e.g., between Intelligent Electronic Devices over fiber) that use routable communication protocols for time-sensitive protection or control functions." PacifiCorp and MidAmerican commented that the exclusion used undefined terms that cause confusion and refer to specific technologies which may become obsolete over time. In addition, PacifiCorp and MidAmerican commented that the exception seems to remove protections indiscriminately rather than addressing the assets to be protected. MidAmerican further commented that the use of capital letters for Intelligent Electronic Device creates confusion because it is not a defined NERC Glossary term and requested that the SDT explain why there is no exclusion for medium or high impact assets. NPPD commented that LERC should specifically exclude communications aiding in relaying used for pilot relaying protection and that the definition should be written to avoid technical terms. Pepco Holdings requested additional guidance on the exclusion.

The SDT revised the exclusion according to the suggestion to use "point to point communications…." The SDT coordinated with protection engineers to ensure the language was clear as to the exclusion. The SDT also put intelligent electronic device into lower case letters. The SDT considered removing the technologies in the parentheses but determined that the examples provided clarity for some stakeholders. The SDT reviewed the language to limit technical terms as necessary and ultimately determined that the revisions made to the definition provide as much detail as necessary to reflect the SDT's intent. The SDT considered guidance related to the definition but determined that guidance would not be helpful because the terms would be moved to the NERC Glossary where there is no associated guidance. Therefore, the SDT focused on including detail in the definition rather than explanations in the guidance. Regarding the lack of exclusion for medium and high impact, the SDT considered this exclusion appropriate for low impact BES Cyber Systems because of the lower level of risk and large scale of applicability. The SDT explains the rationale for the exclusion in guidance stating the intent not to require a LEAP even though there is LERC or to preclude the use of such time-sensitive reliability enhancing functions if they use a bi-directional routable protocol.

Acronyms

EEI, NIPSCO, Oncor, Iberdrola USA, and FirstEnergy suggested that the SDT use the LEAP and LERC acronyms throughout the standard. The SDT agrees and added the acronyms in the definition and throughout the standard.

LEAP and EACMS

Several stakeholders commented on the relationship between LEAP and Electronic Access Control or Monitoring System (EACMS). EEI, NIPSCO, Duke Energy, Iberdrola USA, FirstEnergy, and FMPA commented that the definition and guidance for LEAP does not clearly explain that the Network Interface Card (NIC) (a port) is the LEAP rather than the device containing the NIC and that it is possible to have a NIC port inside a high or medium impact BES Cyber System Electronic Security Perimeter (ESP) in an EACMS. The commenters recommended additional guidance on the relationship between the LEAP and EACMS. TRE recommended removing the last sentence of the LEAP definition regarding EACMS.

The SDT removed the sentence "The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System." The SDT also revised the guidance to address the relationship between LEAP and EACMS.

BPA commented that using the term "access point" in LEAP creates confusion with medium and high impact EAP. The SDT thanks you for your comment. The SDT determined that the similar concepts from the medium and high impact EAP assisted entities in understanding expectations. However, the SDT revised the definition in response to comments to improve clarity.

Other

Entergy Services commented that it disagrees with the application of acronyms to only low impact. The SDT discussed the trade-offs of developing and applying a definition to only one standard. While not ideal to create definitions used in one standard, it resolved many clarity concerns the SDT had with the requirement language. The SDT decided that clarifying the terms used in the requirement language was beneficial.

MMWEC commented that "low impact BES Cyber System" should be "BES Cyber Systems associated with Low Impact assets" and that the SDT should consider changing "communication protocols created" to "communication using protocols created." The SDT thanks you for your comments. In the CIP-002-5 categorization, entities categorize the assets containing low impact BES Cyber Systems. The term low impact assets is not used. The phrase "communication protocols created…" has been replaced.

IESO commented that the definition for LERC states that "Bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s)" and suggested that the statement should include both BES Cyber Systems and BES Cyber Assets as LERC should apply to both systems and assets. The SDT thanks you for the comment. Per the definition, a BES Cyber System is one or more BES Cyber Assets and every BES Cyber Asset must be in one or more BES Cyber System(s); therefore it is a superset and includes both.

AEP commented that the definitions create confusion where they refer to "asset" when it appears the term should be "facility" and suggested changing the second lowercase use of the word "asset" in each definition to be "facility." The SDT thanks you for your comment. The SDT previously considered the term “facility” but this term in lower case creates other challenges. The SDT selected “assets” to be consistent with CIP-002, which cites “assets” containing low impact BES Cyber Systems.

MidAmerican asked whether the Background in the Applicability section of CIP-003 should include the following phrase in the Background section of other CIP standards: “This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.” The SDT thanks you for your comment. The Background for CIP-003 is different from that within CIP-004 though -007 because low impact BES Cyber Systems are distinguished from high and medium impact BES Cyber Systems. This is not relevant for CIP-003-7 because the external routable connectivity is not used in reference to applicability.

Xcel Energy requested clarification on whether the logical network protected by the LEAP extends beyond a physical boundary and on whether the LERC definition is referring to access to or from a system or network. The SDT confirms the logical network protected by the LEAP may extend beyond a physical boundary. The SDT also confirms that designation of a LEAP does not imply additional obligations such as those for EACMS associated with medium or high impact BES Cyber Systems. All obligations for low impact BES Cyber Systems are found in CIP-003-7, Requirement R2.

Kansas City Power and Light (KCPL) and SPP and specific members commented that the new definitions are not clear. They commented that entities should describe their connectivity to their assets and how that’s managed. The SDT attempted many iterations of requirement language before defining the new terms. Use of the terms within the requirement language streamlined the requirement language and made it much clearer to understand the requirement obligations. Clearer requirement language reduces the risk of contradictory interpretations.

Encari requested clarification on the LERC definition and external connectivity and suggested “outside the network” instead of “outside the asset.” The SDT thanks you for your comment. The phrase “outside the asset” is intentionally used to keep the level of control at the asset/location level, but to accommodate the scenario in which a LEAP is located outside of the asset containing low impact BES Cyber Systems. The definition is not making a demarcation at the system level.

SPP-RE commented that it does not agree with the definition of LEAP because a LEAP may be placed external to the asset. Specifically, SPP-RE commented that protected assets could be exposed to the risk of unauthorized access if the communication circuits are over public Wide Area Networks using third-party service providers. In response, the SDT notes that a LEAP may be placed external to the asset, but all LERC must still be protected by a LEAP. The allowance of having an external LEAP does not provide the opportunity of having a Cyber Asset with unrestricted access to the low impact BES Cyber System. In addition, a LEAP must have physical security controls according to Section 2.

SPP-RE agreed with the definition of LERC. The SDT thanks you for your support.

Question 3: Transient Devices

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

Transient Cyber Assets Managed by the Responsible Entity

KCPL, SPP and specific members, and NPPD commented that Attachment 1, Section 1.2 contains requirements covered in other standards and should be removed. The SDT appreciates the comments received. However, the authorization in Element 1.2 is needed to identify who is specifically allowed to use these devices. The SDT agrees that these users may be a subset of the CIP-004-6 authorized users but contends that not all users will be listed in a program, (e.g., medium impact BES Cyber Systems without External Routable Connectivity does not require CIP-004-6 authorizations). Furthermore, CIP-004-6 requires authorization of the individual, whereas CIP-010 section 1.2 allows flexibility to document by individual or group. In response to your comment, the SDT revised the guidance for improved consistency.

AEP commented that section 1.2 regarding authorization of users is not practical when Transient Cyber Assets do not have External Routable Connectivity. The SDT appreciates the comment. However, the SDT considers authorization of users, regardless of External Routable Connectivity, to be necessary to address the risks posed by Transient Cyber Assets.

Luminant commented that section 1.3 “live operating system and software executable only from read-only media” is not clear. The SDT appreciates the comment. However, the SDT considers the current language to be in alignment with the intent of the requirement and technology available. Further, the SDT has concerns with Luminant’s recommendation related to “other required executables”. “Required” could introduce additional documentation elements that would be difficult to sustain. Additionally, Luminant suggested that the SDT should revise the section title for sections 1.4 and 1.5 to include “prevention” and recommended changing the requirement to include prevention and mitigation “if necessary.” The SDT appreciates the comment. However, the SDT considers the title to be appropriate in defining the expectations and in line with the structure of the other elements. The SDT avoided using the term “prevent” to emphasize mitigation efforts over potential compliance concerns with a 100% performance standard that could be associated with “prevent”. With regards to the addition of “if necessary” making the addition would further confuse the required actions.

SPP-RE commented that Section 1.4 should include a requirement to ensure any Removable Media is externally scanned for malware before use with a transient device. The SDT appreciates the comment. Scanning of Removable Media on the Transient Cyber Asset is not prohibited. The malicious code mitigation methods used by the Transient Cyber Asset could suffice in meeting this objective. Additionally, the SDT revised 3.2 to clarify that methods to detect malicious code on Removable Media are to be used on a Cyber Asset other than a BES Cyber System or Protected Cyber Asset.

Southern Companies suggested revising section 1.5 to state “The Transient Cyber Asset must reside within a location with restricted physical access.” The SDT appreciates the comment. The SDT revised the language to read “Restrict physical access.”

Transient Cyber Assets Managed by a Party Other than the Responsible Entity

Dominion and NPCC suggested revising sections 2.1 and 2.2 to state “at least one.” The SDT appreciates the comments received. However, the language currently obligates an entity to use “at least one” through the requirement to “or a combination of” methods. The SDT made additional revisions to clarify the requirements.

Dominion commented that the “per Transient Cyber Asset capability” should be added to section 2.2. The SDT agrees with the comment and has revised the Requirement to address this concern.

SPP-RE commented that the review of a policy or process outlined in Sections 2.1 and 2.2 needs to include a step to confirm that the policy or process has been implemented for the transient devices. The SDT appreciates the comment. The entity is obligated to meet the objective of the requirement to mitigate the risk of software vulnerabilities and malicious code and demonstrate how this was accomplished for parties other than Responsible Entities. The SDT considers these appropriate controls for Transient Cyber Assets managed by a party other than the Responsible Entity in cases where complete verification may not be possible.

BC Hydro recommended that the SDT revise the requirements applicable to Responsible Entities regarding devices owned or managed by other entities because it would be infeasible to monitor other parties’ devices. The SDT used the concept of a “plan” to allow the entity to define the controls and processes that are most appropriate to their organization. This includes determining how the entity will handle devices not under their management with the objective of meeting the performance requirements in Attachment 1, Section 2. Options are provided to enable the entity to be successful in protecting their systems from devices managed by parties other the Responsible Entity.

Exelon asked whether contract obligations could fulfill section 2. The SDT’s response is yes, and further details are included in the Guidelines. To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department Of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [2] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party’s support. Entities should consider the “General Cybersecurity Procurement Language” and “The Supplier’s Life Cycle Security Program” when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

NPCC suggested adding authorization of vendor or contractor use of Transient Cyber Assets to section 1.2. The SDT appreciates the comment. The intent was not to require the entity to document vendor or contractor managed devices in the same manner as their own assets. However, entities should note that they need to demonstrate that the contractually obligated process was followed.

EEI, NIPSCO, Southern Companies, SMUD, MidAmerican, MISO, NPCC, and Iberdrola USA suggested adding “if necessary” to section 2.3 to clarify that entities can accept the device without requiring modifications. The SDT agrees with the comment, but opted to use “any” rather than “if necessary” for sentence structure.

CenterPoint recommended revising section 2.2 to read “...operating system software and other required executables *installed* from read-only media.” The SDT appreciates the comment. However, the current language

[2] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

does not include the obligation to determine what is “required” to be installed on the device. It is simply to require all software, including the operating system be on read-only media.

AEP commented that section 2 should be removed because vendors and contractors are not subject to CIP requirements. The SDT appreciates the comments received and recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity’s responsibility to protect against the introduction of malicious code on their BES Cyber Systems. The SDT used the concept of a “plan” to allow the entity to define the controls and processes that are most appropriate to their organization. This includes determining how the entity will handle devices not under their management with the objective of meeting the performance requirements in Attachment 1, Section 2. Options are provided to enable the entity to be successful in protecting their systems from devices managed by parties other than the Responsible Entity.

Removable Media

EEI and CenterPoint commented that Section 3.2 does not require the entity to take any action other than scanning Removable Media. The SDT agrees with the comment and revised the CIP-010, Attachment 1, Section 3.2 to address this concern.

EEI, AEP, and CenterPoint commented that Section 3.2 should be revised because it presumes that scanning takes place on an external system when technology exists on USB drives, for example, to do scanning. The SDT appreciates the comments received. The SDT extensively discussed and revised Section 3.2 to clarify the obligations. The language seeks to address the risks of scanning for malicious code on the BES Cyber Asset and to prevent introduction of malicious code on the BES Cyber Asset. While the requirement does not address virus scanning on USB drives specifically, it does not preclude the use either since it is external to the BES Cyber Asset. Evidence could include documentation of the implementation of antivirus on the scanning system or procedural documentation of the actions taken. The methods used by the entity should be addressed in the plan document(s). The Guidelines and Technical Basis has been modified to address this matter.

Exelon asked how often entities should scan Removable Media to fulfill Section 3.2. The SDT revised the Guidelines to address this concern.

TVA commented that it is not necessary that a user of an authorized Removable Media device have electronic access to the applicable system because an individual with physical access to a system could be connecting removable media for someone with electronic access but working remotely. The SDT appreciates the comment. To clarify, the entity is required to include in their plan authorization of those using the Transient Cyber Asset or Removable Media to connect to a BES Cyber System. References to CIP-004 authorizations within the guidance have been updated.

BC Hydro commented that Section 3 should be revised to provide clarity regarding authorized users. The SDT extensively discussed Section 3 and revised the Guidelines and Technical Basis.

Measures & Guidance

EEI, NIPSCO, SMUD, Southern Companies, MISO, and MidAmerican requested that the Guidelines address authorization based on a group of assets. The SDT revised the Guidelines and Technical Basis to address this concern.

EEI and NIPSCO recommended that the SDT remove the restatement of requirement language from the Attachment 2 as it is not an example of evidence. The SDT thanks you for and agrees with the comment and revised Attachment 2 to address this concern.

NIPSCO, Southern Companies, and NV Energy commented that Section 3.2 of Attachment 2 should include examples of capabilities or embedded, real-time virus scanning and encryption on USB drives. The SDT appreciates the comment and revised Attachment 2 to address this concern.

Luminant recommended removing the last sentence of the measures for Sections 1.3, 1.4, 1.5, 2.1 and 2.2. The SDT thanks you for the comment; however, the team considers the last sentence to be support of "per Transient Cyber Asset capability" noted in the section.

TRE recommended adding the following language to M4: "including but not limited to a list of in-scope transient devices, and manual or automated logs showing connection periods...." The SDT thanks you for your comment. The use of these devices is limited to the context of change management and vulnerability assessment. The use of a plan to document how the entity implements the requirement should be the sole evaluation criteria for consideration in determining and proving compliance.

ACES Standards Collaborators requested the SDT develop additional guidance regarding what is not considered a transient device. The SDT thanks you for your comment but notes that prior comments requested that guidance on "what is not a transient device" be removed. It is not feasible to note all of the possibilities of what could be included in this list.

EEI, NIPSCO, Southern Companies, FMPA, IMPA, and AEP requested guidance that mitigation does not require that every vulnerability is addressed, as many may be unknown or not have an impact on the system. The SDT thanks you for and agrees with the comment and revised the Guidelines and Technical Basis to address this concern.

EEI, NIPSCO, Southern Companies, and CenterPoint requested clarification in the Guidelines and Technical Basis that the Responsible Entity has flexibility in determining how and when to manage vulnerability and malicious code reviews of their vendors or contractors and when additional mitigation actions are necessitated. Thank you for the comment. The SDT had previously addressed this concept in the Guidelines and Technical Basis. However, additional changes have been made to clarify further.

Luminant suggested the SDT revise the Guidelines and Technical Basis discussion of Section 1.5 to read, "Disk encryption will not protect a Transient Cyber Asset from unauthorized physical access" and "...Physical Security Perimeter or other physical location that manages physical access...." The SDT thanks you for the comment and has revised the Guidelines and Technical Basis to address this concern. Luminant also recommended deleting the statement "Entities should also consider whether malicious code is a Cyber Security Incident" in the Guidelines. The SDT thanks you for your comment but considers this to be important clarifying language to provide appropriate reminders to entities.

TVA suggested removing the following statement from the Guidelines: "Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. These user(s) must have authorized electronic access to the applicable system in accordance with CIP-004." The SDT appreciates the comment. References to CIP-004 authorizations within the guidance have been updated.

Miscellaneous

Duke Energy, KCPL, and SPP and specific members requested clarification on how often an entity needs to review the Transient Cyber Assets owned or managed by vendors or contractors. Thank you for the comment. The SDT used the concept of a "plan" to allow the entity to define the controls and processes that are most appropriate to their organization. This includes the timing and frequency of performance of required sections from Attachment 1.

EEI, NIPSCO, and Southern California Edison Company commented that the placement of “CIP Exceptional Circumstances” is unclear in Requirement R4. The SDT agrees with the comment and revised the requirement to address this concern. Thank you for the comment.

EEI, NIPSCO, and Southern Companies commented that some Transient Cyber Assets could fall under both Sections 1 and 2 in certain circumstances and recommended removing “owned” from the requirements. The SDT thanks you for the comment and agrees with the comment. The SDT revised the requirements to address this concern by removing “Owned or” from Sections 1 and 2.

Hydro-Quebec Production commented that the impacts from these requirements are major for utilities. The SDT thanks you for the comment. However, requirement language is needed to address FERC Order No. 791 directives.

IESO and AEP suggested that transient devices requirements should be in the table format and transient devices should be added to the Applicable Systems column. The SDT appreciates the comment. The SDT received strong support for the plan and attachment format to allow entities flexibility in determining how to fulfill the security objectives based on the entity’s specific facts and circumstances. Therefore, the SDT determined not to put the requirements into a table format.

MMWEC commented that the requirements should be limited to objectives and not specify controls, which should go in the measures. Thank you for your comment. The SDT discussed your recommendation extensively and chose to keep the bullets in Attachment 1. The SDT considers the options listed in Attachment 1 to be necessary and enforceable requirement obligations supporting Requirement R4.

TVA commented that Requirement R4 and its attachment do not clarify what is included in a plan. The SDT thanks you for your comment. The “Background” section of the Standard includes definitions of what constitutes a plan, program, or process. The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter. Similarly, the term program may refer to the organization’s overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

TRE suggested the SDT apply the transient devices requirements to low impact. Thank you for your comment. Due to the wide-area impact of the high and medium impact assets, the SDT limited the requirements to those systems. This includes protection when connecting Transient Cyber Assets to multiple-impact rated systems.

EEI, NIPSCO, Southern Companies, Dominion, MRO NERC Standards Review Forum, NV Energy, MidAmerican, and PacifiCorp commented that the use of “Authorized” in 1.2.1, 1.2.2, 1.2.3, 3.1.1, and 3.1.2 is redundant and unnecessary in that the language of 1.2 and 1.3 requires a Responsible Entity to specify a user, location, and use for each Transient Cyber Asset (or group of) and specify a user and location for each Removable Media, which means an authorization for the Transient Cyber Asset. The plan should include authorization, which identifies the users, locations, and uses for each Transient Cyber Asset (or group of) and users and locations for each Removable Media, giving the Responsible Entity flexibility on how they write the plan to address these authorization elements. Thank you for your comment. In response, the SDT agrees with the comment and revised Attachment 1 to address this concern by changing “specify” to “authorize.”

Southern California Edison suggested that Attachment 1 be revised to clarify the levels of review required based on the control exercised by a Responsible Entity over a Transient Cyber Asset. The language should be revised to describe the requirements when an entity has "full" or "substantial" control through its ownership and management of the asset, as compared when an entity has "minimal" control, as seen when leasing an asset from a vendor. Thank you for your comment. In response, the SDT used the concept of “parties other than the Responsible Entity” to allow the entity to define the controls and processes that are most appropriate to their organization.

AEP commented that the term “security vulnerabilities” is broader than security patch management or malicious code prevention used in CIP-007 and suggested the term be revised. The SDT thanks you for your comment. In response, the SDT revised the term to be “software vulnerabilities.”

Question 4: Transient Devices Definitions

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

General

CSU agrees with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. Since "Media" is itself not a defined term, CSU recommends either defining "Media" or not capitalizing the term. In response, the SDT replaced "Media" at the beginning of the definition with "Storage media" in order to clarify the term and show it is not a defined NERC Glossary term.

Removable Media

IESO commented that the definition of Removable Media refers to media that are "capable of transmitting executable code to:" and suggested that the word "transmitting" is incorrect and should read "transferring". Media such as floppy disks do not transmit but one can transfer executable code from the disk to another media. In response, the SDT agrees and has modified the language.

Transient Cyber Assets

NPCC commented that based on the new definitions, it is unclear on whether a Cyber Asset can be classified as multiple asset types and would therefore be subject to multiple levels of requirements, i.e. a BES Cyber Asset or a Protected Cyber Asset can also be a Transient Cyber Asset. If a BES Cyber Asset or a PCA also meets the definition of Transient Cyber Asset, there is nothing in the language that says one classification supersedes or precludes another. Solely based on the definitions, it would appear that an entity would have to classify an asset by all the definitions that apply. NPCC recommended:

- Add the following sentence to definition of Transient Cyber Asset: "A Cyber Asset that meets the definition of BES Cyber Asset shall not be considered a Transient Cyber Asset."
- Add a minimum requirement to the PCA definition. "If a PCA is connected for less than 30 days then it is a TCA and more than 30 days it is a PCA."

In response, the intent of the SDT was for an asset to be classified under one definition and therefore subject to only one set of requirements. The SDT revised the definitions to clarify Removable Media is not a Cyber Asset and Transient Cyber Assets are not Protected Cyber Assets.

EEI, Pepco, and Iberdrola commented that for the Transient Cyber Asset definition, the "and" in the parenthesis after "A Cyber Asset," is confusing. It could be interpreted as meaning a Cyber Asset must use all of these types of communication connections. Also, the parenthetical for the examples is misplaced; it refers to examples of communication types not Cyber Assets. Also, the definition makes it unclear whether a Transient Cyber Asset could also be a BES Cyber Asset or a Protected Cyber Asset and, therefore, unclear as to which requirements apply. For example, if a Responsible Entity defines a BES Cyber System to include a device, which could also be considered a Transient Cyber Asset, does the BES Cyber System requirements apply, the Transient Cyber Asset requirements, or both? Finally, "directly connected" may be interpreted as meaning only non-routable communications; however, we believe the intent is to include both routable and non-routable communications. Therefore, EEI recommended changing the definition for Transient Cyber Asset to: "A Cyber Asset that is not included in a BES Cyber System and is not a Protected Cyber Asset (PCA) and is capable of transmitting executable code that is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth) for 30 consecutive calendar days or less to (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." Also, if the intent is for the Transient Cyber Asset definition to apply to both routable and non-routable communications, EEI requested clarification in the Guidelines and Technical Basis for CIP-010-2. In response, the SDT has made several modifications to the definition of Transient Cyber Asset, as suggested, to address these issues. The SDT has not indicated the directly connection is routable or non-routable, but rather the examples in the definition list several types of direct connections, both routable and non-routable.

FirstEnergy, MMWEC, and Encari did not agree that the CIP Standards adequately specify the scope of devices that can be classified as Transient Cyber Assets. The definitions and standard language make it unclear whether a Transient Cyber Asset needs to be treated as a BES Cyber Asset or a Protected Cyber Asset and therefore which requirements apply. For example, if a Responsible Entity makes a temporary routable connection between a Transient Cyber Asset and an ESP, would this Transient Cyber Asset also have to meet the requirements for the BES Cyber System or for a connected PCA? In other words, could the BES Cyber System requirements also be construed to apply to a Transient Cyber Asset that is temporarily connected? In response, the SDT has modified the definition of Transient Cyber Asset to indicate it is neither a BES Cyber Asset nor a Protected Cyber Asset.

Tri-State G&T noted that the recent revisions made to the Removable Media and Transient Cyber Asset definitions introduced some unintended ambiguity. Revisions should be made to make it clear what the assets/devices must be connected to, in order to clarify this qualifier of the definition. It is our understanding that the intent of the drafting team was to state "...directly connected... [clause]... to..." where the items after the "to" is what the "Cyber Asset" or "Media" is connected to. One simple solution is to add a comma after the [clause] and before the word "to". Another option is to state the [clause] part after the list of what the "Cyber Asset" or "Media" is connected to. In response, the SDT has made revisions to the definition to address this potential ambiguity. The modifier comes before the indicated preposition.

SMUD, FMPA, and BPA agreed with the changes that were made by the SDT to both Transient Cyber Assets and Removable Media definitions. However, SMUD is concerned with starting the definition of Removable Media with the capitalized "Media" considering that "Media" is itself not a defined term. In response, the SDT has modified the definition to address these comments.

AEP commented that regarding Transient Cyber Assets, the 30 day timeframe prevents a Responsible Entity from being able to consider a device that is temporarily connected to the BES Cyber System as part of the BES Cyber System, and it is arbitrarily beyond what was ordered by FERC. AEP suggests removing the 30 day timeframe to reduce the amount of tracking Responsible Entities must do with respect to these devices. In response, the entity may designate the device as a PCA and follow the applicable requirements for a PCA. The TCA definition was revised to clarify that a PCA would not be a TCA.

Question 5: Implementation Plan

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

Complexity

AEP suggested streamlining the implementation date to the latest date proposed in the Version X and Version 6 implementation plans. KCP&L and SPP & specific members commented that there should be one date for high and medium impact BES Cyber Assets and their accompanying devices and one for low impact BES Cyber Systems. KCP&L and SPP and specific members further recommended that the latest date for each grouping be chosen as a new effective date for all requirements. In response, the SDT thanks you for your comment. With support of stakeholder input, the SDT decided that the added time given under the staggered implementation plan was important to the more labor intensive requirements. While the SDT was unable to move to a later deadline for all requirement areas, in CIP-003, the SDT revised deadline for both sections 2 and 3 to September 1, 2018.

Xcel stated it did not support the revised language providing for tiered deadlines for low impact assets. In response, the SDT thanks you for your comments but states that the majority of industry supports this approach.

Tri-State G&T comments that the timelines are fine, but written in a very convoluted way. It would be helpful to state them more succinctly. In response, NERC will consider creating an informational worksheet to more simply and succinctly see the implementation compliance deadlines.

Protecting LEAP's Before They're Identified

Consumers, EEI, Oncor, Southern Company, MidAmerican, NIPSCO, Duke, First Energy, NV Energy, NRECA, and Hydro Quebec commented on the different effective dates for Elements 2 and 3. Thank you for your comments. In response, the SDT revised the implementation plan to include a September 1, 2018 compliance deadline for CIP-003, Sections 2 and 3.

Excessive Time Period

Texas RE suggests that the proposed implementation time periods are excessive by 12 months, particularly for administrative documentation. Thank you for your comment. The majority of stakeholders supported the proposed deadlines.

Needing More Time

Idaho Power commented that the time frames still do not provide enough time for entities to adjust to an increase in scope of this magnitude. The SDT thanks you for your comment. While the SDT was unable to move to a later deadline for all requirement areas, in CIP-003, the SDT revised the compliance deadline for Section 2 Physical security controls to September 1, 2018.

BPA disagrees with the tiered implementation timeline as currently proposed. BPA believes more time is required to create practices and procedures to implement the policy effectively. BPA suggests that policy (CIP-003-6, R1, part 1.2) be implemented prior to other requirements (CIP-003-6, R2 and CIP-003-6, R2 Attachment 1, items 1-

4). The SDT thanks you for your comment. The SDT was unable to move to a later deadline for all requirement areas, in CIP-003, the SDT revised the compliance deadline for Section 2 Physical security to September 1, 2018.

ACES Standards Collaborators commented that the SDT should consider modifying the implementation dates for electronic access and physical security to be 18 months from the effective date of April 1, 2017. Physical security implementations, depending on the site(s), could have long durations and require additional budget cycles to implement across a diverse geographic and multiple asset types. The SDT thanks you for your comment. The SDT revised the compliance deadline for Section 2 Physical security controls to match the Section 3 Electronic access controls compliance deadline of September 1, 2018, which is 18 months after the April 1, 2017 effective date as ACES proposed.

Support for the Implementation Plan

ATC appreciated the SDT's consideration of previous comments, and supports the adjustments in the implementation plan that accommodate for the time necessary to be successful in implementing Sections 2 and 3 for Low Impact pursuant to CIP-003-6. The SDT thanks you for your support.

SMUD, CSU, Exelon, FMPA, MISO, Occidental Chemical Corporation, NYPA, TVA, NPCC, Dominion, MRO NERC Standards Review Forum, Iberdrola USA, PJM Interconnection LLC, PacifiCorp, Arizona Public Service Company, Encari, Luminant Generation Company, LLC, Rutherford EMC, ATCO Electric, CenterPoint Energy Houston Electric LLC, Manitoba Hydro, Independent Electricity System Operator, Entergy Services, Southern California Edison Company, Pepco Holdings, NRG Energy, and Massachusetts Municipal Wholesale Electric Company supported the implementation plan. The SDT thanks you for your support.

Question 6: Removal of the IAC Language

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

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

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

The SDT’s responses to comments on those revisions are available here.

Question 7: Other Areas Within SAR

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

Some comments from this question were addressed in the previous consideration of comments from the standard drafting team. Those responses only pertained to the revisions in the Version X posting and are available here.

In addition, the SDT addressed the majority of comments in response to this question in other questions in this consideration of comments.

Responses to those not previously addressed are as follows:

Striving for Steady-State

ACES commented on the importance of approving CIP 5 revisions without further changes (so that they are steady-state) to allow for the impacted entities to plan, budget and implement CIP Version 5. The SDT thanks you for your comments and shares the desire to reach a "steady-state" with the CIP standards. The SDT worked to address all four directive issue areas concurrently to respond to the FERC directives in a timely manner. The proposed revisions received passing ballots for all the issue areas in the second posting. However, the SDT felt it important to continue work in response to the constructive comments received and consider further improvements to the revisions. The SDT will post for an additional comment and ballot period and hopes to see additional support for the proposals based on the additional refinements.

NPPD commented that these standards must get to a steady state and changes to the standards should be limited to an absolute minimum. Thank you for your comment. The SDT shares the desire to reach a "steady-state" with the CIP standards. The SDT has worked diligently to address the FERC directives in a timely manner through the NERC iterative, stakeholder process.

Take the Time Needed

AEP urged the SDT to take the time necessary to ensure that the requirements achieve the necessary reliability benefit and that there is broad-based industry support. The SDT thanks you for your comment. The SDT shares AEPs desire to have broad-based industry support for the revisions in response to FERC Order 791. While the revisions for all four issue areas passed stakeholder ballot in the second posting, the SDT felt it important to continue work in response to the constructive comments received. The SDT hopes to see additional support for the proposals based on the additional refinements.

Define Cyber Security Plan

BC Hydro recommended that the term “cyber security plan” be defined or further explained in guidance. Thank you for your comment. The documents developed and implemented in response to CIP-003 R2 are to include the CIP-003 Attachment 1 sections and identify what will essentially become the entity's cyber security plan. The SDT deliberately avoided creating a "Cyber Security Plan" definition, in order to provide entities the flexibility to include these Sections within a more inclusive set of documents, if so desired. For instance, an entity may have an overarching security plan that includes overall physical security, as well as physical security and cyber security for high impact BES Cyber Systems, medium impact BES Cyber Systems, and low impact BES Cyber Systems.

Overly Prescriptive

AEP commented that it was concerned about prescriptive approaches within the standards and the potential to unreasonably restrict the Responsible Entities from defining their own programs. The SDT appreciates the comment. CIP-003-6 Requirement R2 and Attachment 1 have been further revised to strike a balance in FERC's Order 791 determination for greater specificity, providing industry clear options for achieving compliance, as well as flexibility in achieving the Requirement R2 objectives, stated within each Attachment 1 Section. CIP-010-2 R4 and its corresponding Attachment 1 Sections have been further revised as well, seeking the same balance. Many within this SDT and industry believe the current level of specificity, while some may see it as prescriptive, also serves to provide greater predictability and limitations on how various regional auditors might interpret language within those stated objectives.

RSAWs

FMPA commented that their negative votes were due to the current condition of the RSAWs and the status of RAI implementation, in particular on how RAI will address zero tolerance. This SDT submitted comments on the draft RSAWs posted for comment. The SDT continues to be available to work with NERC on RSAWs. In addition, the SDT has forwarded and continues to share the comments on RAI/compliance and enforcement with the relevant NERC divisions. Thank you for your comment.

SMUD also commented that the RSAWs have not sufficiently incorporated the specific language of the standards or the measures. It is unclear from reading the currently posted RSAWs how auditors will use the measures to inform the Compliance Assessment Approach.   The SDT submitted comments on the proposed RSAWs during the comment period and continues to be available to work with NERC on RSAWs.

Quality Review

NPC and NYPA recommended quality assurance review before future postings, to avoid reviewers’ confusion or need to decipher how to connect related information. Thank you for your comment. The SDT and other resources are in place to conduct a quality review prior to the next posting.

Scope of Nonprogrammable Components

BPA disagreed with the CIP-007-6 R1.2 expansion of scope to non-programmable communication components and proposes re-alignment to R1.1. Thank you for your comment. The SDT confirms that this expands the scope of 1.2, but it does so appropriately and in response to the Order 791 directive to address the security of nonprogrammable components associated with BES Cyber Systems. CIP-007-6 Requirement Part 1.2 concerns the physical security of computing equipment ports. Nonprogrammable components did not previously meet the definition and applicability for Cyber Assets but they may have the same vulnerability that this Requirement Part addresses. The expanded scope closes this gap in protection.

Device Types

MRO suggested that the SDT insert “type” in reference to devices into CIP-010-2 Guidelines and Technical Basis Section 1.1. The SDT thanks you for your comment. While "device types" is one method of grouping TCA devices that entities will likely apply per Attachment 1 Section 1.1, the SDT is reluctant to include this citation within guidance and thereby risk limiting the scope of entity's options for grouping.