NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-02
CIP Version 5 Revisions

Consideration of Comments
Initial Comment Period

September 3, 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 June 2, 2014 through July 16, 2014. Stakeholders were asked to provide feedback on the Reliability Standards and associated documents through a special electronic comment form. There were 98 sets of comments, including comments from approximately 196 different people from approximately 142 companies representing all 10 Industry Segments as shown in the table on the following pages.

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 two 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. *The Standard Drafting Team (SDT) developed objective criteria in the processes in CIP-003, Requirement R2 to address the directive in FERC Order No. 791. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.*

Question 1 deals with the directive to develop modifications to the CIP standards to address security controls for assets containing low impact BES Cyber Systems. The SDT sought comments on its approach in modifying CIP-003-6, Requirement R2.

Placement

During the development prior to the initial posting, the SDT discussed the placement of the low impact requirements on many occasions. There were many commenters who suggested spreading out the requirement parts into the relating standards (for instance, CIP-008 for incident response), while a similar amount of commenters suggested keeping the requirements in CIP-003. The commenters supporting the allocation of the low impact requirements to the relating standards suggested to use existing applicability tables and sought justification for why the low impact requirements were in CIP-003 Requirement R2. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require a plan to address the Order No. 791 directive for more objective criteria. The applicability tables are no longer being used.

In response to comments that CIP-003 is a policy standard, the SDT developed the attachment approach where the requirement requires a plan whose elements are detailed in an attachment to the standard. The team also added language to CIP-003 clarifying that Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. The SDT discussed the costs and benefits of the placement issue and came to the conclusion that having the low impact requirements reside in CIP-003 was the best approach because it allows those with only assets containing low impact BES Cyber Systems to focus on one standard. As well, the SDT determined that an entity's management of low impact protections may differ from the medium and high impact protections (such as site level program implementation versus device level program implementation) and therefore the requirements are best suited to reside in one standard.

Reference to CIP-002-5.1

CenterPoint Energy questioned why the SDT deleted the link back to CIP-002-5.1, Requirement R1, Part 1.3. The SDT had removed the link in the previous version believing using "low impact assets" was sufficient. In response to this comment, the SDT has updated the requirement language to return the link to CIP-002-5, Requirement R1, Part 1.3. The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System." The SDT states that this creates the direct link between the CIP-003-6, R2 and CIP-002-5, R1, Part 1.3 language.

Part 2.1

Pacific Gas and Electric, Colorado Springs Utilities, Phillips 66, Consumers Energy Company, City of Tallahassee, and Salt River Project supported the proposed Requirement R2, Part 2.1 as written for reviewing and obtaining CIP Senior Manager approval.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, and Oncor suggested allowing a delegate for CIP Senior Manager approval of policies. In initial crafting of revisions based on industry comment, the SDT did provide the option for a delegate to approve the documented cyber security policies. However, in the most recent revisions,

the SDT rolled the low impact policy requirements into the existing Requirement R1. In that requirement, CIP Senior Managers and not delegates must sign off on the policies for any impact rating. Therefore, only the CIP Senior Manager can approve the policies applicable to assets containing low impact BES Cyber Systems under Requirement R1, Part 1.2.

For the applicability, Exelon proposed "BES Assets containing Low Impact BCS." In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System."

Dominion suggested removing the word "applicable" because it would have to apply controls at Control Centers even if it does not have one. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the evaluation of specific elements related to the assets containing low impact BES Cyber Systems. The evaluation provides the entity with the ability to determine applicability.

Part 2.2

ACES members asked if Part 2.2 was by site or collection of sites. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require a plan. Within the plan, the SDT has stated that entities can develop their plans by "asset or groups of assets."

Pacific Gas and Electric, Colorado Springs Utilities, Phillips 66, Consumers Energy Company, City of Tallahassee, TAL, and Salt River Project supported the proposed Requirement R2, Part 2.2 as written for restricting physical access.

Arkansas Electric Cooperative Corporation, PNM Resources Resources, Luminant Energy Company, LLC, and South Carolina Electric and Gas stated that restricting physical access does not provide sufficient criteria. The entities asked for clarification on what the difference is between operational or procedural controls. The entities also requested that the Guidelines and Technical basis section align with the requirement part language. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. Entities now evaluate possible physical security objective criteria and develop an entity-specific plan.

Similar to its comment for Part 2.1, Exelon proposed that the applicability read, "BES Assets containing Low Impact BCS." In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT is now using "The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System."

Part 2.3

Pacific Gas and Electric, Colorado Springs Utilities, Phillips 66, Consumers Energy Company, City of Tallahassee, TAL, and Salt River Project supported the proposed Requirement R2, Part 2.3 as written for monitoring.

Dominion and Xcel Energy commented to remove this requirement part completely since the breakout of Control Centers is contradictory to FERC Order No. 791. In response, the SDT agrees and has removed the reference to Control Centers.

Duke Energy pointed out that it is difficult to determine and monitor physical access points for lows. Duke suggested requiring a Physical Security Perimeter (PSP) to capture the intent. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. Registered Entities now evaluate possible physical security objective criteria and develop an entity specific plan.

Kansas City Power & Light commented that because reference to physical access points is not in relation to defined PSP, the requirement part is more stringent than CIP-006-5, Requirement R1, Part 1.4. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. Entities now evaluate possible physical security objective criteria and develop an entity-specific plan.

Similar to its comments for Parts 2.1 and 2.2, Exelon proposed that the applicability read, "BES Assets containing Low Impact BCS." Exelon further asked who is considered a visitor. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT has updated the reference to CIP-002 to read, "Each Responsible Entity with at least one asset identified in CIP-002 containing a low impact BES Cyber System." The SDT no longer has specific carve-outs for "Control Centers." With regard to the visitor question posed by Exelon, the SDT has removed that language from the requirement part and attachment, as well as the Guidelines and Technical basis section.

Part 2.4

Northeast Power Coordinating Council, Pacific Gas and Electric, Colorado Springs Utilities, Tennessee Valley Authority, Dominion, Edison Electric Institute, Florida Municipal Power Authority, NiSource, Oncor Electric Delivery Company LLC, PPL NERC Registered Entities (multiple), PacifiCorp, Western Area Power Administration, Large Public Power Council, Tacoma Public Utilities, New York Power Authority, Sacramento Municipal Utility District, Hydro One, Kansas City Power & Light, NV Energy, Salt River Project, Austin Energy, Northeast Utilities, Independent System Operator/Regional Transmission Organization (ISO/RTO) Standards Review Committee (ISO/RTO SRC), Luminant Energy Company, LLC, and South Carolina Electric and Gas had comments on the phrase "external routable protocol paths." There were concerns that this phrase implies some sort of Electronic Security Perimeter (ESP) and inventory, as well as suggestions to address "untrusted" networks (those not owned by the entity). Clarifications were requested to what the phrase means and, more specifically, what "external" was in reference to. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems. The SDT does not use the phrase "external routable protocol paths" and has created definitions for Low Impact BES Cyber System Electronic Access Point (LEAP) and Low Impact External Routable Connectivity (LERC) to further clarify the lows requirement.

CenterPoint Energy, Bureau of Reclamation, and Duke Energy suggested consider of using "authentication" instead of "access control." In response, authentication was considered by the SDT, but the implications of a required list prevented this inclusion. The SDT states that the language as stated does not require a firewall to control access. The SDT developed two definitions and added explanatory guidance to help clarify the intent of the "access control" requirement.

PACIFIC GAS & ELECTRIC, Colorado Springs Utilities, Florida Municipal Power Agency, Xcel Energy, Idaho Power, Hydro One, and Exelon Companies stated that this requirement part implies an inventory must be done to prove compliance. In response, the SDT notes that an inventory may be the best option for proving compliance, but is not the only option and is not the required option.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Oncor Electric Delivery Company LLC, Associated Electric Cooperative, Inc., Phillips 66, Liberty Electric Power LLC, and Georgia Transmission Company commented that requiring justification for every firewall rule results in a significant amount of man-hours. Furthermore, the entities suggested to remove or reduce the part to not include inbound and outbound access permissions and remove the reason for granting access. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. The electronic access controls have been modified to "For any Low Impact External Routable Connectivity, establish a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all

other access." The SDT has removed "reasons for granting access." The SDT has modified the Guidance to explain that entities should maintain some documentation and be able to explain why the access permissions are in place.

Nebraska Public Power District and MidAmerican Energy Company suggested removing "default" as written as it appears that a firewall is the only solution. In response, the SDT removed "by default" and the language as stated does not require a firewall to control access. The SDT included additional discussion in the Guidance section for element 2.4.

Consumers Energy Company commented that the part should clearly state access points can reside either at the sub or at remote end of external routable protocol path. In response, the examples provided in guidance depict examples that the access points can be at the substation specifically or located at a regional or centralized location.

Massachusetts Municipal Wholesale Electric Company suggested to align this part more closely with CIP-005 because by avoiding the ESP and Electronic Access Point (EAP) requirements it becomes difficult to interpret and less effective at protecting. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. The SDT has created two new definitions for Low Impact BES Cyber System Electronic Access Point (LEAP) and Low Impact External Routable Connectivity (LERC).

Part 2.5

Northeast Power Coordinating Council commented that the incident response plan requirement part is inconsistent with CIP-008-5 Requirement R2's incident response plan for Medium/High. In response, the SDT has modified the approach to the assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Tennessee Valley Authority and Exelon asked if one incident response plan can encompass multiple facilities/BES Cyber Systems and if testing of the plan means that testing must occur for each facility. In response, the SDT has modified the approach to require that entities with assets containing low impact BES Cyber Systems develop a plan to address objective criteria in CIP-003-6, Attachment 1. The team intends for entities to have the latitude to develop a plan encompassing multiple facilities if they see fit and added "Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets" to the Attachment language. Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans.

Florida Municipal Power Authority, Tampa Electric Co., and Southern suggested limiting the scope of part 2.5 to low impact Control Centers and removing any reference that might include out-of-scope terms such as ESPs and PSPs. In response, the SDT has removed all specific carve-outs to "Control Centers."

Large Public Power Council commented that CIP-003 Requirement R2, Part 2.5 for low impact BES Cyber Systems should be added to the CIP-008 standard maintaining the 36 calendar months timeframe specific to low impact BES Cyber Systems. In response, the SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Phillips 66 commented that the incident response plan is duplicative of EOP-004 that covers cyber incidents. In response, the SDT states that the Cyber Security Incident response is required to be a part of the CIP standards and not covered in EOP-004.

Tampa Electric Co. and Southern suggested removing the word "paper" to allow for all types of drills. In response, the SDT has modified the incident response elements with the plan.

Consumers Energy commented that the language of the standard needs to clarify that the Responsible Entity can create a holistic incident response plan utilizing physical security mechanisms that lead to Cyber Security Incident identification, classification, and response; and that logging and monitoring of low impact BES Cyber Systems is not required. In response, the SDT has utilized language from CIP-008-5, which is exclusive to cyber security.

Lincoln Electric System recommended either removing Requirement R2, Part 2.5 or add an exclusion for 'Low Impact assets without routable connectivity' in recognition that a cyber-incident at a non-routable connected substation does not affect any other Low, Medium or High Impact BES Asset. In response, the SDT has utilized the language from CIP-008-5, which is exclusive to Cyber Security and does not exclude non-routable connections.

Idaho Power and PNM Resources suggested moving part 2.5 to CIP-008. Similar to the comments earlier regarding placement, the SDT notes that keeping the low impact obligations in one standard is the best place for the objective criteria to reside based on feedback from industry. The SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Exelon suggested the SDT provide clear guidance stating that sites with low impact BES Cyber Systems may be covered by an enterprise-wide Cyber Security Incident response plan or other approach, and assurance that a Cyber Security Incident response plan is not required for each site. In response, the SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Southern Company suggested providing additional information in the Guidelines and Technical Basis section on the use of the term "Cyber Security Incident" as it applies to low impact BES Cyber Systems. In response, the SDT has added language in the guidance that the entity should have a documented Cyber Security Incident response plan that includes each of the topics listed. For assets that have limited or no connectivity external to the asset, it is not the intent to increase their risk by increasing the level of connectivity in order to have real-time monitoring. The intent is if in the normal course of business suspicious activities are noted at an asset containing low impact BES Cyber Systems, there is a Cyber Security Incident response plan that will guide the entity through responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Part 2.6

CenterPoint, Northeast Power Coordinating Council, Dominion, Edison Electric Institute, Large Public Power Council, Southern, NiSource, Public Service Enterprise Group, New York Power Authority, Xcel, PNM Resources, Exelon, NV, American Electric Power, Georgia Transmission Corporation, Northeast Utilities, MEC commented that the level of detail for security awareness is beyond what is required for mediums and highs. In response, the SDT has modified the language for security awareness to align with CIP-004, Requirement R1.

Tennessee Valley Authority, Idaho Power, PNM Resources, Exelon, and MidAmerican stated that this part should be located in CIP-004. In response, the SDT notes that keeping the low impact obligations in one standard is the best place for the objective criteria to reside based on feedback from industry. The SDT has modified the approach to assets containing low impact BES Cyber Systems to require the development of a plan to address objective criteria. In Attachment 1, Responsible Entities with multiple impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the elements for the development of low impact cyber security plans. Each Responsible Entity can develop a cyber security plan either by individual asset or groups of assets.

Edison Electric Institute, Tampa Electric Co., NiSource, and Oncor suggested removing the references to the subpart requirements as they may not apply to all entities. The commenters also suggested removing the quarterly component. In response, the SDT has modified the language for security awareness to align with CIP-004.

PPL, Edison Electric Institute, Tampa Electric Co., Southern, Phillips66, NiSource, Public Service Enterprise Group, Xcel, and NV Energy recommended removing the language surrounding quarterly and modifying it to annually. In response, the SDT has modified the language to “at least once every 15 calendar months” from “quarterly.”

Consumers Energy commented that the language of the standard needs to clarify that the Responsibility Entity’s security awareness program applies only to its employees, but could include non-employees, and that posters, emails, and topics at staff meetings are sufficient delivery method and that tracking of reception is not required. LES had a similar comment regarding how security awareness is provided and proven on a per asset basis. In response, the SDT notes that methods of delivery are addressed in the guidance, and that the scope of awareness training is left to Responsible Entities to determine (non-employee vs. employee).

Dispersed Generation Resources (DGR)

Edison Electric Institute, Tampa Electric Co., NiSource, Oncor, We Energies, PNM Resources, Exelon, NV Energy, Florida Power & Light, and MidAmerican commented that the scope of dispersed generation in the CIP-003-6 Applicability section should be limited and similar to PRC-005. In response, the CIP SDT notes that coordination with the DGR SDT has been occurring and will continue to occur. Since CIP-002-5.1 is not being revised from the FERC Order No. 791 directives, the DGR SDT is best suited to modify the applicability and post the revised changes to CIP-002-5.1 for an initial comment and ballot period. Not slated as a “high priority standard” in the DGR’s project plan, CIP applicability changes can fall into the DGR’s “medium priority” bucket as it continues its work on modifying certain standards to address dispersed power producing resources. The DGR SDT has an upcoming meeting in September 2014 and the CIP applicability change is on its agenda. The CIP SDT will continue to coordinate with the DGR SDT as necessary to provide technical basis and justification for any work the DGR SDT provides in revising CIP-002-5.1. A timeline for that posting should come out relatively soon to give commenters assurance that work will continue through the DGR SDT’s SAR.

Reliability Standard Audit Worksheets (RSAWs)

Pacific Gas & Electric recommended the performance of an annual sampling assessment of such classified systems to determine the state of their security controls. This could be done using NERC sampling guidelines. In response, the SDT notes that this is most appropriately addressed through the RSAW approach.

Florida Municipal Power Authority commented that the RSAWs do not provide any level of clarity as to how an entity can expect to be audited. Large Public Power Council, Tacoma, New York Power Authority, and Sacramento Municipal Utilities District commented that specific RSAWs can be created for the low impact requirements that reduce the number of RSAWs that need to be completed by entities. In response, the SDT notes that there is a

specific RSAW working group focused on revising the posted RSAWs. That team will take into account the RSAW comments and revise them accordingly.

Exelon encouraged the RSAW development team to continue its work in modifying the RSAWs and possibly include RAI components for the assets containing low impact BES Cyber Systems to demonstrate how RAI can alleviate compliance concerns. In response, the SDT notes the RSAW working group will take into account the RSAW comments and revise them accordingly.

FirstEnergy had concerns with the RSAWs and support Edison Electric Institute's comments. In response, the SDT notes that there is a specific RSAW working group focused on revising the posted RSAWs. That team will take into account the RSAW comments and revise them accordingly.

General Comments

CenterPoint commented that Measure M2 should be revised to reflect the pattern in other Measures of CIP-003. CenterPoint further suggested that the SDT consider the pattern found in other standards and remove the word "any" from the draft Measure. In response, the SDT has made the appropriate modifications to the Measures based on the revised language in CIP-003.

Edison Electric Institute, Tampa Electric Co., NiSource, Oncor, and We Energies suggested revisions to the background and guidelines and technical basis sections to align the drawings and the words of the requirement. In response, the SDT has modified the current language to remove the table within Requirement R2, electing to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Duke Energy commented that there are the same control measures in place as medium impact BES Cyber Assets, which will become extremely burdensome and provide little benefit to reliability. In response, the SDT has modified the language to ensure a compliance burden less than high and medium impact BES assets based on risk to the BES.

Southern commented that the Applicable Systems column should be amended to state "Assets containing low impact BES Cyber Systems." In response, the SDT has modified the current language to remove the table within R2, electing to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Rayburn asked if the standard sufficiently covers the appropriate levels and tactics expected to be used to be compliant. In response, the SDT has modified the current language to remove the table within R2, electing to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Dynegy requested the SDT provide guidance in the standard as to how to determine low impact BES Cyber Systems without using the detailed inventory process. In response, the SDT has modified the current language to maintain "policy and program" level within the requirement and include additional objective language within an associated Attachment.

Occidental commented that subjective interpretations by Regional Entities are still a very real concern. In response, the SDT has forwarded the comments to NERC.

Idaho Power suggested that the applicability section of all these requirement parts addresses low impact BES Cyber Systems. It is counterintuitive to think that a list of low impact BES Cyber System will not be required to show compliance. In response, the SDT states that anticipating high counts of low impact BES Cyber Systems, the

SDT intends to allow Responsible Entities to shift their compliance approach away from rigorous Cyber Asset list maintenance and toward consistent maintenance of the low impact controls identified in CIP-003-6. The SDT believes the list of assets containing low impact BES Cyber Systems generated as a result of CIP-002-5.1, R1 is sufficient. However, Responsible Entities are not prohibited from developing and maintaining individual inventories of their low impact BES Cyber Systems components for their own business needs.

Hydro One suggested modifications to the VSLs. The SDT has made the revisions to the VSLs.

Encari commented that the Guidelines and Technical Basis section continues to use "external routable connectivity" in the discussion of Requirement R2 in parts 2.3 and 2.4. In response, the SDT has modified the current language to maintain "policy and program" level within the requirement and including additional objective language within an associated Attachment.

Kansas City Power & Light suggested that the Guidelines and Technical Basis section includes references to "belief" and "intent" along with descriptions of what entities "should" be doing. The need for such language indicates that the requirement language is not able to stand on its own and results in a need to be audited by the Guidelines and Technical Basis section. Section 2.4 - The two sentences beginning with "The electronic access controls should address..." go beyond the purview of the language of the requirement and serve to dictate what "should" be addressed. It is recommended that these sentences be stricken from the Guidelines and Technical Basis section. In response, the SDT has modified the Guidelines and Technical Basis section throughout the standard based on the comments received and the revisions made.

Nebraska Public Power District commented that while the drafting team has tried to show in the guidance what would be acceptable and what would not, in essence they have determined the "how" the requirement will be audited by showing only a firewall solution. In response, the SDT has modified the language to provide clearer objective criteria which allows for flexibility to Registered Entities.

American Public Power Association and National Rural Electric Cooperative Association commented that the SDT has gone too far in certain aspects of specificity of the requirement parts and the compliance costs exceed the reliability benefit to the BES. In response, the SDT has modified the language to provide clearer objective criteria and allows flexibility to Registered Entities. This allows for entities to tailor their internal plans to cover the risk that to assets containing low impact BES Cyber Systems pose.

National Rural Electric Cooperative Association recommended that NERC use the Requirements on low impact assets to demonstrate how RAI can alleviate the compliance concerns and create a reasonable approach to compliance. The SDT notes that it has forwarded these comments on to NERC.

Northeast Utilities commented that there are inconsistent testing time frames. Instances where there was a failure to extend implementation time-frame beyond the original version 5 effective compliance date. In response, the SDT has modified the implementation schedule to address inconsistencies.

MidAmerican provided suggested revisions to the Background section to include a paragraph referencing the tables and applicable systems column. The SDT has modified the approach to the low impact directive. The tables and applicable systems column are no longer being used.

Empire commented that the measures are about the documentation of operational controls and show nothing to prove implementation. There is an inconsistency between the requirement and what will be needed to show compliance to the requirement. In response, the Measures have been revised according to the revisions made to the Requirement and Attachment 1. A Measure provides identification of the evidence or types of evidence that

may demonstrate compliance with the associated requirement. Entities must show evidence of implementation of their plans to demonstrate compliance to the Requirement.

Southwest Power Pool Regional Entity disagreed with the premise in the Guidelines and Technical Basis section of the standard that compliance can be demonstrated purely through presentation of the documented processes at audit. There is an expectation that the documented processes will be implemented by the Responsible Entity. The guidelines should inform the Responsible Entity and the auditor what is expected to comply with the requirements and not how the requirements should be audited. The comment that the SDT strongly believes sampling is not necessary is inappropriate and should be removed. In response, the SDT has revised this section and removed the sampling component from this section.

Manitoba Hydro commented that section C of the Compliance section 1.3 is unclear, specifically that the meaning of “Complaints Text” is unclear. In response, the SDT has removed the word “Text” to be consistent with the other NERC Reliability Standards.

Luminant provided suggested revisions to multiple aspects of the Guidelines and Technical Basis section. The SDT has considered those suggestions as it went through the section as a whole and provided updates based not only on comments received, but also on the revisions made to CIP-003-6.

Massachusetts Municipal Wholesale Electric Company suggested that the Implementation Plan allow for a phased in approach. In response, the SDT agrees and has proposed a phased approach to the Implementation Plan allowing an additional implementation time for physical and electronic access.

Question 2: CIP-006-6 and CIP-007-6

2. *The SDT developed CIP-006, Requirement R1, Part 1.10 and revised CIP-007, Requirement R1, Part 1.2 to meet the directive in FERC Order No. 791 to address protections for nonprogrammable components of communication networks. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.*

Question 2 deals with the directive to create a definition of "communication networks" and develop new or modified standards that address the protection of communication networks.

CIP-006-6, Requirement R1, Part 1.10

Encryption

In response to ISO/RTO SRC and Tennessee Valley Authority, the SDT does not believe the Reliability Standards are an appropriate location for approved cryptographic protocols. This is due primarily to the ever-changing number of protocols and vulnerabilities in cryptosystems. Also, an approved encryption concerns both protocol and implementation. This type of information is best left to guidelines.

ERCOT suggested a Critical Infrastructure Protection Committee (CIPC) guideline be developed on acceptable encryption protocols, methods, and key management. In response, the SDT notes that CIPC may develop guidelines as part of its charter, which states that guidelines are documents that suggest approaches or behavior in a given technical area for the purpose of improving reliability. Reliability guidelines are not binding norms or mandatory requirements. Reliability guidelines may be adopted by a Responsible Entity in accordance with its own facts and circumstances. Any entity may submit a request for the CIPC to develop guidance, and the SDT will consider this suggestion after the second posting and discuss with NERC staff.

American Public Power Association and Florida Municipal Power Authority showed support for encryption as an option, but would reevaluate if encryption were removed or scope expanded. The SDT thanks those entities for their comments.

Tampa Electric Co. commented that monitoring the status of communication link is duplicative of COM-001-1.1 R1.1. Failure of communication links does not necessarily need to be reported through the BES Cyber Security Incident Response Plan. In response, the SDT states the communication link failure is specific only to the nonprogrammable components outside of the PSP and not the communication to other entities covered by COM-001-1.1 R1.1. The incident response component is only necessary if the monitoring/response option is used to protect the cabling and components. The incident response is included because monitoring alone does not provide the necessary physical security to the BES Cyber System.

NextEra Energy commented that rather than allow encryption and monitoring, require secure conduit, cable trays or defense-in depth approach for the BES facility. In response, the SDT notes that secure conduit and cable trays meet the obligation to restrict physical access. These options are mentioned specifically in the Guidelines and Technical Basis section for CIP-006-6. The defense-in-depth approach for the BES facility may also meet the same obligation, but encryption and monitoring are provided as specific and measurable options.

Tri-State commented that for monitoring controls, a 15-minute window for notification is typically not enough time to respond to an event. In response, the 15-minute window is to issue the alert or alarm in response to an event. The actual response does not have a time obligation. The SDT agrees time measured responses are not appropriate for this requirement part.

Pacific Gas & Electric and Southwest Power Pool Regional Entity commented that for monitoring controls, a timeframe does not exist for response or investigation and that ignoring a momentary interruption could result in not detecting a tap. Also, for short-run cables, investigation is not feasible. In response, the SDT does not believe a time obligation for response is appropriate for this requirement part. Operational variances in responding to an incident are best left to the entity's incident response plan. In response to Southwest Power Pool Regional Entity regarding tap detection, the entity would contemplate this scenario when selecting this option for protection. The SDT states that the controls, as written, sufficiently guard against this risk.

Pacific Gas & Electric recommended that for monitoring controls, a CIP Senior Manager sign-off should be required to ensure implementation remains intact as designed. In response, the CIP Senior Manager sign-off would not change the obligation for the entity. An entity may choose to employ a sign-off as part of their internal controls program, but this should not be a requirement.

Kansas City Power & Light commented that a Physical Access Control System (PACS) or PSP is not specifically required, and it may be possible to comply with CIP-006 without having a PACS or PSP. Kansas City Power & Light suggested requiring these as part of CIP-006 Requirement R1. In response, this comment is outside the scope of the Standards Authorization Request for this project. A PSP is not specifically required because an entity may be able to meet the objectives of physically securing the BES Cyber System without a PSP or PACS.

Tacoma Public Utilities stated a concern that a detailed cable map for every cable path relevant to the ESP will be required to demonstrate compliance. In response, the obligation to maintain a detailed cable map is not a Requirement of the Reliability Standards. The SDT has passed these concerns to the NERC Compliance staff to guide development of the RSAW.

Exelon suggested clarification that applicability only applies to ESPs with External Routable Connectivity. The SDT has provided additional guidance to clarify the bounds of this Requirement Part is the ESP. By definition, Electronic Access Points provide External Routable Connectivity.

Luminant Energy Company commented that for CIP-006-6 R1 and R2, a reason for removing all but the Severe VSL needs to be provided. For example, what if an entity had a process to retain logs for 90 days but instead retained all of the logs? In response, the CIP-006 VSLs have been binary (i.e. Severe only) since version 2 because of the FERC Order addressing VSLs for CIP stating: "Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary rather than gradated Violation Severity Levels."

Equally Effective Solution and Suggested Revisions

Dominion, Bureau of Reclamation, Xcel Energy, Texas Reliability Entity, Tri-State, Empire District, Southwest Power Pool Regional Transmission Organization, ISO/RTO SRC, ERCOT asked how "equally effective logical protection" be measured. The commenters suggested possibilities: (1) equal to other options, (2) describe how protection would be measured, (3) cable travels through facilities that provide physical access only to authorized personnel, (4) use of armored wire, (5) level of encryption, or (6) altogether removal of the 3rd bullet. In response, the SDT notes that the intent of including other effective logical protection is to allow entities the option of defining this protection. An entity may demonstrate compliance by showing how it protects the cabling and nonprogrammable components similar to the other options listed in the Requirement Part. The guidance for CIP-006-6 has been updated to make this clear. The specific suggestion to have cable travel through facilities that provide physical access to only authorized personnel would be considered physical access restrictions and has been included in the Guidelines and Technical Basis of CIP-006-6. The use of armored wire is functionally equivalent to the required physical access restrictions.

Similar to the comment raised above, Southwest Power Pool Regional Transmission Organization, ISO/RTO SRC, and Southern California Edison Company stated concerns on whether evidence will be necessary to show that physical access restrictions cannot be implemented. Suggestion to make clear that there is a choice between physical access restriction and alternative means of protection. In response, if an entity selects one of the alternatives in this Requirement Part, the Requirement language makes clear this is when such physical access restrictions *"are not"* implemented. Therefore, there is no additional obligation for the entity to demonstrate it cannot apply physical access restrictions. The Requirement leads with physical access restrictions to make sure the physical security objective is maintained.

Bonneville Power Administration and Massachusetts Municipal Wholesale Electric Company commented that control coverage is insufficient to provide adequate protection of the BES. Massachusetts Municipal Wholesale Electric Company further suggested CIP-006-6 should also include requirements for low impact BES Cyber Systems. In response, the SDT proposes the standards revisions as adequate and appropriate to protect the reliability of the BES. In doing so, the level of effort to meet the Requirement has been weighed against the risk posed to the BES.

CIP-007-6, Requirement R1, Part 1.2

Associated Electric Cooperative, Inc., National Rural Electric Cooperative Association, and American Electric Power stated that this requirement part is duplicative and overlaps with CIP-010-2 Requirement R4. In response, the Requirement to protect ports for Removable Media is different than the CIP-010-2 R4 Requirement for Removable Media. CIP-010-2 Requirement R4 concerns the Removable Media while CIP-007-6 Requirement Part 1.2 concerns the BES Cyber System ports.

Northeast Power Coordinating Council, New York Power Authority, and Hydro One suggested adding rationale for part 1.2 to the guidelines. Furthermore, the commenters suggested adding illustrative examples to the Measures and guidelines so entities and auditors will have the same interpretation. In response, additional clarification regarding the applicability has been added to the Technical Guidelines to make clear the scope of this Requirement Part as well as approaches to meeting the Requirement.

Duke and Exelon sought clarification that applicability means (a) devices located inside both a PSP and an ESP and not (b) devices within a PSP and devices within an ESP. Furthermore, the comments suggested the following for clarity: "Nonprogrammable communication components used for the connection between applicable Cyber Assets within the same ESP and within a PSP." In response, the SDT confirms that the applicability means devices located inside both a PSP and ESP. The SDT has added illustrations to the Guidelines and Technical Basis section to assist entities in understanding the applicability.

Associated Electric Cooperative, Inc. and National Rural Electric Cooperative Association sought more clarity around the term "nonprogrammable communication components." In response the SDT has provided additional examples in the Guidelines and Technical Basis that nonprogrammable communication components include unmanaged switches, hubs, and patch panels. This requirement only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and nonprogrammable communications components exist inside the PSP, that protection is afforded to these communication elements and therefore this requirement no longer applies. The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order No. 791 is one of the physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify

or explain why it chose another protection mechanism. It may choose physical security protections or the logical protections identified in the requirement at its choice.

Northeast Utilities requested additional guidance on meeting this requirement for patch panels. The entity asked, 1) if cyber assets in the ESP have disabled unnecessary ports and services, is additional protection necessary? And 2) is signage or tamper tape required for all ports that are not used or disabled? In response, there are several options to protect against the use of these unnecessary ports. The entity should select the controls that make the most sense in their environment. Disabling ports, signage or tamper tape are all possible controls.

Definitions

Consumers Energy Company, Kansas City Power & Light, and Exelon suggested defining "nonprogrammable electronic components." The SDT does not agree defining nonprogrammable communication devices would provide additional clarity. The SDT suggests the term with the use of examples provides the common understanding necessary to meet the new Requirements.

Idaho Power and Tri-State stated that this does not address the FERC directive to create a definition of communication networks and developing new or modified standards. In response, the SDT reviewed the directives related to submitting a definition for communication networks and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The existing and modified requirements cover more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.

Kansas City Power & Light raised a concern that entities will have an obligation to keep an inventory of nonprogrammable electronic components. In response, the obligation to maintain an inventory of nonprogrammable electronic components is not a Requirement of the NERC Reliability Standards. The SDT has passed these concerns to the NERC Compliance staff to guide development of the RSAWs.

Question 3: CIP-010-2

3. *The SDT developed CIP-010, Requirement R4 and revised CIP-004, Requirement R1, Part 2.1.9 to meet the directive in FERC Order No. 791 to address transient devices (Transient Cyber Assets and Removable Media). Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.*

Applicability and Placement

ISO/RTO SRC, FirstEnergy, and Tacoma Public Utilities commented to move the requirement parts to the applicability of relevant CIP-007 requirements. In response, the SDT has not moved the requirements to the applicability of other standards. Since the use of these devices is limited to the context of change management and vulnerability assessment, the SDT determined that placing the requirements within CIP-010 is appropriate. While the requirements are similar to other standards, the requirements for Transient Cyber Assets and Removable Media are not the same as the requirements for BES Cyber Systems and other permanent assets.

Encari suggested that the applicable systems should be expanded to include the EACMS and PACS that are associated with high and medium impact BES Cyber Systems. In response, the SDT has chosen to focus the requirements to the assets that are to be connected to the BES Cyber Systems that provide a BES reliability operating services, as well as those residing within the same ESP. The goal is to protect the systems that can have a direct impact on real-time operations.

San Diego Gas & Electric sought clarification that devices not directly connected to the BES Cyber System should be exempt or considered out of scope such that other devices or media that are connected to the Transient Cyber Asset would be out of NERC CIP scope. In response, the SDT considers any other Cyber Asset or Removable Media connected to a Transient Cyber Asset to require the same protections as the Transient Cyber Asset or any other Removable Media.

Duke Energy, Southern Company: Southern Company Services, Inc., Alabama Power Company, Southern Company Generation, Southern Company Generation and Energy Marketing, Luminant Energy Company, LLC, Exelon Companies, and MidAmerican Energy Company stated that there were inconsistencies in the use of the applicability part of the table. In response, the SDT notes the tables supporting CIP-010-2 Requirement R4 have been eliminated. Please refer to the definitions of Transient Cyber Asset and Removable Media for specifics of the assets in scope.

Measures

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Exelon Companies, Texas Reliability Entity, and Bureau of Reclamation commented that the measures do not align with the requirement language and that some of the measure language is unclear on the meaning. In response, the tables supporting CIP-010-2 R4 have been eliminated. The requirement obligates the entity to create and implement plans for Transient Cyber Assets and Removable Media. The measure supports this requirement. Clarification of many topics has been added to the guidance.

Guidance

CenterPoint Energy recommended removing examples of statements from Guidelines and Technical Basis to reduce redundancies with definitions of Transient Cyber Asset and Removable Media. The SDT notes that while the examples are similar to those in the definitions, the examples in the guidance are more defined and provide guidance that has been requested by industry.

Dominion requested additional language to clarify the phrase "per Cyber Asset capability." The SDT has modified the guidance to clarify "per Cyber Asset capability."

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing recommended striking the term "physical proximity" as this is not required by the standard as written. In addition, these entities recommended removing the phrase "process is to include testing and installing of updated signatures or patterns." In response, the SDT removed the language.

Edison Electric Institute and NiSource suggested the SDT correct inconsistencies in the "Applicable Systems" of the Guidelines and Technical Basis. The SDT modified the guidance to align to the attachment sections.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, and Luminant Energy Company, LLC suggested the SDT consider removing the bullets under "Examples of these devices include…" and consider strengthening the intended meaning of the list of examples to improve clarity and provide guidance to industry. The SDT considers the example list of asset types to be appropriate guidance for the industry. These are examples and are not intended to be an all-inclusive or exhaustive list.

Edison Electric Institute, NiSource, San Diego Gas & Electric, and MidAmerican Energy Company commented that the guidance goes beyond the scope of the standard in Bullet 2 under Requirement Part 4.1 of the guidance because it includes low impact. These entities further commented that the SDT should consider that transient devices should be required to have a uniform level of protection sufficient to ensure that a designated and approved transient device could be used at any facility. The SDT notes that the requirements do not apply to low impact. However, the SDT believes it is worth providing guidance to the industry that the higher impact assets should be protected from the vulnerabilities from any other asset.

Southwest Power Pool Regional Entity and Northeast Utilities recommended that the SDT add alternatives to the use of anti-malware in the Guidelines and Technical Basis. The SDT modified the standard to include an attachment with options that may be applied to address malware prevention.

Tampa Electric Company recommended clarification of the Guidelines to allow for Removable Media to be validated on a periodic basis instead of on a per-use basis. The SDT modified the requirement to obligate the entity to create and implement management plans for Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization.

Northeast Utilities suggested the SDT expound upon the "CAUTION" statement in the Guidelines and Technical Basis regarding the use of secure wireless network to only access a secured network drive containing relay configuration data. The SDT defined more guidance and Requirement language for the use of secure, restricted communications in Attachment 1.

Part 4.1 – Authorization

Dominion, Duke Energy, Large Public Power Council, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Florida Municipal Power Authority, Exelon Companies, Austin Energy, and National Rural Electric Cooperative Association commented that the requirement to authorize "Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability)" should be removed. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that

are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions.

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, and American Electric Power requested Requirement R4, Parts 4.1 and R4.6 be applicable to just high impact BES Cyber Systems and their associated PCAs and Part 4.1 be removed or modified to apply to medium impact BES Cyber Systems with External Routable Connectivity. In response, due to the wide-area impact of the high and medium impact assets, the SDT considers the application of these requirements to these assets as appropriate. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization.

Hydro One commented that the requirement Part 4.1 should state clearly who can authorize the Transient Cyber Assets. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. Any process or plan meeting compliance requirements should be owned and maintained by the appropriate parties within the entity's organization.

ISO/RTO SRC, MidAmerican Energy Company, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing commented that: 1) Authorization should include purpose for connecting the Transient Cyber Asset, start date/time, duration, and which ESPs the Transient Cyber Asset is authorized to connect to; 2) Authorization of acceptable use exceeds FERC's directive; and 3) Acceptable use should not be required to be "authorized" for each initial use of a Transient Cyber Asset, but should be separated to allow for addressing acceptable use at the policy/procedure level. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions. This also allows for assets to be documented individually, by group, or by type.

Hydro One, ISO/RTO SRC, MidAmerican Energy Company, Oncor Electric Delivery Company LLC, PACIFIC GAS & ELECTRIC, Salt River Project, and South Carolina Electric and Gas recommended revising or removing the phrase "internally installed software," requested revision of the language to allow for pre-authorized operating system, firmware, and intentionally installed software, and recommended changes to require sampling of transient devices security baselines. In response, The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions. This also allows for assets to be documented individually, by group, or by type.

MidAmerican Energy Company, Edison Electric Institute, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, NiSource, and NV Energy commented that authorization of users should not be required for the Transient Cyber Asset if users are already authorized for the applicable systems. Part 4.1 also does not consider that CIP-004-6 Requirement R4, Part 4.1 also addresses authorization, which overlaps with the CIP-010-2, Requirement R4, Part 4.1. The Transient Cyber Asset requirement (Part 4.1) should not require users to be authorized twice, once under CIP-004 and again under CIP-010. In response, the SDT modified the requirement to obligate the entity to create

and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard. The entity could use its other authorization processes to document those authorized to use Transient Cyber Assets in its plan. However, the entity needs to review the appropriateness for every person with physical access to a facility or every user with logical access to a BES Cyber System to be able to use a Transient Cyber Asset.

South Carolina Electric and Gas, Dominion, and Pacific Gas & Electric 1) recommended language changes to allow entities to implement controls and maintain flexibility to address multiple device types and functions; 2) Requested clarification that allows entities to authorize classes or groups of Transient Cyber Assets; and 3) Requested revisions to require procedures defining the acceptable use of Transient Cyber Assets and a listing of authorized Transient Cyber Assets. Such a list needs to be generic allowing entities to authorize groups of Transient Cyber Assets. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard. The plan allows for assets to be documented individually, by group, or by type.

Parts 4.2, 4.3, 4.4, and 4.5 - Malware

City of Tallahassee, ISO/RTO SRC, and Hydro One stated that parts 4.2 and 4.3 appear to be identical. In response, while the requirements are similar, there are key differences. Cyber Assets are programmable devices that may be capable of running antivirus. Removable Media are not programmable, and therefore unable to run antivirus.

Southwest Power Pool Regional Entity suggested that CIP-010-2, Part 4.2 could be construed as mandating anti-malware on a transient device. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including optional provisions for mitigation of vulnerabilities.

Tampa Electric Co. suggested that the SDT should add the “per device capability” to CIP-010-2 R4 Part 4.3 to address device limitations. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard including provisions for mitigation of vulnerabilities. “Per Transient Cyber Asset capability” is addressed where appropriate within the attachment.

American Electric Power, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Exelon Companies, ISO/RTO SRC, and Hydro One requested clarification that remediation or updating completion is required prior to use of the device and clarification on the handling of discovery of malicious code following connection of the device to a BES Cyber System. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including optional provisions for mitigation of vulnerabilities. Elements were added to the attachment that require the device to be managed or updated on demand before connection to an applicable BES Cyber System.

National Rural Electric Cooperative Association commented that Part 4.4 focused on mitigating the threat of malicious code to Transient Cyber Assets and Removable Media but should focus on protecting the BES Cyber Asset. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the

program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard including provisions for mitigation of vulnerabilities. “Per Transient Cyber Asset capability” is addressed where appropriate within the attachment.

Part 4.6 - Inspection

Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Florida Municipal Power Agency, and Duke Energy commented to consider requiring the definition of acceptable use of Transient Cyber Assets, and the process to authorize usage and evaluation of Transient Cyber Assets. The commenters requested removal of CIP-010-2 Requirement R4, Part 4.1.4 and Part 4.6. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. For assets owned by the entity, the entity is required to document its defined acceptable use of the device, limiting the activities to business functions.

Salt River Project recommended changing the language to address Entity-owned and -maintained transient devices separately from vendor or contracted support-owned and -maintained transient devices. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the Standard including provisions for mitigation of vulnerabilities. The attachment addresses assets owned by the entity, as well as those owned by vendors and contractors.

Luminant Energy Company, LLC and ISO/RTO SRC suggested considering adding an additional requirement to remediate anything found in the evaluations conducted in accordance with the requirement related to patching or unauthorized physical access and requested strengthening of the requirement to mandate that remediation or updating completion prior to use of the device. In response, The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. The attachment requires implementation of one or more of the protective measures before connecting the device.

Dominion commented that clarity is needed regarding whether an entity expected to reauthorize the baseline list of “Operating system(s) or firmware where no independent operating system exists, and intentionally installed software” for a Transient Cyber Asset when it’s changed as a result of executing Part 4.6. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. This removed the concept of base-lines from the requirements.

Exelon Companies and Hydro One suggested to consider incorporating R4.6 into R4.1 and requested rewording of Requirement R4, Part 4.6. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities.

Part 4.7 - Patching

Southwest Power Pool Regional Entity, Tennessee Valley Authority, Edison Electric Institute, NiSource, Large Public Power Council, American Electric Power, MidAmerican Energy Company stated that CIP-010-2, Part 4.7 should require the transient device to be fully patched and not permit an alternative mitigation plan. The commenters suggested that clarification is needed that any mitigation of a vulnerability must be completed prior to use of the asset. Lastly, the commenters suggested that the requirement should clearly note that mitigation of a vulnerability is permitted in lieu of applying a patch, when justified. In response, the SDT states that there may be instances where patching the device is not permitted or advised. Therefore, the option to create a plan to mitigate the specific vulnerability addressed by the patch would be appropriate. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities.

Tampa Electric Co., Florida Municipal Power Authority, Large Public Power Council, Southern Company: Southern Company Services, Inc.; Alabama Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing, Exelon Companies, and ISO/RTO SRC sought clarification as to whether the entity can evaluate and apply the patches monthly and not have to evaluate prior to each use. The commenters also had concerns with the need to track both the 35-day update timeframe and each use to be able to show performance to the requirement part, that the 35-day update requirement is more aggressive than for CIP-007, R2.2 and R2.3 that allow 35 days to evaluate and 35 days to install, and whether a single evaluation within 35 days prior to use would be sufficient to comply with the requirement. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard including provisions for mitigation of vulnerabilities. The attachment addresses assets owned by the entity, as well as those owned by vendors and contractors. The attachment also allows for the entity to perform activities either in a managed program state or through on demand activities.

Other

CenterPoint Energy, Kansas City Power & Light, and Southern California Edison Company commented that the administrative burden associated with Transient Cyber Assets and Removable Media is exceptionally challenging or even unattainable, and is not aligned with the risk introduced to the BES. In response, the tables supporting CIP-010-2 Requirement R4, have been removed since the initial posting. The requirement obligates the entity to create and implement plans for Transient Cyber Assets and Removable Media. The measure supports this requirement. Clarification of many topics has been added to the guidance.

Pacific Gas & Electric recommended language changes to require a security policy for transient devices. In response, the SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan elements are addressed in Attachment 1 of the standard.

Bonneville Power Administration and Pacific Gas & Electric commented that the use of direct remote access should be prohibited and to consider an implementation of a method which allows vendors to perform their work without directly accessing systems. In response, the SDT states that any vendor connecting to a BES Cyber System remotely is subject to Interactive Remote Access requirements. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization.

Bonneville Power Administration suggested that the proposed requirement language should also address assets containing low impact BES Cyber Systems. In response, due to the wide-area impact of the high and medium impact assets, the SDT limited the requirements to these assets. This includes protection from lower impact assets.

Exelon Companies commented that the sentence in the rationale referencing the relative rigor should be removed. In response, the SDT notes that the sentence has been removed.

Southwest Power Pool Regional Transmission Organization, Hydro One, and Tri-State G&T, for CIP-004 Requirement R2, Part 2.1.9, suggested deleting the word "including" as neither TCAs nor Removable Media are Cyber Assets and also suggested removing the word "with." In response, the SDT notes Transient Cyber Assets are Cyber Assets. The requirement is to address the interconnection of Cyber Assets, which includes Transient Cyber Assets. The requirement is also to address the interconnection with Removable Media, which is not a Cyber Asset.

Bonneville Power Administration, Network & Security Technologies, MidAmerican Energy Company, Exelon Companies, and Luminant Energy Company, LLC commented that 1) the requirements should focus on transient devices at the time of connection; 2) the meaning of "use" and "prior to use" is ambiguous; and 3) there are concerns with having to track each and every use of the transient device. In response, the SDT notes that the requirement for Transient Cyber Assets and Removable Media is included in CIP-010 to allow entities to align their recordkeeping of the devices to the change management activities being supported. The SDT modified the requirement to obligate the entity to create and implement plans for Transient Cyber Assets and Removable Media. The plan approach allows the entity the flexibility to define the program and controls that are most appropriate to its organization. The plan elements are addressed in Attachment 1 of the standard and are focused on addressing security vulnerabilities and malicious code protections.

Question 4: Definitions

4. *The SDT proposed new definitions for Transient Cyber Assets and Removable Media and revised definitions for BES Cyber Asset and Protected Cyber Assets. Do you agree with the new and revised definition? If not, please offer suggested revisions.*

BES Cyber Asset

Edison Electric Institute, NiSource, We Energies, PNM Resources Resources, and Oncor commented that the BES Cyber Asset definition is inaccurately quoted in the Guidelines and Technical basis in CIP-002-5.1. The SDT appreciates the comments but is not revising CIP-002-5.1 at this time. The scope of the SDT's Standard Authorization Request is focused mainly on the directives contained in FERC Order No. 791. Therefore, the SDT revised only those standards that should include language addressing the directives.

Nevada Energy suggested the SDT revise the guidance regarding BES Cyber Asset because it seems that devices whose loss could preclude a BES Reliability Operating Services (BROS) would be a BES Cyber Asset. The SDT appreciates the comments. The proposal to revise CIP-002-5.1 guidance is out of the defined Standards Authorization Request for this SDT, but we submit additional context in which the BES Cyber Asset and guidance language was drafted in CIP-002-5.1. The BES reliability operating services are provided in guidance to assist entities with a more granular description of adverse impact to the BES. For CIP Version 5, the more generic definition and specific guidance struck a balance with industry comments to provide enough granularity but still allow flexibility in the Requirement language.

Dominion and ISO/RTO SRC suggested moving the clarification on Transient Cyber Assets into that definition rather than keeping it in the BES Cyber Asset definition. The SDT removed the last sentence regarding Transient Cyber Assets from the BES Cyber Asset definition.

Protected Cyber Asset

Dominion and ISO/RTO SRC suggested moving the clarification on Transient Cyber Assets into that definition rather than keeping it in the Protected Cyber Asset definition. The SDT removed the last sentence regarding Transient Cyber Assets from the Protected Cyber Asset definition.

Transient Cyber Asset

Tennessee Valley Authority requested clarification on what "directly connected" means and if it includes specific media types. The SDT clarifies that "directly connected" means that there is nothing in between the Transient Cyber Asset and the Cyber Asset or network to which it is connected.

Southwest Power Pool Regional Entity commented that the Transient Cyber Asset definition is broad so that entities could disconnect assets categorized as BES Cyber Assets and Protected Cyber Assets as Transient Cyber Assets. ISO/RTO SRC questioned what would happen to a Transient Cyber Asset that has been connected longer than 30 days. The SDT considers any device connected for more than 30 days to be part of the BES Cyber System.

Kansas City Power & Light and Hydro One commented that the Transient Cyber Asset definition needs clarification regarding electronic access control and physical access control. The SDT has chosen to focus the requirements to the assets that are to be connected to the BES Cyber Systems that provide BES reliability operating services, as well as those residing within the same ESP. The goal is to protect the systems that can have a direct impact on real-time operations.

Massachusetts Municipal Wholesale Electric Company commented that the Transient Cyber Asset definition should not include examples. The SDT appreciates the comment. The SDT notes that other glossary terms use examples in the definitions. The SDT determined that the examples add clarity to assist the Responsible Entity in determining the scope and breadth of the term.

National Rural Electric Cooperative Association and Associated Electric Cooperative, Inc. commented that the Transient Cyber Asset definition is broad because directly connected could apply to any programmable device. The SDT added a clarification to the definition to indicate that Transient Cyber Assets are those devices "capable of transmittal of executable code" to the Cyber Assets and networks listed in the definition.

Removable Media

Southwest Power Pool Regional Entity commented that the certain portable media, such as external hard drives, should not be considered Removable Media and suggested clarification in the name of the term. The SDT appreciates the comment but determined that external hard drives should be included in the Removable Media definition. The SDT reasons that any media capable of introducing malicious software to the BES Cyber System should be subject to the appropriate requirements.

Edison Electric Institute, NiSource, We Energies, PNM Resources Resources, Oncor, Empire District Electric Company, ISO/RTO SRC, Seattle City Light, Large Public Power Council, Massachusetts Municipal Wholesale Electric Company, and American Public Power Association commented that the Removable Media definition is not consistent with the Transient Cyber Asset definition because it does not clarify to what the Removable Media is connected. Duke Energy and MidAmerican Energy Company suggested adding the three items listed in the Transient Cyber Asset definition as well as "directly connected" to the Removable Media definition. The SDT added "directly" in front of connected in the Removable Media definition and revised it to indicate that the device is "capable of the transmittal of executable code to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset," which is similar to the Transient Cyber Asset definition. This makes the definitions consistent and gives clarity on the device's connection.

Seattle City Light, Large Public Power Council, Massachusetts Municipal Wholesale Electric Company, and American Public Power Association suggested that the SDT remove "portable media" from the definition because it may add confusion. Large Public Power Council and American Public Power Association suggested adding "capable of removal without powering down the system." The SDT removed "portable" from the definition and added "capable of the transmittal of executable code" to the definition.

Southern Company and Oncor suggested that the Removable Media definition be more specific to higher risk forms of media and other diagnostic devices. The SDT reasons that any media capable of introducing malicious software to BES Cyber Systems should be subject to the appropriate requirements. Each type of Removable Media has an element of risk and should be reviewed.

Southern Company and Oncor commented that the Removable Media definition states that a Cyber Asset is not Removable Media but that the Transient Cyber Asset definition does not explicitly exclude Removable Media. The SDT appreciates the comment but notes that because a Transient Cyber Asset is a Cyber Asset, Removable Media cannot be a Transient Cyber Asset because it is not a Cyber Asset.

Kansas City Power & Light commented that the Removable Media definition needs clarification regarding electronic access control and physical access control. The SDT has chosen to focus the requirements to the assets that are to be connected to the BES Cyber Systems that provide BES reliability operating services, as well as those residing within the same ESP. The goal is to protect the systems that can have a direct impact on real-time operations.

ISO/RTO SRC commented that the SDT should include tape as an example of Removable Media. The SDT considered the addition of tape as an example of Removable Media; however, determined that tape systems are not traditionally connected directly to BES Cyber Systems.

ISO/RTO SRC commented that the SDT should clarify if "A Cyber Asset is not Removable Media" is trying to say that Removable Media are not a Cyber Assets. The SDT revised the language to read "Removable Media are not Cyber Assets."

ISO/RTO SRC questioned whether Removable Media need to comply with additional requirements once they have been connected longer than 30 days. The SDT considers any portable media connected for more than 30 days to be part of the BES Cyber System.

American Electric Power requested clarity on why Transient Cyber Assets are associated with Removable Media in the standard. The SDT moved the language in the requirements to an attachment and separated the elements applicable to Transient Cyber Assets from those elements applicable to Removable Media.

Other

PacifiCorp, South Carolina E&G, Georgia Transmission Corporation, National Rural Electric Cooperative Association, and Pacific Gas & Electric suggested the SDT revise CIP-010-2, Requirement R4.

PacifiCorp recommended that the SDT revise the applicability columns in CIP-010-2, Requirement R4, Table 1 to include Transient Cyber Assets and Removable Media. The tables supporting CIP-010-2 Requirement R4, have been eliminated and the elements of a plan for Transient Cyber Assets and Removable Media has been moved to an attachment.

PacifiCorp, Georgia Transmission Corporation, National Rural Electric Cooperative Association, and South Carolina Electric & Gas commented that part 4.1 would be administratively burdensome. The SDT agrees and has modified its approach in CIP-010-2.

Georgia Transmission Corporation commented that the SDT should not borrow from medium impact requirements for transient devices. The SDT agrees and has modified its approach in CIP-010-2.

South Carolina SG&E commented that personnel with high and medium impact BES Cyber Systems access should not need additional authorizations and that entities should be able to designate personnel who can supervise unauthorized maintenance personnel (similar to NIST 800-53 MA-5). The SDT clarifies that users may be authorized by group in the plan(s) for Transient Cyber Assets and Removable Media. Therefore, an entity may choose to list an authorized user group as those that already have been authorized for access to high and medium impact BES Cyber Systems.

Pacific Gas & Electric commented that Requirement R4 should be required across all components within the ESP regardless of classification. In response, the SDT maintains that the requirements are targeting those BES Cyber Systems that have a direct impact on the BES.

Pacific Gas & Electric commented that user authorization should be by individual and not by group. The SDT appreciates the comment but notes that it is important to give entities the flexibility to capture authorization by group. For example, an entity may choose to list an authorized user group as those that already have been authorized for access to high and medium impact BES Cyber Systems. This eliminates redundancy of individual user authorization but ensures entities designate users of entity-owned or managed Transient Cyber Assets.

ACES commented that it is supportive of the revisions as long as RAI is fully implemented by the effective date. The SDT refers ACES to the question 5 comment response.

MRO NERC Standards Review Forum commented that CIP-002-5.1 should be updated with the new and revised definitions. The SDT appreciates the comments but is not revising CIP-002-5.1 at this time. The scope of the SDT's Standards Authorization Request (SAR) is focused on the directives contained in FERC Order No. 791. Therefore, the SDT revised only those standards that should include language addressing the directives.

Question 5: Identify, Assess, and Correct

5. *The SDT removed the Identify, Assess, and Correct (IAC) language from 17 requirements to meet the directive in FERC Order No. 791 to remove or modify the IAC language. Do you support this revision approach? If not, why not and what alternative approach do you recommend?*

Support Removal

Dominion, Bonneville Power Administration, Public Service Enterprise Group; MidAmerican Energy Company, CenterPoint Energy, ACES Members, MRO NERC Standards Review Forum, Edison Electric Institute; Seattle City Light, Peak Reliability, Florida Municipal Power Authority, Large Public Power Council, Southern Company, NiSource, IESO, Southern California Edison Company, Tacoma Public Utilities, PNM Resources Resources, Kansas City Power & Light, Exelon Companies, American Public Power Association, National Rural Electric Cooperative Association, Oncor, The Empire District Electric Company, and Southwest Power Pool Regional Transmission Organization supported the removal of the IAC language. In response, the SDT thanks those entities for their comments.

Oppose IAC Removal

Portland General Electric, Nebraska Public Power District, City of Tallahassee, Tri-State G & T, and Idaho Power commented that the inclusion of this language in the CIP Version 5 standards was a large part of the reason that the industry voted to pass the standards in the first place and that the directive allowed for a modification of the IAC language. The SDT appreciates the concerns raised with the removal of IAC. However, the majority of stakeholders indicated a preference in removing the IAC language to address the FERC directive. NERC continues to develop Reliability Assurance Initiative (RAI) to address the compliance concerns that IAC sought to address. The comments opposing the removal of IAC and the underlying compliance concerns that remain are being forward to NERC Compliance.

Modify IAC/Standard Language

Dominion commented that an alternative approach to RAI would be to address FERC's concerns by modifying the individual Parts of each of the CIP Requirements. The SDT appreciates the suggestions to modify the IAC language to meet the FERC Directive. However, the majority of stakeholders indicated a preference in removing the IAC language to address the FERC directive.

Southwest Power Pool Regional Entity suggested that a performance metric could be developed that allowed for an infrequent (frequency to be defined) occurrence as long as the entity's detective controls detected the unauthorized implementation activity within a to-be defined detection period (perhaps 24 hours) and the unauthorized change was promptly investigated. In response, the Cyber Security Order 706 SDT previously explored incorporating performance metrics into the requirements, but the approach proved problematic by triggering a new host of questions related to the metric. As a consequence, the requirement lost focus on the real intent of the security measure. The IAC language attempted to balance the security objective with reasonable compliance expectations. At present, NERC continues to develop RAI to address the compliance concerns that IAC sought to address. The comments received on IAC are being forwarded to NERC Compliance. Performance or qualitative metrics may have a useful role under the RAI program whether as part of a risk assessment methodology or other element.

Portland General Electric commented that it would be worthwhile to modify the language to add a qualitative aspect to address zero tolerance concerns, and Occidental Chemical Corporation suggested to encode the IAC concept into separate sub-requirements under each of the affected requirements. The SDT appreciates the

comments on including a qualitative aspect and IAC in a different structure in the language. During development, the SDT explored options in the requirement language to address the zero defect concern rather than just removal of IAC. Ultimately, the SDT determined that this additional language did not provide clarity on performance obligations in the requirement and did not address zero tolerance concerns. The SDT noted that NERC continues to develop RAI to address the compliance concerns that IAC sought to address. The comments opposing the removal of IAC and the underlying compliance concerns that remain are being forward to NERC Compliance.

Liberty Electric System commented that, at a minimum, the VSLs and Measures should be rewritten to allow for minor instances of errors. For example, instead of a single instance of failing to revoke access for a transfer, rewrite the requirement to require a process that assures the access is revoked, with a low violation if the process fails to keep instances under 5% annually, or less than two in cases where there are small numbers of transfers each year. Tampa Electric Co. expressed a similar comment to modify the VSLs for a future revision. In response, the SDT notes that VSLs define the degree to which compliance with a requirement was not achieved. The SDT states that RAI is the appropriate mechanism to address the zero tolerance concern.

Idaho Power stated that more work should be done to see if there is a way to fix the IAC language prior to it be discarded. In response, the SDT is supportive of the removal of the language as the IAC paradigm will be addressed in RAI.

Tri-State G&T suggested defining IAC as one defined term instead of three separate words. The entity further commented to change “deficiencies” to “possible violations.” In response, the CMEP program, from the auditing and enforcing perspective, handles possible violations and it is not appropriate for reference to violations to reside within the Requirement language itself.

Clarify RAI and Compliance

Pacific Gas & Electric commented that defining clearer requirements, scope definitions and obligations in the NERC Compliance Monitoring and Enforcement Program. In response, the comments relative to RAI and other compliance concerns are being forwarded to NERC. The SDT will emphasize the concerns about RAI implementation timing.

Tennessee Valley Authority requested clarity on the RAI process regarding reporting timeframe and definition of “minimal risk.” In response, NERC notes that assessment of risk is based on facts and circumstances. For a more detailed explanation of assessing risk and the factors to consider in the assessment, NERC encourages entities to refer to the Self-Report User Guide, located here. Also, NERC has posted more than 1,100 minimal risk CIP FFTs on its webpage to provide Registered Entities with information on what constitutes minimal risk and how to mitigate minimal risk noncompliance.

Bonneville Power Administration commented that a lack of clearly defined measures results in inconsistent audit approaches and findings. In response, NERC notes that NERC and the Regional Entities have developed the ERO Enterprise Compliance Auditor Manual and Handbook and the ERO Auditor Checklist to define techniques, tools, and methods to perform compliance monitoring in a consistent manner. The ERO Enterprise is hosting training webinars prior to full implementation in the fourth quarter of 2014.

Idaho Power stated that industry is left with no time frames or guarantees of what RAI will become or when it is implemented. Nebraska Public Power District stated that RAI is an enforcement mechanism and not a compliance action. In response, NERC notes that several RAI projects have begun implementation in 2014, including the user guides, triage process, compliance exceptions, and aggregation of minimal risk issues programs. Development of the compliance monitoring-related programs is underway for implementation in 2015. The lessons learned from the development and early implementation of these programs will inform a filing to FERC in the fourth quarter of 2014. A current timeline and description of RAI activities is available on the RAI webpage, located here. The

aggregation of minimal risk issues and compliance exceptions are the two programs most relevant to these Standards. With aggregation, select Registered Entities[2] may track their minimal risk noncompliance without having to submit a Self-Report for each failure to comply with a Requirement. Such noncompliance would presumably be treated as a compliance exception. A compliance exception is a minimal risk noncompliance that is mitigated or can be mitigated within one year. Compliance exceptions do not become Possible Violations and do not initiate an enforcement process.

Peak Reliability suggested that concrete threshold reporting criteria for certain Requirements should be set. The SDT has chosen not to set such concrete threshold reporting criteria in the Requirements.

ISO/RTO SRC asked when will industry see a specific description of the RAI program as applied to CIPv5 standard compliance enforcement and expectations of RE's for collecting evidence to support the RAI process. In response, NERC conducted a joint webinar on June 19 for both the CIP Version 5 revisions activity and the RAI program. NERC will look into conducting something similar in the future and is continuing outreach on the RAI program.

Kansas City Power & Light commented that this concept would be addressed in tools and frameworks accomplished through the RAI, however, consistency in auditor training and approach will be critical to the success of the RAI program. In response, NERC agrees with the importance of auditor training and RAI components are a crucial aspect of the ERO training now and going forward.

Clarify RAI Prior to Implementation or Final Ballot

Public Service Enterprise Group commented that it would like to have additional clarity and finalization of the RAI process prior to the implementation of the new standard language. In response, the SDT understands that RAI is one of the biggest goals of the ERO. NERC's continued outreach on RAI will help alleviate industry's concerns. ACES Members are supportive of the approach as long as RAI is fully implemented.

MidAmerican and NV Energy stated that NERC can support the SDT efforts by implementing compliance exceptions prior to the second or final ballot. In response, NERC notes that it began implementation of the compliance exceptions program as of November 2013 for select Registered Entities. Eligibility expanded to additional Registered Entities in May 2014, and compliance exception treatment will be available January 1, 2015 to all Registered Entities for minimal risk noncompliance discovered through any method.

Need to address zero tolerance

Dominion, Southwest Power Pool Regional Entity, Bonneville Power Administration; Portland General Electric, Public Service Enterprise Group, We Energies, Occidental Chemical Corporation, Liberty Electric Power LLC, Idaho Power, City of Tallahassee, NV Energy; Nebraska Public Power District, Edison Electric Institute, Florida Municipal Power Authority, Large Public Power Council, ISO/RTO SRC, Southern Company, NiSource, Tacoma Public Utilities, Xcel Energy, PNM Resources Resources, and Oncor commented that the zero tolerance issue needs to be addressed. In response, while the removal of the IAC language returns the requirements to a zero tolerance construct, NERC committed to alleviate the zero tolerance concerns through the implementation of the RAI compliance approach (see the Q4 response and others in the FAQs document). In response, the comments relative to compliance concerns will be forwarded to the NERC Compliance department.

Other

American Public Power Association encouraged the SDT to provide guidance to NERC staff on the development of the proposed RSAWs. In response, while the SDT is not part of the RSAW development team, the SDT submitted

[2] The Enforcement Activities Overview, available on the RAI webpage, contains further details on eligibility for the aggregation program.

team comments on the RSAWs posted for comment during the initial comment period. The SDT continues to engage with the RSAW development team to provide input on the RSAWs.

Question 6: Implementation Plan

6. *The Implementation Plan uses the existing effective date of the FERC approved CIP V5 Standards for CIP-003-6 Requirement R2 and provides additional time for compliance for CIP-006-6, Requirement R1, Part 1.10; CIP-007-6, Requirement R1, Part 1.2; and CIP-010-2, Requirement R4. Are the timeframes reasonable and appropriate? If not, please explain.*

CIP-003-6

Duke Energy, Nebraska Public Power District, American Public Power Association, and Bonneville Power Administration suggested a later enforcement date, specifically that the low impact requirements should be enforceable one year later (January 1, 2018). American Public Power Association suggested that the implementation plan should call out two years after FERC approval or April 1, 2017, whichever is later for compliance. In response, the SDT understands the additional specification for Requirements applying to low impact BES Cyber Systems requires additional resources for implementation. In weighing the specificity with the already approved deadline of April 1, 2017, the SDT proposes an implementation plan which considers both the effort of implementation and the general impact to the BES. Requirements that entities can implement organizationally retain the same date of April 1, 2017. These Requirements include cyber security policy, awareness, and incident response plan. The physical and electronic access Requirements have obligations which generally necessitate deployment of technical controls. For these, we have graduated the implementation based on the technical controls. This approach balances the objective to implement on a similar schedule as CIP-003-5 with the additional effort to meet the new specific Requirements.

Similar to the comments above, Exelon Companies commented that the implementation plan should allow at least a year from the effective date of CIP-003-6. The Implementation Plan should make it clear that CIP-003-6, Requirement R2 will replace CIP-003-5 Requirement R2. In response, in addition to the SDT's response above, CIP-003-5 is retired with the implementation of CIP-003-6 and the Requirement applying to low impact BES Cyber Systems will be replaced as suggested.

CIP-006-6/CIP-007-6

Southwest Power Pool Regional Entity commented that the implementation plan for CIP-006-6, Requirement R1, Part 1.10 should be consistent with the actual Version 3 expectation and that additional time is not needed for CIP-007-6 Requirement R1, Part 1.2. In response, the Implementation Plan for CIP-006-6 Requirement Part 1.10 does consider the version 3 expectation and only provides additional time "for new high or medium impact BES Cyber Systems at Control Centers identified by CIP-002-5.1 which were not identified as Critical Cyber Assets in CIP Version 3". Regarding CIP-007-6, the additional 9 months may be necessary depending on how entities disable physical ports. This is an additional effort on top of what is necessary to implement version 5. For large control centers, this may require additional inventory work to ensure nonprogrammable components meet this Requirement.

Southwest Power Pool Regional Transmission Organization recommended that the six-month window for CIP-007-6 R1, Part 1.2 be extended to a nine-month window, reducing the number of dates and outlying requirements. In response, the additional requirements in CIP-006-6 and CIP-007-6 now have the same additional 9 months for compliance.

CIP-010-2

CenterPoint Energy stated that the timeframe for CIP-010-2 Requirement R4 is not appropriate, and recommended that Registered Entities not be required to comply with Reliability Standard CIP-010-2,

Requirement R4 until at least one year after the effective date of Reliability Standard CIP-010-2. In response, the SDT notes that the implementation period for CIP-010-2 Requirement R4 calls for nine calendar months after the effective date of CIP-010-2 which allows entities enough time to prepare for compliance based on SDT discussion of all the implementation compliance dates for modified requirements.

Southwest Power Pool Regional Entity commented that CIP-010-2 Requirement R4 does not need nine additional months. In response, this Requirement has been modified and the additional time is necessary for entities to develop and implement their plan(s) to address transient devices.

Overall Implementation

Colorado Springs Utilities, Tennessee Valley Authority, Western Area Power Administration, and Salt River Project recommended changing the Implementation Plan time schedule to fall after the CIP Version 5 standards implementation dates. In response, the SDT states that the implementation plan is drafted to account for the Version 5 Standards as suggested. The Version 5 effective dates are used as the minimum bound for Version 5 Revisions. This ensures a seamless transition across versions on April 1, 2016 and April 1, 2017. Additional time beyond the version 5 effective dates is given for all but the Requirements in which the IAC language was removed. The IAC removal does not provide any additional obligations to Responsible Entities.

City of Tallahassee commented that FERC should issue an order to extend the effective date at least another full six months for each standard/requirement for which a modification to the language was made. In response, additional time beyond the version 5 effective dates is given for all but the Requirements in which the IAC language was removed. The IAC removal does not provide any additional obligations to Responsible Entities.

Exelon Companies commented that the Implementation plan uses “months” and “calendar months” and requested clarity whether there is a difference between the two terms and, if no difference is intended, suggested to use one for consistency. In response, the SDT has modified the Implementation Plan to address this inconsistency.

National Rural Electric Cooperative Association commented that not balloting the Implementation Plan separately was a violation of the Standards Processes Manual (SPM). In response, in section 4.4.3 of the SPM, “The implementation plan is posted with the associated Reliability Standard or Standards during the 45 (calendar) day formal comment period and is balloted with the associated Reliability Standard.” Therefore, the implementation plan was included as a component of the Reliability Standard comment period and ballot.

National Rural Electric Cooperative Association also requested that the SDT consider using the same additional time for compliance for all revised or new requirements under the current CIP V5 revision project. In response, the additional requirements in CIP-006-6 and CIP-007-6 now have the same additional nine months for compliance. The SDT has modified the Implementation Plan for low impact Requirements in response to other commenters.

Arkansas Electric Cooperative Corporation expressed support for addressing all four directive areas in the one-year timeframe. Arkansas Electric Cooperative Corporation went on to further comment that it is important to have industry-developed objective criteria for the low impact BES Cyber Systems when the requirements go into effect on April 1, 2017. The industry begins its 7th year in which these standards have been in development. It is difficult to grow and mature security programs with so much change in the compliance rules. Arkansas Electric Cooperative Corporation stated they hope the industry, NERC, and FERC can come to an agreement in the coming months and provide finality to these Reliability Standards for a time. The SDT thanks you for your comments.

Question 7: Canadian or Other Regulatory Requirements

7. *Are there any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.*

There were no commenters who responded to this question identifying any jurisdictional specific regulatory requirements.

Question 8: Other Areas Within SAR

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

Low Impact

Tennessee Valley Authority requested clarification on the threshold for the low impact categorization and whether the BES definition establishes the lower boundary. In response, the Applicability section and Attachment 1, Section 3 of CIP-002-5.1 establishes the lower boundary, and while the BES definition is a basis for the lower boundary, it does not always establish it. The use of Facilities in the Applicability section ties back to the BES definition, but it is possible to have systems or equipment, such as Control Centers and systems or those critical to system restoration.

Southwest Power Pool Regional Transmission Organization sought clarification on the security awareness component of CIP-003-6. South Feather Power Project and Seattle City Light commented that the security awareness requirement should be annual instead of quarterly. The SDT has modified the language to "at least once every 15 calendar months" from "quarterly." In addition, the SDT removed the training component from CIP-003-6 because training is addressed in CIP-004-6.

Seattle City Light also suggested that the SDT change the presentation of the low impact controls, either by dispersing them throughout the other standards or creating a CIP-012-1. The SDT considered dispersing the low impact controls throughout the CIP standards but determined that they could not fit into the table format because the medium and high impact controls apply at the system level whereas the low impact controls apply at the asset containing low impact BES Cyber System level. The SDT also considered drafting CIP-012-1 to include low impact requirements. However, the SDT determined that it was more appropriate to keep the low impact policy requirement in CIP-003-6 because the policy requirements for high and medium impact were located there as well. To address comments on reorganizing low impact requirements, the SDT determined that it would put the low impact technical requirements into an attachment to CIP-003-6, Requirement R2, which requires a plan to address the elements in the attachment. In addition, the SDT placed the low impact policy requirement into CIP-003-6, Requirement R1 to consolidate the policy requirements for low, medium, and high impact into one requirement.

MidAmerican Energy Company also suggested adding "for its assets identified in CIP-002-5.1" into Requirement R2 to clarify the assets to which it applies. The SDT added "Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems" into Requirement R2 to clarify applicability.

Rayburn Country Electric Cooperative and Wisconsin Electric Power Company suggested the SDT develop guidance in CIP-003-6 to address compliance concerns. In response Rayburn County Electric Cooperative, see the comment response summary for Question 1. The SDT has provided more specific examples and guidance to the Requirement applying to low impact BES Cyber Systems. In response to Wisconsin Electric Power Company's concern that entities cannot go beyond the Requirement objective, the NERC Reliability Standards should not contain language about compliance and notes that the language included in the background sections of these standards may be inappropriate to include. The SDT may revisit the background sections of the standards at a later date.

American Public Power Association commented on compliance concerns and suggested a survey of entities to determine the administrative workload for the low impact requirements. In response, the SDT notes that NERC

will consider the need for a survey. If you have any information on this topic that would assist NERC, please submit them in your comments.

Exelon Companies and National Rural Electric Cooperative Association expressed support of getting the low impact requirements to a steady-state. The SDT continues to develop revisions to the low impact requirements in an effort to build consensus and gain approval prior to the February 3, 2015 FERC filing.

Revise CIP-002-5.1, CIP-005-5, and CIP-008-5

Edison Electric Institute, Tampa Electric Company, NiSource, and Nevada Energy suggested the SDT make conforming changes to CIP-002-5.1, CIP-005-5, and CIP-008-8 to maintain consistency throughout the CIP suite of standards. Southwest Power Pool Regional Entity submitted errata changes to the Guidelines and Technical Basis section of CIP-002-5.1. ISO/RTO SRC and Entergy recommended making all CIP standards version 6. Manitoba Hydro and Duke Energy suggested changing the effective dates of the Version 5 standards to make all consistent. Southern Company and Georgia Transmission Corporation requested clarification of "associated with" in CIP-002-5.1. Wisconsin Electric Power Company commented that Criterion 2.3 of CIP-002-5.1 Attachment 1 is not specific enough as to which BES Cyber Assets meet the criterion and recommended that CI-002-5.1, CIP-005-5, and CIP-008-5 clarify in guidance that those entities going above and beyond the requirements would not incur additional compliance obligations. Massachusetts Municipal Wholesale Electric Company suggested revising CIP-005-5 and CIP-008-5 to reference low impact BES Cyber Systems.

The SDT appreciates the comments regarding revisions to CIP-002-5.1, CIP-005-5, and CIP-008-5. At this time the SDT continues to focus on the four main directive areas from Order No. 791. As a result, the SDT will not revise CIP-002-5.1, CIP-005-5, and CIP-008-5 during this phase of development.

Reliability Standard Audit Worksheets (RSAWs)

Florida Municipal Power Agency (Florida Municipal Power Authority) requested that NERC run non-binding polls and post comments received on the RSAWs. Edison Electric Institute, Florida Municipal Power Authority, and First Energy commented that the CIP-002-5.1 RSAW expands beyond the scope of the standard. Florida Municipal Power Authority noted that the CIP-003 RSAW has the wrong number in 6a of Requirement 2.5. Edison Electric Institute and FirstEnergy emphasized that the SDT and the RSAW development team should continue coordination during the standards development. Exelon Companies commented that the RSAWs do not provide relief from zero tolerance concerns and suggested the RSAWs be revised and posted for industry comment during the next revisions to the standards.

The SDT coordinated with the RSAW development team during drafting activities and will continue this coordination for the next revisions. As part of this collaboration, the SDT will pass the comments received on the RSAWs to the RSAW development team.

Reliability Assurance Initiative (RAI)

Northeast Power Coordinating Council (Northeast Power Coordinating Council), Exelon Companies, and National Rural Electric Cooperative Association requested more scenarios as to how CIP requirements will work in the RAI context and suggested using the low impact or "identify, assess, and correct" (IAC) requirements to demonstrate RAI concepts. Avista and National Rural Electric Cooperative Association commented that RAI should be finalized prior to final ballot.

The SDT appreciates the comments regarding RAI and recognizes the relationship between the removal of IAC language and RAI. The SDT continues its coordination with NERC staff on RAI and will pass on these and other relevant comments to NERC staff involved in the development of RAI.

Other Comments

Northeast Power Coordinating Council and Hydro One commented that the SDT should be able to help clarify issues discovered during the CIP Version 5 Implementation Study, particularly on the transfer trip issue, programmable devices definition, and clarification on "effect within 15 minutes." The SDT appreciates these comments but continues to focus effort on the four main directive areas from FERC Order 791. NERC has employed an industry stakeholder group to review and provide guidance toward these issues outside of the standards setting process.

Northeast Power Coordinating Council and Hydro One suggested adding "or" to CIP-010-2, Requirement R4, Part 4.1.4 to make it consistent with Requirement R1, Part 1.1.1. The SDT proposes to revise Requirement R4 to have an attachment with the elements related to transient devices.

Pacific Gas & Electric requested guidance on how Electro Magnetic Pulse (EMP) anomalies should be considered in risk assessments or policies and procedures, and in response, the SDT notes the CIP Cyber Security Standards have the objective of protecting BES Cyber Systems against cyber security risks. EMP and other related threats associated with the BES and BES Cyber Systems are outside the scope of this SDT.

Southwest Power Pool Regional Entity commented that there is an inconsistency in the implementation plan for CIP-004-6 because six months is allowed if government authority is required and only three months is allowed if government authority is not required. In response, this has been corrected to allow three calendar months after approval by a government authority.

PacifiCorp agrees with the communication networks revisions and does not recommend further edits. The SDT appreciates the comment and PacifiCorp's support of the revisions.

Dynegy requested that the webinars on the SDT's revisions and on RAI be posted to the website. The SDT's webinar and slides may be found here and here. The RAI webinar and slides may be found here and here.

Western Area Power Administration requested clarity on the object of the standards and align them with the risk to the BES so auditors and entities have a consistent approach. The SDT appreciates these comments but notes the rapidly changing and variant cyber security risk profile across the BES make this approach particularly unsuitable for Reliability Standards development. The approach is to develop standards for cyber security controls that address a wide set of common cyber security vulnerabilities.

Manitoba Hydro noted that the Compliance Enforcement Authority (CEA) definition is incorrect in Section C1.1 of the standards because Public Utility Board is its CEA. In response, the purpose of the compliance section of the standard is to describe the CEA's activities. If a province in Canada is not subject to the ROP provisions related to the CMEP and has its own enforcement, then these provisions simply would not apply.

Exelon Companies requested more guidance language be developed to support the requirements. The SDT appreciates the comment and will draft guidance language to support the proposed Requirements and additional revisions.

Texas Reliability Entity commented that entities should be required to demonstrate evidence of the effective execution of controls and not just that they have a policy or procedure. The SDT appreciates the comment and notes that the "implement" term in the requirements means that entities should execute the performance requirements and provide documentation of the implementation.