NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02
CIP Version 5 Revisions

Consideration of Comments
Additional Comment Period

January 23, 2015

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 November 25, 2014 through January 9, 2015. Stakeholders were asked to provide feedback on the Reliability Standards and associated documents through a special electronic comment form. There were 66 sets of comments, including comments from approximately 143 different people from approximately 99 companies representing all 10 Industry Segments.

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 one face-to-face meeting to appropriately consider all comments received.

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 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-003-7

1. *For the requirements applicable to assets containing low impact BES Cyber Systems, the Standard Drafting Team (SDT) maintained the structure of CIP-003, Requirements R1 and R2 from the prior comment period and ballot, but revised the language in response to stakeholder comments. Do you agree with the revisions in CIP-003-7? If not, please explain your objections and offer suggested revisions.*

Section 1

Dominion NERC Compliance Policy commented that Section 1 of CIP-003, Attachment 1 does not address the target audience similar to CIP-004, Requirement R1, Part 1.1. The SDT thanks you for your comment. Since CIP-003 requirements focus on the asset containing low BES Cyber Systems and not the people, the Low Impact Cyber Security Plan(s) can identify the target audience.

Kansas City Power and Light commented that the requirement is less clear with the inclusion of the phrase, "which may include associated physical security practices" and that the SDT should not provide statements regarding what an entity may want to do. The SDT thanks you for your comment. The addition of the parenthetical was in response to comments from a previous posting. The addition of the parenthetical reference is to align the requirement with CIP-004-5, Requirement R1 and allow the awareness of physical security practices as part of an entities' cyber security awareness.

Section 2

Northeast Power Coordinating Council (NPCC), Santee Cooper, Dominion NERC Compliance Policy, Utility Services, Northeast Utilities, Entergy, and Hydro-Quebec transEnergie commented that "need" may lead to multiple interpretations. The SDT thanks you for your comment. Without "based on need" there is no basis for the selection of physical security controls. The SDT 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. The Guidelines and Technical Basis explains that authorization and approval processes are not required.

Santee Cooper, South Carolina Electric and Gas, American Electric Power (AEP), and Oncor Electric Delivery Company, LLC (Oncor) suggested removing "restrict" and replacing "control" in the context of physical access because the word "control" implies that an entity must know who can and cannot enter the restricted space. The SDT thanks you for the comment. The word "control" was selected in response to comments in the last ballot. It is not the intent to require an authorization process or a list of individuals.

Edison Electric Institute (EEI), the United Illuminating Company, MidAmerican Energy Company (MidAmerican), Wisconsin Electric Power Company, Ameren, and Westar Energy commented that "control physical access" can imply that only physical access controls or perimeter controls may be used to meet the requirement. However, the Guidelines and Technical Basis states that an entity may use a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. The commenters suggested to clarify the language within the standard because it is enforceable. The SDT thanks you for your comments. The SDT moved the bulleted list to Guidelines and Technical Basis because it was itself not an exhaustive list of physical security controls. The use of monitoring is a type of physical security control. The measures also include documentation using monitoring controls.

Utility Services commented that Section 2 lists (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) and questioned whether the Guidelines and Technical Basis should accordingly be revised from "for access to site or systems" to

"for access to locations, systems, or LEAPs." Thank you for the comment. The SDT intended systems to included LEAPs. To clarify, the SDT modified the sentence in the Guidelines and Technical Basis to say "assets and systems, including LEAPS."

Kansas City Power and Light commented that the phrase "control physical access" is confusing because the requirement implies an entity must maintain absolute control of physical access but then implies entities may do what they desire due to the phrase "based on need." The SDT thanks you for your comment. It is not the intent of the word "control" to have "absolute control" of physical access and to seek perfection. The use of "based on need" is to provide the flexibility to an entity to document their specific asset characteristics related to physical security controls. Many considered the previously used word "restrict" to require more formal authorization processes for physical access.

Section 3

Tennessee Valley Authority (TVA) suggested the SDT replace "from or to" with "to or from" in the Guidelines and Technical Basis for Section 3, paragraph 3. Furthermore, TVA commented that the SDT should remove "all" from paragraph 4 in the Guidelines and Technical Basis for Section 3. The SDT thanks you for your comments. The SDT made the recommended changes to the Guidelines and Technical basis.

NPCC, First Energy Corp., Santee Cooper, NIPSCO, South Carolina Electric and Gas, Northeast Utilities, CenterPoint Energy Houston Electric LLC (CenterPoint), Tampa Electric Company (TECO), Hydro-Quebec transEnergie, and Luminant Generating Company, LLC (Luminant) commented that Reference Model 4 is inconsistent with the Low Impact External Routable Connectivity (LERC). The commenters stated that where an IP/Serial converter is used, the end-to-end session is not entirely bidirectional routable protocol according to the definition. The SDT thanks you for your comment. The SDT revised the Guidelines and Technical Basis to further clarify Reference Model 4 to demonstrate its consistency with the LERC definition.

Dominion NERC Compliance Policy questioned whether a LEAP not located at the asset containing the low impact BES Cyber Systems is required to be compliant with Attachment 1 Section 2, (2). The commenter further noted that 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 commenter stated that 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. The commenter recommended changing applicability statement to: "Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems and LEAPs." The SDT thanks you for your comment. The SDT retained the title as the LEAP is required to be protected as a result of applying the requirements to the asset containing the low impact BES Cyber Systems regardless of the location of the LEAP. The title in the Attachment 1 is not inclusive of Applicability as in the requirements for medium and high impact BES Cyber Systems.

Xcel Energy commented that by stating that LEAP is required for these network-connected low impact assets, the actual scope of CIP controls must increase to ensure the LEAP 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 LEAP controls are effective. The commenter expressed concern regarding the ambiguity and the actual increase in scope, even though not stated directly in requirement language. The SDT thanks you for your comment. The SDT did not intend to imply compliance to a specific list of activities. The requirements for compliance are specifically related to physical security and inbound and outbound access permissions.

Entergy recommended 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 the needs dictated by the Responsible Entity's configuration. The SDT thanks you for your comment. The SDT recognizes the implementation of physical security controls and electronic access controls are different. With physical security controls, the asset containing the low impact BES Cyber System could have varying characteristics. For the electronic access controls, the obligations are specific to the routable protocol and only focus on applying physical security and inbound and outbound access permissions.

Waterfall Security Solutions commented that hardware-enforced unidirectional gateways are not intended to be bidirectional communication, precluding these types of communication from being considered LERC. The commenter suggested the SDT develop a reference model for a common unidirectional deployment model. The SDT thanks you for your comment. The SDT has provided a set of Reference Models to depict configurations to clarify the obligations. The reference models are not an exhaustive set of configurations, but ones that the SDT felt were instructive and could be crafted in the time available to the team.

Pepco Holdings Inc. commented that LEAP applies to both LERC and Dial-up as written in Section 3.1. Pepco suggested capturing the difference between authentication only as it applies to Dial-Up access points. The SDT thanks you for your comment. The LEAP only applies to LERC and not Dial-up. Authentication for Dial-up communication is only required if Dial-up exists.

Bonneville Power Administration (BPA) commented that the SDT's reference models show the possibility of business network connections having some kind of connectivity to low impact BES Cyber Systems. BPA noted that Cyber Assets and systems can also be located on a completely isolated network, such that the BES asset boundary has no penetrations to or from other network systems. BPA's interpretation suggested this architecture is evidence enough to meet the Electronic Access Controls requirement in CIP-003-7 attachment 2 Section 3. BPA requested validation of this approach and a new reference model drawing showing this approach. The SDT thanks you for your comment. If there is no communication external to the asset containing the low impact BES Cyber System, there is no LERC and providing such documentation is sufficient for compliance to Section 3, Electronic Access Controls. If there is communication between one asset (e.g. station, or low impact control center) to another asset (e.g. station, or low impact control center), then there is LERC and a LEAP is required; unless the communication meets the exclusion included in the definition.

Southern Companies (Southern) commented that the Guidelines and Technical Basis state that 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. Southern recommended the team consider revising the language to indicate that the BES assets are sharing the Cyber Asset with multiple LEAPs. The SDT thanks you for your comment. The SDT evaluated the noted section of the Guidelines and Technical Basis. The SDT made revisions, but opted to revise the sentence differently than proposed.

Section 4

Dominion NERC Compliance Policy requested clarification on what triggers an update to the Cyber Security Incident response plan, if needed. The commenter noted that there is an obligation to maintain the plan(s) based on triggering events in CIP-008. The SDT thanks you for your comments. The test or the actual incident is intended to trigger consideration of making updates to the response plan. The SDT considered removal of 4.6 in response to comments in previous postings, but decided that updating a plan in response to information learned in a test or incident was a reasonable security obligation.

Southern noted that the measures in Attachment 2 for Section 4 need to say "groups or individuals" rather than "groups of individuals." The SDT thanks you for catching the typo and making your comment. The SDT has made the requested change.

Other

TVA, Santee Cooper, Xcel Energy, New York Power Authority, American Electric Power (AEP), and Seminole Electric Cooperative (Seminole) objected to the placement of the requirements applicable to low impact in CIP-003 only. The SDT thanks you for your comment. The SDT received support in the ballot for the use of the Attachment structure.

Dominion NERC Compliance Policy recommended that the SDT remove the sentence, "Responsible Entities will use their list of assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber Systems" from the Rationale for Requirement R2. The SDT thanks you for your comment. The SDT changed "list of" to "identified."

EEI, the United Illuminating Company, Wisconsin Electric Power Company, Ameren, Westar Energy, and MidAmerican Energy Company reported that a Regional Entity will not consult the Guidelines and Technical Basis for enforcement. The commenters asked that this be addressed. The SDT thanks you for your comments. The SDT relayed this comment to NERC. NERC notes that it strives for consistency across the Electric Reliability Organization (ERO) and will encourage all Regional Entities to consult the Guidelines and Technical Basis for better understanding of the standards. For the SDT, development of the Reliability Standard and Standards' revisions involves balancing the diverse set of stakeholder perspectives and interests expressed through comments and outreach. Throughout the development process, the SDT received competing preferences for the amount of language to include in the requirements. The SDT strives to propose language that provides enough specificity but does not overly restrict flexibility. The SDT utilizes the Guidelines and Technical Basis to expand upon the intent behind the requirement language and offer clarifying details. The Guidelines are to be consistent with the requirement language but do not typically represent an exhaustive description of scenarios that can be compliant with the requirements. The information provided in the requirements and the Guidelines is expected to work together and be a resource for implementation and compliance.

Xcel Energy and Idaho Power Company commented that 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. The SDT thanks you for your comment. The SDT intent is not to imply requirement of a list, but also not to exclude it as an option to demonstrate compliance. The SDT has modified the sentence.

Consumers Energy Company commented that the requirements, measures, and documentation obligation is above that of the prior version 5 level and provide less flexibility. The SDT appreciates the comment. In revising CIP-003, the SDT aimed to strike a balance in meeting FERC's Order No. 791 determination for greater specificity, and providing industry clear options for achieving compliance, as well as flexibility in achieving the Requirement R2 objectives as stated within each Attachment 1 Section.

Utility Services commented that the VSLs associated with Section 2 should be strictly tied to the need determination being made and not allow for inadequacies or subjective third party considerations of the need determination. The SDT appreciates the comment. The SDT notes that a potential violation of a requirement is determined based on the language of the requirement. Once it has been determined that the potential violation is a violation of the requirement, enforcement looks to the VSLs to determine the degree of severity of the violation, not whether a violation has occurred.

Kansas City Power and Light commented that there is more information in the Guidelines and Technical Basis than in the standards, which leaves the requirements ambiguous. The SDT thanks you for your comment. The Guidelines and Technical Basis does not overrule the Requirements. The SDT has written Guidelines and Technical Basis to clarify the technical nature of the Requirements.

MidAmerican Energy Company commented that the SDT should continue coordination with the Dispersed Generation Resources (DGR) SDT in order to develop an exemption for DGR. The SDT thanks you for your comments. The SDT worked with the DGR SDT to explore potential language to address DGR concerns. While some foundational discussions took place, in order to continue, further work is needed to clarify the justification for the revisions and to clarify the security and compliance considerations. At this point, it may be appropriate for DGR stakeholders to further research the implications of CIP-003 and, if revisions are deemed necessary, consider a new SAR specifically focused on the concerns.

Tri-State Generation and Transmission Association commented that the Background section mentions training as part of the cyber security awareness program requirement. The SDT thanks you for your comment. The sentence has been modified. There is no training requirement for low impact.

Luminant recommended several minor revisions to the language of the Guidelines and Technical Basis to further clarify the language. The SDT revised the language accordingly. Luminant also commented that Reference Model 5 does not include LERC. The SDT determined that the reference model accurately reflects sufficient access controls. Luminant further commented that the Guidelines and Technical Basis and Reference Models suggest that a non-BES Cyber Asset within a BES asset containing low impact BES Cyber Systems do play a role in protecting those BES Cyber Systems and recommended removal of language. The SDT notes that the bullet point and explanatory paragraph describing the reference model accurately reflect a scenario of insufficient access controls. A non-BES Cyber Asset could perform the function of electronic access control. The addition of "without disabling IP forwarding" in the bullet further clarifies the SDT's intent. The SDT removed 3G/4G before wireless card earlier in the guidance. Luminant also commented that the explanatory paragraph of Reference Model 3 should state that low impact BES Cyber Systems at the asset are externally accessible using routable protocol. The SDT thanks you for the comment but notes that the focus is on the accessibility not the protocol in Reference Model 3. Luminant suggested that the SDT label the Cyber Asset within the BES asset in Reference Model 6 should be labeled as Non-BES Cyber Asset to be consistent with Reference Model 5. The SDT thanks you for the comment but notes that the focus of the reference model is on stopping the direct access to tie back to the definition of LERC.

NPCC commented that the Reference Models should indicate the actual data paths. The SDT notes that the diagram in conjunction with the explanatory paragraph describe the data flows. The data flows are depicted by green arrows in the reference models.

ACES suggested that the SDT remove 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." The SDT determined that the language is consistent with LERC because it is referencing bi-directional routable protocol connectivity. ACES also suggested that the SDT remove the statement, "A Responsible Entity using this technology is not expected to implement a LEAP even though there technically is LERC" because it is inconsistent with LERC. The SDT removed part of the sentence to clarify the intent.

Question 2: Low Impact Definitions

2. *The SDT revised the proposed definitions for Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) based on stakeholder comment. Do you agree with these proposed revisions? If not, please explain your objections and offer suggested revisions.*

LERC and LEAP

EEI, FirstEnergy, Lincoln Electric System, United Illuminating Company, Oncor, and TECO requested the SDT clarify that only devices with routable connections can have LERC. The commenters stated that 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." The commenters further noted that Reference Model 4 seems to contradict the plain language of the LERC definition, which could bring many non-routable connected devices into the scope of this requirement. The SDT thanks you for your comment. The SDT added some language to the Guidelines and Technical Basis to further clarify Reference Model 4.

EEI, United Illuminating Company, Oncor, and TECO commented that the CIP-003-7 Guidelines and Technical Basis interpretation of external routable connectivity for Low Impact BES Cyber Systems will 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. Specifically, the commenters were concerned the scenario in Reference Model 4 would be applicable to medium and high impact BES Cyber Systems. The SDT thanks you for your comments. The SDT used a different set of terms given its limited focus on low impact. The CIP Version 5 Transition advisory group as part of the transition program is developing a lessons learned on ERC. The SDT notes that LERC/LEAP are terms applied to assets containing low impact BES Cyber Systems. ERC is applied to individual BES Cyber Systems. The concepts and definitions are applied at two different levels.

EEI, United Illuminating Company, Oncor, and TECO commented that at least one Regional Entity has communicated that it will not consult the Guidelines and Technical Basis for enforcement. The SDT relayed this comment to NERC. NERC notes that it strives for consistency across the ERO and will encourage all Regional Entities to consult the Guidelines and Technical Basis for better understanding of the standards.

Lincoln Electric System commented that the proposed definitions do not take into account the exclusion for communication networks in Section 4. The 4.2.3.2 exemption in CIP-003-6 does not apply here because low impact assets do not associate with the ESP concept. Additionally, such an exemption is not necessary because CIP-003-6 R1 and R2 have no requirements applicable to communication networks external to the entity identified LEAP. The "BES Asset Boundary" labels in the diagram delineate the physical boundaries (i.e. the fence line) of the BES Asset. This is only used in the Guidelines and Technical Basis section as a convenient term to illustrate the site-level requirement concept.

Duke Energy commented that the SDT should add the phrase "up until the devices at which the routable protocol connection terminates" to the LERC definition. The SDT thanks you for your comment. The SDT determined that the phrase was not needed in the definition and encourages the commenter to look at Reference Model 4 and the revised guidance in the Guidelines and Technical Basis of CIP-003.

Santee Cooper, Corn Belt Power Cooperative, SCE&G, and BPA commented that the definitions were vague and suggested that the SDT revise the definitions of ERC and EAP to include lows rather than creating the new definitions of LERC and LEAP. The SDT thanks you for your comments. The SDT purposefully separated the

connectivity concepts between high/medium impact scenarios and low impact scenarios. Since all of the high/medium impact concepts, definitions, and requirements are based on Electronic Security Perimeters, which do not involve lows, the SDT determined not to intermingle the concepts and create separate definitions.

Consumers Energy Company commented that not having to create a list, inventory, or discrete identification of low impact BES Cyber Systems or BES Cyber Assets behind the LEAP causes compliance uncertainty and audit vulnerability. The SDT's intent is that entities have a list of 'assets containing low impact BES Cyber Systems' from CIP-002-5 and demonstrates at the asset level whether or not LERC exists to low impact BES Cyber Systems within the asset. If LERC exists for that asset, then an entity can provide evidence regarding a LEAP that protects that communication for that asset (and by reference, all low impact BES Cyber Systems within it) without inventories of low impact BES Cyber Systems.

Flathead Electric Cooperative, Inc. commented that it preferred the inclusion of the phrase, "The Low Impact BES Cyber System Electronic Access Point is not an Electronic Access Control or Monitoring System." The SDT thanks you for your comment. In previous drafts, it was pointed out by industry commenters that this statement was unclear as a LEAP is an interface on a Cyber Asset and an EACMS is an entire Cyber Asset. The SDT took the opportunity to make this clear in draft 3, as well as provide further examples in the reference diagrams (see reference model 7).

Dominion suggested that the SDT revise LERC to state that the connection to a low impact BES Cyber System from a Cyber Asset should say a "Cyber Asset other than a LEAP." The SDT understands this proposal to address the case where a LEAP is placed external to the asset containing low impact BES Cyber System (Reference Model 3). In this case, the proposed revision to the definition is unnecessary. An entity would identify any LERC and then designate a LEAP for all LERC, and the LEAP may exist outside of the BES asset boundary. The external LEAP can still perform the obligation of 3.1. The communication path from the LEAP to the low impact BES Cyber System has no obligations for additional access control at the site. In addition, using the LEAP term in the LERC definition creates a circular reference.

Seminole Electric Cooperative commented that the use of the word "location" is ambiguous and may be interpreted in multiple ways as used in the LEAP definition. The SDT thanks you for your comment. The SDT has used the term 'location' so as not to prescribe where a LEAP must reside. With the number of assets in the BES that will contain low impact BES Cyber Systems, the SDT did not want to require a LEAP per asset.

Occidental Chemical Corporation, Arizona Public Service Commission (APS), and AEP commented that the LERC definition should have a broader exclusion than only Transmission. Furthermore, APS suggested that any additional details, such as the exclusion, should be in an explanatory document and not the definition. The SDT's intent for the revision to the third draft was to further limit the exclusion to IED to IED communications between transmission stations or substations so that the exclusion could not be used to exclude all communications from Control Centers that only contain low impact BES Cyber Systems to all Transmission stations or substations that only contain low impact BES Cyber Systems. The SDT did not intend to exclude generation stations that may have the same configuration. This was an oversight; however, making the revision would constitute a substantive change. Given the strong ballot support for the third proposal, the SDT opted to move the proposal to final ballot. If a future revision is proposed, the SDT intent behind this section of the standard language should support such a revision. As for having exclusions in the definition, the SDT determined that what a term does not include is equally of value as what it does include. If exclusions were not in the definitions, then everywhere the term was used in the standards the exclusion would need to be addressed, unnecessarily complicating the requirements.

KCP&L commented that the LEAP definition does not specify what is meant by "controlling" LERC and noted that it is subject to multiple interpretations. The commenter suggested revising the definition. The SDT chose the term 'controls' over its previous term 'allows' because previous industry comments pointed out that 'allows' is

extremely general. The SDT intent behind the choice of 'control' is documented in CIP-003-7 Attachment 1 Section 3.

Question 3: Transient Devices

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

Revisions

TVA suggested that the SDT revise CIP-010, Attachment 1 to retain theft recovery tools as a valid method of mitigating the risk of unauthorized use of Transient Cyber Assets. The SDT thanks you for your comments but notes that entities may use theft recovery tools as an "other method" according to the requirements. The Guidelines and Technical Basis and measures sections provide more detail on what methods an entity may use to meet the requirement.

Santee Cooper commented that Section 1.1 of Attachment 1 seems to require an entity to review a Transient Cyber Asset before it is attached to a different BES Cyber System and recommended revisions. The SDT thanks you for your comment. The SDT would refer the entity to the Guideline and Technical Basis regarding the management of Transient Cyber Assets in developing their plan to meet the objectives.

Duke Energy recommended adding a time requirement to Attachment 2, Section 1, similar to the one found in Attachment 1, Section 1. The SDT thanks you for your comment and clarifies that it used the concept of a "program" 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 elements from Attachment 1.

Seminole Electric Cooperative commented that the use of the word "location" is ambiguous and may be interpreted in multiple ways. Seminole further commented that there is no direct relationship between business function and cyber security in this environment. Seminole also commented that the authorization requirements are excessive. The SDT has used the term 'location' so as not to prescribe where a Transient Cyber Asset must reside but rather allows the entity to develop a plan with enough flexibility to use locations in which to manage authorizations. The SDT modified the Guidelines and Technical Basis to add clarity to the term "business function" by including the examples from the definition of TCA. The examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. The SDT notes that it balanced the burden on entities with what it determined was necessary for authorization. The SDT notes that authorization includes intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

NIPSCO recommended the SDT edit Section 3.2.1 to read, "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…." The SDT thanks you for your comments but notes that the posted language received a high percentage of industry approval. Therefore, the SDT determined not to make changes to the language.

SCE&G recommended the SDT revise Section 1.1 to include a provision that allows an entity to use a transient device within an ESP if it has been tested upon initial use in that ESP. The SDT thanks you for your comment. The SDT used the concept of a "program" to allow the entity to define the controls and processes that are most appropriate to their organization. This includes determining how the entity will meet the compliance objectives specified in Attachment 1.

Pepco Holdings Inc. commented that the SDT's use of the word "Caution" is inconsistent with the manner in which requirements are typically drafted. The SDT thanks you for your comment but notes that the word was used to add emphasis to the section. The SDT deemed it appropriate for the purposes of this requirement.

Definition and Guidelines and Technical Basis

FirstEnergy commented that the language for the Transient Cyber Asset definition does not appropriately establish the scope of devices that should be classified as Transient Cyber Assets. FirstEnergy also noted it agrees with the structure of the standard language but referred to Question 4 for more comments. The SDT responded to these comments in Question 4 of this Consideration of Comments.

Southern Companies, United Illuminating Company, Oncor, Centerpoint, TECO, MidAmerican, and EEI commented that the Guidelines and Technical Basis section needs to be revised according to any changes made to the Transient Cyber Asset definition. Southern and EEI also commented that it is comfortable with the language of the requirements but referred to Question 4 for more comments. The SDT responded to these comments in Question 4 of this Consideration of Comments.

Format

Santee Cooper commented that it is concerned with the format for these requirements and recommended the SDT use the tabular format similar to other CIP requirements. The SDT appreciates the comments regarding the placement of the Transient Cyber Asset requirements and determined to retain the current CIP-010 plan structure due to a majority of stakeholder support.

Interpretation Questions

Lincoln Electric System commented that although it agrees with the need for flexibility in the requirements, it is concerned that the "other methods" language does not provide enough detail as to what will be expected by auditors. The SDT provided this option to allow flexibility in developing the plan to meet the objectives. When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code. Lincoln Electric System further commented that the Guidelines and Technical Basis should indicate that Transient Cyber Assets are capable of transmitting executable code *to the BES Cyber Systems*. The SDT appreciates the comment and has determined to retain the current language as supported by a majority of stakeholders.

Oncor requested clarification on whether the "per Cyber Asset capability" for Section 1.2.2 applies to medium impact BES Cyber Assets without ERC. In the alternative that it does apply, Oncor recommended the SDT revise the requirement to exclude embedded device platforms or to limit applicability to medium impact BES Cyber Systems with ERC. The SDT thanks you for your comments and notes that the plan structure of R4 grants flexibility for entities to determine the approach to meet the objectives. The SDT declines to revise the requirement at this time due to a majority of stakeholder support for the requirement as written.

ACES Standards Collaborators asked what specific system hardening requirements are needed outside of those listed. The SDT thanks you for your comments. Entities may choose to use one or a combination of methods to meet the objective. If you chose system hardening you will need to meet the objective of mitigating the risk of

vulnerabilities posed by unpatched software. The Guidelines and Technical Basis provides guidance regarding system hardening practices.

Question 4: Transient Devices Definitions

4. *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.*

Asset Categorization

EEI, Centerpoint, Oncor, Southern Companies, FirstEnergy, and TECO commented that the Transient Cyber Asset definition requires that a Transient Cyber Asset cannot be a Protected Cyber Asset or BES Cyber Asset. The commenters further stated that any Cyber Asset connected within an ESP with a routable protocol would be required to be categorized as a Protected Cyber Asset regardless of the duration of the connection. The commenters recommended revision. The United Illuminating Company, Northeast Utilities, NPCC, and New York Independent System Operator suggested that the SDT further clarify that a Transient Cyber Asset is not a Protected Cyber Asset or BES Cyber Asset. The SDT thanks you for your comments. The definitions of BES Cyber Asset (BCA), Protected Cyber Asset (PCA) and Transient Cyber Asset (TCA) were modified during the previous comment period in such a way to ensure entities have latitude to designate and categorize these assets as mutually exclusive and therefore only subject to one set of requirements. Specifically, the BCA and PCA definitions have the 30-day time frame exclusion removed. In exchange, the TCA definition was revised to include Cyber Assets, which: (a) have been connected for 30 days or less and (b) are neither part of a BCS (not a BCA) nor a PCA. The SDT made this revision to clarify the mutual exclusivity of these definitions. So if an entity designates a Cyber Asset as a TCA, then emphatically, it is neither a BCA nor a PCA. Moreover, in response to comments, an entity may have a Cyber Asset they designate as a BCA, but they have a need to replace it or disconnect it prior to 30 days of commissioning. It should not then haphazardly fall under the TCA definition and CIP-010-3 R4 merely because of the connection time frame. The SDT developed the definition and requirements with the premise that Transient Cyber Assets are generally portable and frequently connected and disconnected from systems which is typically not a characteristic of a BCA or PCA.

The SDT made a decision early in the drafting process to use examples rather than specify functions in the definition of TCA. This is because of the added complexity to the definitions and the potential to miss certain functions. Furthermore, with the rate of change in technology, it is not practical to create an all-inclusive list that would remain valid over a long period of time. When considering the proper categorization of assets, the SDT notes the purpose of the asset should be the primary deciding factor as shown in the examples in the definition and reinforced in the Guidelines and Technical Basis of CIP-010-3. The connection duration in the definition, while important as an objective threshold, is not intended to be the focus of categorization.

Luminant and NIPSCO requested the SDT consider revising the Transient Cyber Asset definition to read “is not categorized by the entity as a Protected Cyber Asset.” The SDT thanks you for the comments. 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 the categorization of their assets.

FirstEnergy and Dominion NERC Compliance Policy commented that the Transient Cyber Asset definition should limit the scope of Cyber Assets to those used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. The SDT thanks you for the comments. The SDT moved the examples from the definition in response to earlier comments and to avoid necessity of creating an all-encompassing list of functions. The information was moved to the guidance. The intent is for requirements to apply to anything connected.

Idaho Power Company commented that part (ii) of the definition should say “is not a BES Cyber Asset” instead of “is not a BES Cyber System.” The SDT thanks you for the comment. However, the SDT considers the current definition sufficient to make the distinction noted between BES Cyber System and BES Cyber Asset.

Electric Reliability Council of Texas, Inc. (ERCOT) commented that the purpose of the connectivity of the Cyber Asset is more important in classification than the length of connectivity. The SDT thanks you for the comments. The SDT aligned the requirements for TCA to change and configuration management because the Cyber Assets meeting the definition of TCA align with the activities noted in CIP-010.

ERCOT commented that there are instances where a prescribed task takes longer than 30 days to complete and recommended the SDT address these instances. The SDT thanks you for the comments. The entity should be mindful of the 30 day requirement when defining their plan for using Transient Cyber Assets. Following 30 days, a device may be a PCA or BCA. Under CIP version 5 development, the 706 SDT selected 30 days to accommodate devices connected to perform functions of a temporary nature.

MidAmerican recommended that the SDT add the 30-day exclusion back into the Protected Cyber Asset definition. The SDT thanks you for the comments. The SDT removed the 30-day exclusion to address prior industry comments regarding PCAs and BCAs that may be connected for less than 30 days. The intent was to clarify that a PCA would not also be a TCA.

Guidelines and Technical Basis

EEI, Centerpoint, Southern Companies, and NIPSCO commented that the Guidelines and Technical Basis should be clarified to indicate that if a Cyber Asset meets the Transient Cyber Asset definition, then only the Transient Cyber Asset requirements apply. The SDT thanks you for the comments. 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 the categorization of their assets. The SDT intended for entities to have flexibility in the determination. The SDT determined that the Guidelines and Technical Basis is sufficient to support this clarification.

ERCOT requested the SDT develop guidance to provide clarity to ensure proper delineation between direct connectivity to a Cyber Asset and direct control of a Cyber Asset. The SDT appreciates the comment. The SDT considers the language of direct connectivity to be clear and not requiring modification. Direct connectivity does not imply direct control. It is addressing the means of connecting to a system and not the permissions or capabilities once connected.

Pepco Holdings Inc. recommended that the SDT use “assignee as applies to Transient Cyber Asset and Removable Media” rather than “custodian” to eliminate concerns regarding chain of custody when removing these items from Physical Security Perimeters. The SDT thanks you for the comment. The SDT removed reference to Transient Cyber Asset or Removable Media from CIP-011, R2 guidelines cited in your comment to correct an inaccuracy.

Removable Media

Luminant recommended the SDT consider a revision of the Removable Media definition to allow for direct connection to a Transient Cyber Asset. The SDT thanks you for the comment. However, the SDT considers the current definition sufficient to make the distinction noted. The requirements apply only when connecting the Removable Media to asset types listed.

Waterfall Security Solutions commented that 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.

The SDT thanks you for the comment. However, the SDT considers the current definition sufficient to make the distinction noted. The entity is provided the flexibility to classify their asset appropriately and apply the pertinent controls.

Executable Code

Duke Energy requested an example of a device that is not capable of transmitting executable code. The SDT thanks you for your comment and notes that an example includes a relay test set that only interfaces using current voltage and frequency probes.

Supporting Comments

ACES Standards Collaborators expressed support for the clarification in the definition of Removable Media that storage media is not a Cyber Asset. The SDT thanks you for your supportive comments.

Sacramento Municipal Utility District supports and appreciates the changes made by the SDT, and Florida Municipal Power Agency strongly supports the SDT's position on the Reliability Standard Audit Worksheets. The SDT thanks you for your supportive comments.

Question 5: Implementation Plan

5. *In response to stakeholder comments, the SDT revised the implementation plan compliance date for CIP-003-7, Attachment 1, Section 2 to align with CIP-003-7, Attachment 1, Section 3. Do you agree with this proposed revision? If not, please explain your objections and offer suggested revisions.*

Implementation Plan Comments

Santee Cooper and SCE&G recommended an additional 1 year extension for the low impact requirements. The SDT has proposed compliance dates for the CIP-003-7 Requirements applying to low impact BES Cyber Systems in response to comments and outreach. The Implementation Plan recognizes the necessity of additional time for electronic and physical access controls beyond the CIP-003-5 effective dates.

NIPSCO, Flathead Electric Cooperative, and NPCC noted that they cast a negative vote on the implementation plan because of concerns with the associated standards. The SDT thanks you your comment. It is helpful to understand the reason for negative votes.

ACES Standards Collaborators, NRECA, SMUD, and FMPA expressed support of the implementation plan. The SDT appreciates your supportive comments.

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. The SDT responded to this comment in Question 1 of this Consideration of Comments.

Question 6: Other Areas Within SAR

6. *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 second 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.*

Low Impact

NPCC commented that the SDT should show the data flows in the Reference Models in the Guidelines and Technical Basis. Thanks for your comments. The clean versions show data flows for Reference Models 1-6. These were difficult to see in the redline versions, but they are included.

ACES Standards Collaborators commented that it agrees with the objectives in the requirements but urged the SDT to make it clear that the guidance and comments made in the Guidelines and Technical Basis section are not enforceable. The SDT thanks you for the comment. The SDT and external reviewers have tried to pay close attention to the relationship between the language in the Guidelines and Technical Basis and the requirement language.

ACES Standards Collaborators commented on several aspects of the CIP Standards. The commenter asked why response was capitalized in Attachment 1, Section 4 of CIP-003 but lower case in Requirement R1. The commenter further suggested removing 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. Finally, the commenter recommended that the SDT remove the phrase, "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." The SDT thanks you for your comments. The word "response" in CIP-003, R1 was made lower case for consistency with the other subparts and to distinguish components that are a defined term and those that are not. In Attachment 1, Section 4, "response" was considered the title of a plan section. Regarding the commenter's first recommendation to revise the guidance, the SDT removed part of the sentence to more accurately accommodate the scenario. Regarding the second recommendation, the SDT determined that the language is consistent with the intent of the requirements.

Duke Energy suggested revising the language in CIP-003, Section 2 to the language from the previous posting of the standard. The commenter noted that as currently written, Section 2 could be interpreted to require an authorized users list. Thank you for your comment. Following the second posting, the SDT made a number of revisions in response to stakeholder comments. A greater portion of stakeholders supported the third proposal than the second proposal. The SDT intent is not to imply requirement of a list, but also not to exclude it as an option to demonstrate compliance.

Duke Energy commented that the measures in Section 2 of Attachment 2 do not match the current requirement language. The SDT thanks you for the comment. In response to comments in the second posting, the SDT removed examples from the requirement, but felt they were still valid to clarify potential ways to meet the requirement objective.

Lincoln Electric System commented that Section 1 does not specify who is to receive the reinforcement of cyber security practices. The SDT thanks you for your comment. Because CIP-003 requirements focus on the asset

containing low BES Cyber Systems and not the people, the Low Impact Cyber Security Plan(s) can identify the target audience.

Indiana Municipal Power Agency commented that the Guidelines and Technical Basis section includes important information that should be included in the requirement language. Specifically, the commenter suggested the SDT put the language regarding an entity not having to track who received the awareness in the requirement. Thank you for your comment. Throughout the development process, the SDT received competing preferences for the amount of language to include in the requirements. The SDT settled on the proposed language to provide enough language to explain the intent but not restrict flexibility. Specific to the example cited, the intent for CIP-003 is for entities to deliver awareness material. The intent is that entities will not have to track the individuals subject to the awareness program.

The United Illuminating Company commented that there are inconsistencies between the LERC definition and the Guidelines and Technical Basis. The SDT thanks you for your comments. In response to previous comments regarding how entities would demonstrate compliance when LERC is not present, the SDT included specific language within the Guidelines and Technical Basis that entities are not required to establish LERC and can document the absence of LERC in their low impact cyber security plan. The SDT meaning of the word "via" in the definition of LERC is that meaning found in the dictionary such as, "using," "by means of," "by way of," or "through," etc. The SDT created Reference Model 4 to highlight that just because there is a protocol change from IP to serial, the protocol change, itself, does not mean that LERC is not present. The SDT also uses the word "access" within the definition of LERC to call attention in Reference Model 4 that the IP/Serial converter has extended the "access" over the serial conversion communication; thereby extending the bi-directional routable protocol connection. The SDT specifically provided Reference Model 5 and Reference Model 6 to highlight two examples of how "access" can be managed so there would not be LERC. Responsible Entities are expected to identify if there is communication that is external to the asset containing the low impact BES Cyber System to determine whether there is LERC. This can be done in many different ways, including analyzing the communication of the low impact BES Cyber System at the asset containing the low impact BES Cyber System or analyzing the communication to the asset containing the low impact BES Cyber System or some other method that yields identifying whether there is LERC.

Transient Devices

ACES Standards Collaborators requested additional guidance on the documentation needed for the review of antivirus, malicious code, and system hardening practices in Section 2.1. Furthermore, the commenter wanted to know which entity is responsible for any security failure of a vendor Transient Cyber Asset that went through the review process. The SDT thanks you for your comment. The plan allows flexibility for the entity to provide documentation such as emails, contract, and change orders, among other documentation. The entity's responsibility is to review, and the entity will be audited to that requirement.

Lincoln Electric System requested clarification on what the authentication protocol would be for full-disk encryption. The commenter further asked if it means full-disk encryption with pre-boot authentication. The SDT discusses full-disk encryption with authentication in the Guidelines and Technical Basis. Please see page 43 of CIP-010-7.

NIPSCO commented that the SDT did not adhere to the directive in FERC Order No. 791 regarding transient devices. The commenter did not agree with the SDT's removal of the 30-day exemption. Thank you for your comments. Through the stakeholder development process, the SDT developed a set of requirements applicable to transient devices. The SDT received input and insight from stakeholders including NERC and FERC staff, to devise the proposed requirements. The SDT feels the proposed requirements address the risks presented by the use of transient devices and responds to the directives in Order No. 791.

Implementation Plan

ACES Standards Collaborators expressed concern over the difficulty of managing three versions of standards during implementation and asked whether the implementation plan would be consolidated. In addition, the commenter asked for an explanation of an unplanned change. Thank you for your comment. Because the revisions in response to Order 791 did not result in revision to all of the CIP version 5 standards, the implementation schedule for the unrevised standards will remain active. Version 7 incorporates the revisions made in "version 6." Since the version 7 revisions are expected to be complete for the upcoming filing, the "version 7" implementation plan will be submitted to FERC for approval. To illustrate the implementation deadlines in simpler terms, the SDT is working with NERC to create a reference worksheet for entities to see the version 5 and version 7 deadlines in one place. The Implementation Plan for CIP Version 5 discusses the CIP-002-5 annual assessment as the timing to identify unplanned changes. This portion of the CIP Version 5 Implementation Plan will remain in effect and will apply to CIP-002-5 when effective on April 1, 2016.

NRECA requests that the SDT consider adding further clarity to the CIP V5 Revisions Implementation Plan. Thank you for your comment. NERC advised the SDT that because, as you note, the current revisions do not revise all of the CIP version 5 standards, the formal Implementation Plan for this project will not replace the version 5 Implementation Plan. However, the SDT is working with NERC to create a reference worksheet for entities to see in one place the compliance deadlines for the version 5 standards and the revised version 5 standards. The SDT conveyed your request to post such a reference during final ballot.

AEP suggested that the SDT should consider providing additional implementation time for CIP-010 in consideration of entities with large numbers of transient devices. Thank you for your comment. A majority of stakeholders approved the proposed implementation plan for CIP-010-7, Requirement R4.

Other

ACES Standards Collaborators suggested the SDT revise "again" to "against" in the mapping document and suggested the SDT use the defined term Cyber Security Incident in the VSLs. The SDT revised the mapping document and VSLs accordingly. The commenters also suggested removing Special Protection System from the standards because Remedial Action Scheme was adopted by the NERC Board. The SDT thanks you for your comment and will submit the revision to any future review of the standards once the definition is FERC-approved.

AEP expressed concern in implementing the CIP standards while the Implementation Study participants, NERC, and the Regional Entities are still developing guidance. AEP recommended NERC resume the interpretation process as soon as possible. In response, NERC notes that the Standard Processes Manual outlines the interpretation process and NERC continues to process the requests as they are received.

SMUD requested clarification on how the Guidelines and Technical Basis section will be used for regional audit approaches. The SDT relayed this comment to NERC. NERC notes that it strives for consistency across the ERO and will encourage all Regional Entities to consult the Guidelines and Technical Basis for better understanding of the standards.

Exelon and American Public Power Association suggested that NERC make the RSAW development more transparent and work with the SDT to post revised RSAWs. The SDT relayed this comment to NERC. The SDT continue to be available and willing to work with the RSAW development team.

Centerpoint expressed concern that the SDT made revisions to standards that had already received sufficient stakeholder approval. Thank you for your comments. The SDT felt that the constructive comments submitted in the second posting warranted additional revisions even though the proposals passed ballot. The increase in

affirmative votes in the third posting suggests that the additional work was justified to stakeholders. The SDT will proceed to final ballot and anticipates delivering the revisions to the NERC Board in February 2015.

NRECA and Exelon support the SDT's efforts to complete revisions in all four issue areas by the February 2015 filing deadline. Thank you for your comments. The SDT worked with this goal in mind. If the proposed standards pass final ballot and the NERC Board adopts the revised standards, NERC committed to file revisions in response to all four directive areas in February 2015.

Northeast Utilities recommended that the SDT continue working on the standards. Thank you for your comments. A majority of stakeholders approved the proposed revisions. The proposals will advance to final ballot.

Duke Energy and Northeast Utilities stated that they support the comments from EEI, and Florida Municipal Power Agency stated that it supports SMUD's comments.

Flathead Electric Cooperative, ACES Standards Collaborators, NRECA, Exelon, Northeast Utilities, American Transmission Company, AEP, MidAmerican, and Florida Municipal Power Agency thanked the SDT for its work on the standards. The SDT sincerely appreciates the support and active participation from all entities throughout the development process.