NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments Cyber Security Order 706 Version 5 CIP Standards

Comment Form
Combined Question 1 and Question 2 Summaries
October 26, 2012

The Project 2008-06 Drafting Team thanks all commenters who submitted comments on the Version 5 of the CIP Cyber Security Standards and its Implementation Plan for consideration by the SDT in finalizing Version 5 and related documents. The 10 standards were posted for a 30-day formal comment period from September 11, 2012 through October 10, 2012 and successive ballots through October 10, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 112 sets of comments, including comments from approximately 258 different people from approximately 153 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's 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, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

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

Table of Contents

Introduction

The Standard Drafting Team (SDT) thanks all commenters for their continued focus on providing constructive and useful feedback for improving and refining the standards. In response to draft 3 of the Version 5 CIP Cyber Security Standards, the SDT received input that was focused on several issues that assisted the SDT in refining the standards to the final set of standards now posted for recirculation ballot. The SDT carefully considered all comments in determining whether to make particular changes to the standards.

In response to comments provided to draft 3, the drafting team greatly appreciates those entities that focused their comments on the issues most critical to them, as it facilitated a qualitative representative assessment of the areas requiring the greatest review. The focus on those major concerns that were essential as a condition to find consensus was greatly appreciated.

Furthermore, the SDT wishes to thank the industry for their significant engagement and support in developing these standards. Industry participants and observers, whether formally or informally, and whether in person or through other means, provided important perspectives and subject matter expertise that facilitated the SDT's consideration of the complicated issues and technical matters reflected in these standards. This truly was a collaborative process with participation from virtually every facet of our diverse and committed industry. Security and reliability were reflected in each consideration, and the extensive and consistent industry participation throughout the process is reflected in high approvals in response to the successive ballot from draft 3 that ended October 10, 2012.

At this stage, the drafting team has reached a point where it has made a good faith effort at resolving applicable objections, and it has not made any substantive changes since posting draft 3. Therefore, the team is posting the standards, related definitions and implementation plan for a recirculation ballot. As in past drafts of the Version 5 CIP Cyber Security Standards, the SDT thoroughly considered proposed changes and evaluated them carefully by considering several important variables, such as, but not limited to, whether such changes were in the interest of cyber security and reliability, whether they would improve or reduce consensus, whether they had unintended consequences for other types of entities, and whether they were in support of the SDT's obligation to respond to regulatory directives, most notably from FERC Order No. 706. The SDT has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestion and also recognizing the considerable diversity of entities and assets to which the standards will apply.

In the accompanying comment form for draft 3, the drafting team asked the following two questions:

1. If, after reviewing the posted standards and General Summary of Consideration of Comments, you do not support one or more of the 10 standards, the implementation plan or set of definitions, please indicate the specific item you do not support (the standard and Requirement number, specific defined term, or implementation plan) and the specific reason you cannot support it here.
2. If you have a brief comment you would like to provide that has not already been provided among the previously submitted feedback in response to draft 1 and draft 2, please provide it here. Please limit your comment to 200 words or less.

In reviewing comments, the SDT determined that some common issues were presented by different entities in response to either Question 1 or Question 2, depending on how the particular entity organized its comments. As a whole, the SDT found that the responses were thoughtful, organized, and focused. In this summary, the SDT is responding to all comments from industry that were submitted in response to both Question 1 and Question 2 in one consolidated summary form rather than providing a separate summary for each of Question 1 and Question 2. Since most issues and comments were not isolated in response to one question or the other, this single summary provides the most efficient and thorough method with which to provide the SDT's response.

Commenters addressed a wide variety of topics in their comments, but the most commented upon subjects include comments on the Transmission Operator (TOP) Control Center Criterion in CIP-002-5's Attachment 1 and comments regarding the SDT's use of the "in a manner that identifies, assesses, and corrects deficiencies" language. The TOP topic is discussed in detail under the CIP-002-5 portion of this summary, and the "identifies, assesses, and corrects deficiencies" topic is addressed immediately below as part of this summary's general discussion. Other topics are discussed relative to their particular standard or definition, and the associated table of contents for this document lists most topics of discussion.

"Identifies, Assesses, and Corrects Deficiencies" Comments

As noted in the background sections of the standards, and in response to comments from draft 2, the SDT has incorporated within CIP Version 5 a recognition that certain Requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain Requirements. The intent is to change the basis of a violation in those Requirements so that they are not focused on *whether* there is a

deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. For purposes of this summary, the "identifies, assesses, and corrects deficiencies" phrase is sometimes referenced as simply "IAC."

This topic was a source of several comments on draft 3, and the SDT appreciates the comments, feedback, and the spectrum of concern or support on this issue. The SDT believes that Version 5 is the right time to take a step in a direction that promotes security and reliability by incorporating a self-correcting aspect in certain Requirements. This is a new step, but it is informed, collectively, by implementation and audit experience from Versions 1 through 3 of the CIP Cyber Security Standards.

Many commenters support the SDT's addition of a self-correcting aspect and applaud the overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. The commenters support the shift from zero tolerance for deficiencies to encouraging finding and correcting deficiencies. The SDT considers such self-correction as an essential component to improved reliability and security, and it thanks commenters for their support. Though there were several specific suggestions or concerns, as noted below, the consensus position of the industry is one of support for the approach, as reflected in both comments and the overwhelming approval of the standards that use the approach.

While this is a new direction, the SDT believes there is tremendous benefit in eliminating the zero-defect language in the standards, and it is therefore worthwhile of inclusion in the CIP standards. However, the SDT acknowledges this is a developing concept and encourages the industry to continue to work alongside NERC in implementing the compliance monitoring strategy for the language.

Some commenters presented concern that there is no clear mechanism with how this approach will be audited or that there may be inconsistent audits across Regions. The SDT is well aware of this concern, and it is encouraged by ongoing coordination and support among both NERC and several regions. The SDT expects that NERC will continue to develop tools such as the Reliability Standard Audit Worksheets (RSAWs) in a manner that involves the industry and the members of the SDT. Importantly, the language to "identify, assess, and correct deficiencies" modifies "implement" where used, and it is meant simply to express that implementation of the Requirement is not in a "zero defect" manner.

Commenters also questioned whether this approach indeed does require internal controls. The SDT notes that the compliance initiatives that relate to internal controls are not the same as the approach in the standard. The SDT contemplates that the "identify, assess, and correct deficiencies" language is appropriate regardless of how compliance may be monitored, while noting that the standards approach is also supportive of the compliance approach where and if used. At its core, the SDT intends in using the language to signal an important transition to self-correction as part of the expected performance of a Requirement itself as opposed to a mere deficiency constituting the basis for violation.

Some commenters also proposed alternative, additional, or supporting language to augment the "identify, assess, and correct deficiencies" language in the Requirements or other supporting components of the standards, or proposed addition of the language to other requirements. The SDT has previously considered such alternative language and evaluated carefully where the language should be used, and, upon reexamining those proposals in response to comments, the SDT continues to support those concepts in the compliance monitoring approach and documents rather than in the standards themselves. Language noting that certain actions are not violations is too prescriptive for either the Requirements or the measures, and they do not comport with the style and form of the standards. With continuing input, coordination, and education, the SDT is confident that the Requirement language as presented is the appropriate mechanism to empower the industry to focus on correcting deficiencies as part of the expected performance of the Requirements while not requiring or prescribing a particular assessment of the how the entity accomplishes it.

Additionally, in response to perspectives expressed by commenters on the "identify, assess, and correct" deficiencies language, the SDT shares the view that NERC must ensure going forward that the compliance monitoring approach is consistent. The SDT believes that most of the industry is ready to transition to a new approach and that this reflects the consensus position. The SDT and the industry have an opportunity to incorporate significant improvements and lessons learned from implementation and audit of previous versions, and the SDT is encouraged by not only industry support, but also from NERC's direction in continuing to work with the industry in implementation of risk-based initiatives. The SDT will remain engaged after approval of the standards to work with NERC to provide input into the RSAW development process.

Section 4 - Applicability

There were many comments that "group of Elements" from the standards' applicability section, parts 4.1.2.4 and 4.2.1.4 should be deleted on the bases that it is redundant with Cranking Path and would create ambiguity, citing that these and initial switching Requirements are included in the Cranking Path. The SDT considered the language that is included in Requirement R1.5 of EOP-005-2, which says: "Identification of Cranking Paths and initial switching Requirements

between each Blackstart Resource and the unit(s) to be started." The addition of the term "group of Elements" is based on this Requirement that includes "and initial switching Requirements" in addition to the Cranking Path, and it is meant to include the group of Elements that is included in these initial switching Requirements.

One commenter requested clarification on the applicability of Section 4 with respect to Distribution Providers (DPs). The SDT notes that the clarification is included in the Guidelines and Technical Basis section of the standards relating to applicability. The guidance specifically says: "Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2." This means that DPs that own assets listed in 4.2 are subject to the standard. In addition, "For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above" are excluded from applicability of the CIP standards. That means that only systems and equipment listed in 4.2.1 are subject to the CIP Cyber Security standards.

Many commenters stated that the qualifications for applicable assets in section 4 for Cranking Paths unfairly includes non-BES facilities for DPs while excluding those from Transmission Owners (TOs) and TOPs, for which all BES Facilities are defined under section 4 as applicable. Alternate language was proposed to only include BES facilities in the scope for Cranking Paths. The SDT clarifies that those TOs that own BES Facilities as well as non-BES facilities that are qualified for DPs will also be registered as DPs. A review of the registry listing from September, 2012 showed that 232 of the 340 registered TOs (68%) are also registered as DPs. The SDT further points out that the inclusion of DPs in the applicability ensures that non-BES facilities, such as those that support the restoration of the BES, that are impactful to the reliability and operability of the BES are included.

One comment read that it appears that small entities that own stand-alone UFLS systems with no communication facilities would have applicable Requirements under these standards. It is the intent of the SDT to include all UFLS systems that meet the criteria defined in section 4. These criteria do not include any exclusion based on connectivity. The SDT points out that for DPs, only those UFLS systems that can automatically shed 300 MW or more under a common control system are qualified for applicability. The Requirements that are applicable based on connectivity are specified in CIP-003 through CIP-011. The commenter also stated that, "Further a small entity that is part of a larger load shedding program should maintain their program, but the entity that is responsible should be the one with the cyber security based on the common control system." The SDT clarifies that the owner of all qualified cyber systems is the entity responsible for compliance of these cyber systems: while the common control system that is capable of shedding 300 MW qualifies that UFLS, all cyber systems that impact the reliable operation of the UFLS system become in scope. The

responsibility for the compliance of each of these cyber systems to applicable Requirements belongs to the owner of that cyber system.

One commenter stated that the Functional Entities in section 4.2.1.3 and the Impact Rating Criteria in Attachment 1, section 3.6, for DPs to include facilities containing "A Protection System that applies to Transmission ..." is a new (initially introduced in draft 2) unsubstantiated Requirement for low impact assets. The SDT points out that among the tasks of the DP in the Functional Model is to "design and maintain protective relaying systems, under-frequency Load shedding systems, under-voltage Load shedding systems, and Special Protection Systems that interface with the transmission system." Further, the NERC Statement of Compliance Registry Criteria (Appendix 5B of the NERC Rules of Procedure) includes:

> "III.b.2 Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System:
>
> - a required UFLS program.
> - a required UVLS program.
> - a required Special Protection System.
> - a required transmission Protection System."

The same commenter suggested that the inclusion of all BES Facilities in section 4 is excessive. The SDT takes the position that cyber systems that impact the real-time operation of any BES Facility must be subject to some form of protection that is commensurate with its impact. The SDT points out that only those BES Cyber Systems that have a real-time impact to the BES are included by definition. This is also in consideration of comments in FERC Order No. 761.

Another commenter wrote that the use of the defined term "BES Facilities" in the applicability section would exclude such assets as Control Centers and Protection Systems. While these facilities are not BES Facilities per se, they are facilities essential to the reliable operation of the applicable BES Facilities and are included for applicability because of the function they are providing for reliable operation of BES Facilities.

One commenter stated that the clause "is subject to one or more Requirements in a NERC or Regional Reliability Standard" was unclear and proposed "can affect the reliability of either Medium or High Impact Facilities." The SDT believes that DPs have to comply with NERC Reliability Standards for some facilities they own and that the current clause

provides certainty as to what those facilities are since these DPs are required to comply with these standards. The SDT feels that the proposed language provides less certainty and is more subjective.

One commenter noted that exempting utility owned communications infrastructure (exemption of communications facilities between ESPs) creates a cyber security issue. The SDT believes that utility owned carrier services should be treated in exactly the same way a third party carrier is viewed in terms of trust, and that adequate protection measures should be taken to protect against an untrusted (from the BES Cyber System point of view) service provider.

Draft Reliability Standard Audit Worksheet

Some commenters provided input and feedback in their comments to the draft RSAW for CIP-006-5 that NERC Compliance Operations posted concurrently with draft 3 of the CIP Cyber Security Standards. The intent of the SDT in contributing to the development of a draft RSAW for CIP-006-5 was to begin the initiative of developing RSAWs in concurrence with standard development projects. The SDT provided input to the draft of the RSAW, and it is encouraged by the opportunity for the SDT and industry to continue to provide input as the RSAWs continue to be developed subsequent to the industry's approval of these standards. The SDT has forwarded these constructive inputs to NERC Compliance Operations for their continuing consideration.

"Annual" and Other Time Parameters

Some commenters pointed out that in a few instances, the SDT inadvertently continued to use the "at least once each calendar year (or similar)" language in conjunction with the convention to not exceed 15 calendar months. The SDT has reviewed the standards and eliminated those "calendar year" references where the SDT intended to use only the phrase "at least once every 15 calendar months."

A few commenters continued to suggest alternatives or expressed preference for retaining only the "annual" reference, which would result in continued reliance on CAN-0010. The SDT has not implemented that change because within Version 5 there is an opportunity and an obligation to unambiguously reference the periodic time parameter. The SDT also explained this in greater detail in response to draft 2 of the Version 5 CIP Cyber Security Standards on pages six and seven of summary consideration of comment form A.

One commenter expressed a desire to adopt a "once per month" convention instead of using, "At least once every 35 calendar days..." where that phrase is used. This is similar to the discussion on "annual," and for similar reasons, the SDT has not made the change. The SDT intends for these time periods to be repeatable on a basis that approximates

performance on the same day per month, or more frequently. The SDT believes it is reasonable to use 35 calendar days to account for those scenarios where a month may begin or end on a weekend, or for holidays.

Authorized Access List and Specific Rights Reviews in Multiple Standards

One commenter identified possible issues with a lack of understanding and inconsistent implementation for authorized access lists and specific rights review in Versions 1 through 3 of CIP-004 Requirement R4, CIP-003 Requirement R5, and CIP-007 Requirement R5. The commenter further stated that there was a concern that the quarterly and annual verification of CIP-004-5 Requirements Parts 4.2 and 4.3 are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve existing issues.

Similarly to the comment above, another commenter had issues with a lack of understanding and an inconsistent implementation for authorized access list and specifics rights review with the multiple standards as mentioned in the previous paragraph. The commenter was concerned that CIP-004-5 Requirement Parts 4.2 and 4.3 quarterly and annual verifications are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve the existing issues. Furthermore, the commenter stated that access authorizations and provisioning warrant further clarity in the recirculation ballot because they require significant resources, involve extensive complex data and are among the most currently violated Requirements. In response to the two aforementioned comment responses, the SDT has modified Requirement Parts 4.2 through 4.5 to state up front to which type of access each Requirement Part applies. CIP-007-5 Requirement Part 5.2 is a security hardening control applying to the enabling or disabling of generic accounts (From the Technical Guidelines section: A generic account is a group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type).

The key distinction between CIP-007-5 Requirement Part 5.2 and CIP-004-5 Requirement Part 4.3 it that generic accounts and associated privileges are not authorized nor is there the same concept of "need to know." CIP-004-5 Requirement Part 4.3 applies to user accounts only and would not necessarily indicate a full listing of user accounts and privileges on the system. However, one could envision a process by which an entity finds it more efficient to perform a full account listing and thereby produce evidence in compliance for both Requirement Parts. The SDT also point out that the identification of default or generic accounts occurs only once and does not require annual verification.

The SDT acknowledges the listing of individuals with authorized access to shared accounts (CIP-007-5 Requirement Part 5.3) has a connection to the authorization of CIP-004-5 Requirement R4 because entities must know the list of individuals

authorized to a shared account in order to fully perform the quarterly and annual assessments. However, entities may comply with the Requirement to authorize access to a BES Cyber System without specifying how they obtain such access. Overall, the SDT sees valid arguments for this Requirement Part residing in both CIP-004-5 and CIP-007-5. Because of the history of prior versions, the difference in applicability, and the significance in moving a Requirement Part to a different standard, the SDT choose to retain the Requirement in its original location.

Data Retention Requirements

There were several commenters that stated specifically and in general to exclude any data retention Requirements from the standard. In response, these few Requirements are not intended to specify a retention period as done in the Compliance section of standards, but to retain information for the purpose of incident response and analysis.

CIP-002-5

Draft 3 of CIP-002-5 obtained an affirmative ballot result of 74.9% with a quorum of 80.6% of the ballot pool at its successive ballot of October 2012. This result indicates a very significant improvement from the previous ballot and achieves a high level of stakeholder consensus.

One commenter noted an inconsistency in sub-Requirement numbering in the standard. This has been corrected and the part numbers have been changed in CIP-002-5 to remove the "R" from Requirement "R1.1", etc., to "1.1", etc.

There was a comment that stated the purpose of the standard is inconsistent with the approach, further noting that "the standard as written evaluates only the impact of a degradation to a group of Facilities instead of evaluating the degradation of a BES Cyber System." The SDT notes that the standard has taken the approach that the categorization of qualified BES Cyber Systems is based on the impact of the functions performed by the assets they are supporting. This is consistent with risk management approaches that evaluate risks based on the functional objective of the organization (in this case the reliable operation of the BES). The same entity proposed a multilevel evaluation of the impact of cyber systems based on functional impact as well as the individual impact of the cyber system within the functional impact. This multilevel approach was one that was proposed to stakeholders early in the development process: industry comments called for a simpler approach which resulted in the current one.

Another commenter stated that the CIP-002-4 and Version 5 "bright-line criteria" step away from a risk based method to a prescriptive approach. The commenter further wrote that it is an inverted philosophy from the approach draft 3 used in the other CIP Version 5 standards. The SDT notes that CIP-002-5 follows on the approach used in Version 4, which has been approved by the industry and by FERC, for using bright lines instead of an entity-defined risk-based methodology for evaluating the impact of assets, and the SDT is extending the concept with a multi-tiered approach to categorizing all BES Cyber Systems according to impact.

There was a comment that the standards use the term "Transmission stations or substations," and the commenter proposed some other terms such as "switchyards." The SDT points out that a brief clarifying paragraph is included in the Guidelines and Technical Basis explaining the use of these terms in the section on Transmission criteria: "*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain*

autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist." The SDT also made minor editorial changes when using this term for more consistency.

There was a comment that the paragraph in the Background section that deals with the 300 MW UFLS threshold should be moved to the Guidelines and Technical Basis section. The SDT points out that section 4 is a common section that is in all the standards and believes that the explanation of the 300 MW threshold used in the common section 4 should be included in the common part of the Background section to carry it into all the CIP standards in this series.

One commenter provided general feedback on the approach taken for CIP-002-5. The commenter cited concerns on the Facilities-based approach to evaluating the impact of BES Cyber Systems. The SDT had extensive discussions in the last several years on the merits of both the systems-based and facilities-based approaches. The SDT points out to the commenter that entities are free to use any method to arrive at the identified and categorized BES Cyber Systems. Regarding the evaluation of the impact based on the function of the assets, a fundamental concept in risk management frameworks, including the National Institute of Standards and Technology (NIST) Risk Management Framework, is that the evaluation of the risk for systems must be related to the mission of the organization, in this case, the reliability of the BES. The entity also commented on the lower level of protection for low impact BES Cyber Systems. This is consistent with tailoring the level of protection according to the risk (in this case, the impact) and optimizing available protection resources for the systems that most need the protection according to their impact on the mission of the organization. The commenter also commented on the consideration of "interconnectedness". The SDT has taken the approach of considering connectivity in the development and application of Requirements.

There was a comment made that the section on BES reliability operating services in the Guidelines and Technical Basis section should be removed as it contains many subjective areas. The SDT has gone through several iterations of including these in the standards or as guidance and has resolved to providing guidance on functions for applicable functional entities based on the functional model. The section has been well-received with comments requesting the included enhancements in the past drafts.

A recommendation was made that the undefined term "adversely impact" should be replaced with "Adverse Reliability Impact" throughout the standard and definitions document to be consistent with the defined term in the NERC Glossary. The SDT disagrees, because where the SDT has used the term Adverse Reliability Impact, it has used it precisely for the meaning defined in the NERC Glossary. It is not appropriate to use the NERC Glossary term when it is not the intent of

the SDT to use the meaning of the defined term. The NERC Glossary term is very specific to a level of impact on the reliability of the BES. This is not always the appropriate level or meaning in all cases where the term "adversely impact" is used.

One commenter noted that the diagram at the end of the Guidelines and Technical Basis section is confusing. In response, the SDT notes the flowchart is an actual use case provided by an observer and may not be applicable in all environments. It is meant to provide one approach used by an entity.

Requirement R1

There were several commenters that noted there was inconsistency in the words used in Requirement R1 and Attachment 1, criterion 3.4 of section 3 (Low Impact), regarding restoration, with terms used in EOP-005-2 and with terms used elsewhere in the standard. The SDT has made changes to these sections to be consistent with the terms used in EOP-005-2: Blackstart Resources and Cranking Path and initial switching Requirements.

One commenter requested that additional reference to the specific standards be included where the term "...is subject to one or more Requirements in a NERC or Regional Reliability Standard" is used. The commenter furthermore stated that this term is not specifically used in Requirement R1 or the Requirement Parts. However, it is used in section 4 to qualify UVLS/UFLS, Special Protection Systems and Protection Systems owned by DPs that are subject to these CIP standards. In response, the SDT notes the intent is to include only those assets for DPs that are covered by a NERC Reliability Standard, which would be those, by implication, that are related to the reliable operation of the BES. References to other standards within a standard are not recommended practice in NERC standards drafting.

There was a comment that the last sentence in the opening paragraph for Requirement R1 in the Guidelines and Technical Basis section for Requirement R1 is confusing. The SDT has clarified and simplified the sentence.

One commenter stated that the use of the term "considers" in Requirement R1 leads to the same confusion as exists with the existing CIP-002-3 standard as some entities will argue that "consider" does not mandate a required subsequent action. The commenter proposes that the Requirement should be restated as "For each asset type enumerated below, each Responsible Entity shall: . . ." In using the term "considers", the SDT recognized that all entities do not own all the types of assets listed. The proposed language assumes that all entities own all of the types of assets listed. In providing this consideration, the SDT seeks to avoid situations where entities end up having null lists for each one of the type of asset that it does not own.

The same commenter stated that the assertion in Requirement Part 1.3 that the entity is not required to produce a list of low impact BES Cyber Systems renders this Requirement not auditable for accuracy or completeness; and that to demonstrate that all high and medium impact BES Cyber Systems have been properly categorized, the entity must be prepared to produce a list of all BES Cyber Systems that were evaluated, the remainder of which represent the low impact BES Cyber Systems. The commenter further stated that the entity must be prepared to demonstrate the minimal Requirements applicable to low impacting BES Cyber Systems have been properly implemented, also requiring a list of impacted systems. The SDT has considered the considerable increase in the scope of cyber systems included in this version and has taken the approach that those Requirements that apply to the anticipated large number of low impact field systems should be focused on program components that provide the corresponding level of protection, rather than a disproportionate effort in managing compliance for these systems.

One commenter suggested the removal of Requirement Part 1.3 and the low impact category in Attachment 1. The SDT has taken the approach that all BES Cyber Systems should be subject to some level of protection. The SDT has provided an approach to allow the specification of the commensurate level of protection for low impact cyber systems while providing a framework that would minimize entities' compliance burden for the large number of low impact cyber systems that it anticipates.

One commenter recommended that the six asset categories included as part of Requirement R1 be removed and the drafting team instead reference Attachment 1, if needed, to ensure consistency in language as well as prevent unnecessary duplication. The inclusion of the asset types in Requirement R1 is a direct result of comments from a large number of stakeholders on draft 2 to provide some reference to asset types required to be considered in Versions 1 through 3. The SDT has made modifications to improve overall consistency within the standard.

Another commenter noted that, in Requirement Part 1.3, the intent is to provide protection at BES Facilities that do not meet Attachment 1, criteria 1.1 through 2.13. The commenter added that the wording is technically flawed and conflicts with the definitions of BES Cyber Assets and BES Cyber Systems. The commenter continued to add that, by definition, to qualify as a BES Cyber Asset and System the asset must have a 15 minute impact on reliability of the BES and that a low impact facility cannot have such an impact to the BES. The SDT points out that while the definition of the BES Cyber System and BES Cyber Asset assumes impact on the function of the Facilities, systems and equipment (asset), an asset in the low impact does not assume that it has no impact on real-time operation of the BES. The 15 minute stipulation in the definition of BES Cyber Asset describes an impact on the function performed by the low impact asset for the BES.

One question arose which asked how an auditor is to verify identification of all BES Cyber Systems that are applicable to Requirements Parts 1.1 and 1.2. There are current Requirements to identify Critical Cyber Assets in Versions 1 through 4. The SDT expects that auditors will continue to use similar methodologies used to verify compliance to such Requirements.

One commenter stated that its interpretation of Requirement R1 meant that each qualified cyber asset must be marked. This is not the intent, and the SDT does not believe that the language in Requirement R1 is specifying any such marking for cyber assets at each asset. The clause "at each asset" is purposely included in close proximity to "BES Cyber Systems," which is the phrase that "at each asset" is intended to qualify, not the word "identify". Certainly, the expectation is that the identification of the BES Cyber System would include information in some fashion about which asset it is "at". The proposed language "Identify and list each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at the asset level," does not meet the intent of the Requirement, since it must be clear that the identification must have enough information to identify the BES Cyber System, including the information on what asset it is located at.

Requirement R2

Many commenters noted that alternative, clearer language for Requirement Part 2.1 would ensure that there is no implied Requirement for updates outside of the annual Requirement review. The SDT believes the 15 month review is sufficient for categorization of BES Cyber Systems, and it has modified the language to provide additional clarity.

Attachment 1

There was a proposal that the language should be modified to specify that the applicable functional obligations referenced within criteria 1.1 through 1.4, 2.11, and 2.12 apply to only those real time tasks identified in the Functional Model. The SDT points out that the applicability of the Requirements is to BES Cyber Systems, and that the definition of BES Cyber Assets (and by reference, BES Cyber Systems) only includes those that impact real-time operation. The functional model does not define the tasks of the functional entity in terms of real-time or non-real-time, but the term real-time is used rather to describe its relationship with other functional entities.

Many commenters reiterated their comment on the rationale for categorization as high impact those Control Centers that control at least one of the medium impact facilities. The SDT responds that the localized impact of a facility at a single location is different and less impactful than the impact of a Control Center that controls one such facility and other facilities in the wide area.

There was one comment that stated Attachment 1 does not specify where within-hour generation and interchange scheduling systems related to Balancing, Managing Constraints, and Inter-Entity Coordination fall within the high-medium-low impact framework. The SDT clarifies that these systems used to perform functions that are not impactful to real-time operation of the BES, as such would not be defined as BES Cyber Systems, unless these systems are also performing functions impactful to the real-time operation of the BES. They would be included in scope in the initial scoping of supporting the functional obligations of the relevant functional entity, but systems strictly performing these functions in the absence of other functions impactful to real-time operation would fall out of scope.

There was a comment that the first bullet under the overall heading of the Guidelines and Technical Basis section for Attachment 1 makes several references to the term "BES Asset." The SDT has corrected the inappropriate capitalization of BES asset and uses the term BES asset as referenced in Requirement R1 of CIP-002-5.

One commenter expressed concerns that restoration facilities were categorized as low impact facilities. This issue was raised in comments received in previous drafts and the SDT has discussed this at length, reaching out to other NERC technical committees. After consideration of the overall risks to the availability of adequate restoration resources, the SDT's resolution was to categorize restoration facilities as low impact, as explained under the Guidelines and Technical Basis section of CIP-002-5, on pages 30 and 31.

Many criteria in Attachment 1 relate to Interconnection Reliability Operating Limits (IROLs). One commenter wrote that this may be a problem in the WECC area where the RCs have not yet defined IROLs. Consultation with WECC indicated that WECC is in the process of defining IROLs and that IROLs will be defined well within the implementation timeline of these standards.

Another commenter stated that since the term "associated data centers" has been removed from Attachment 1 and that it should be removed from the Guidelines and Technical Basis section. The term has been moved to the definition of the Control Center and an additional clarification has been included where it is referenced in the Guidelines and Technical Basis section.

Criterion 1.2

One commenter noted that the 3000 MW minimum specified in criterion 1.2 is excessive and does not appropriately reflect the potential risk a network-connected Balancing Authority (BA) has not only upon its own service area but also

upon the rest of North American BA, Reliability Coordinator (RC), and TOP registered entities with which it is directly or indirectly connected via the ICCP communication networks. The SDT carefully considered discussions from stakeholders and reviewed data on the distribution of BAs that would be affected. The SDT concluded that the threshold would include the majority of BAs with significant impact.

Criterion 1.4

Many commenters noted that this criterion would require that a 1500 MW Generator Operator (GOP) Control Center take on a High impact rating, while the rest of the Facility is medium impact. The commenter added that even if the criterion is intended to apply to multiple locations, the aggregated generation should be 3000 MW or greater - consistent with the risk level assigned to a BA Control Center. The SDT points out that a control room for a single generating plant at a single location does not meet the definition of a Control Center. The criterion has not defined a specific numeric bright line for a generation Control Center. For example, a generation Control Center could control three 1200 MW generation Facilities, for a total of 3600 MW, at more than one location, and still be qualified for a medium impact generation Control Center if none of these meet criteria 2.1, 2.3, 2.6 or 2.9. It is true that if one of the generation Facilities the Control Center controls meets criterion 2.1 for 1500 MW, it would be categorized as a high impact asset.

Criterion 2.1

One commenter requested clarification on the relationship between a single plant location and a single Interconnection used in the defined term meaning. In making these qualifications, the SDT considered scenarios where sets of units within a single plant location may service multiple Interconnections, as pointed out by the commenter. In these cases, the SDT wanted to ensure that the impact considered is consistent with the bright line defined in this criterion, which was based on numbers reviewed for each Interconnection. The same entity inquired about “multiple generators with different interconnection facilities which connect to different parts of the same substation.” It is not clear whether the commenter is using the general term interconnection (meaning connection to the Transmission System) or in the meaning of the defined term.

One commenter felt that the use of the word “by” in the first sentence of this criterion does not make sense and should be reworded. The use of the word provides an entity with the capability of evaluating groups of units when a single plant location may be servicing multiple Interconnections and is logically partitioned into more than one generation output. There are further qualifications which may provide additional grouping criteria, such as common cyber systems.

One commenter suggested that the 15 minute stipulation should be extended to 30 minutes to be consistent with some criteria in reliability standards. Some standards have used 15 minutes, which the SDT has used as its criterion. The commenter seems to suggest that the 15 minutes is "tighter" than 30 minutes. Extending the interval to 30 minutes would in fact reign in more cyber systems rather than reduce the number of cyber systems (by extending the criterion for real-time, more cyber systems are likely to meet this criterion than 15 minutes).

One commenter requested clarification on the term "commissioned generation." The term is used to specify generation resources that have been commissioned for operation and is intended to exclude generation that has not been commissioned for operation (such as mothballed generation, generation shut down for maintenance, or new generation that has not been commissioned for operation yet).

Criterion 2.3

There were many comments that the term "planning horizon of one year or more" is unclear and could be misinterpreted. The SDT has added guidance on this to make it clear that the planning horizon of one year or more means that the plan covers a reliability planning span of one year or more and that it does not necessarily mean that the operating day is over one year. The intent is to exclude generation required to operate or keep on operating to temporarily avoid reliability impacts.

There were many comments on the guidance relating to the role of the Regional Entity (RE)/ Regional Reliability Organization (RRO) and noted that the RE/RRO is not required to perform coordination of the actions resulting from planning studies. The commenter also noted that the term RRO is no longer the appropriate term. The necessary changes have been made.

One commenter asked whether the term "generation Facility" in this criterion is designed to cover a single unit at a facility, or all units at a single plant or Interconnection, as described in section 2.1. The SDT intended to include in this criterion all generation Facilities required to meet the designation: these can be a single unit, a set of units or all the units in the plant.

One commenter noted that the Guideline and Technical Basis section omitted the TP as one of the possible entities that could designate the generation Facilities. The SDT notes this has been corrected.

A commenter asked whether the phrase, “such as due to a Category C3 contingency” was intended to provide guidance to what faults to run and whether the term “Adverse Reliability Impact” which is used in Attachment 1, meant to be the criteria for all types of contingencies. The phrase “such as due to a category C3 contingency” is intended to provide an example of the type of condition that could lead a Planning Coordinator (PC) or Transmission Planner to designate “must run” generation Facilities. The term “Adverse Reliability Impact” is used here to qualify the reason the PC or TP would designate such generation Facilities. In response, the SDT notes it is intended to distinguish from designations made for power market management reasons.

One entity commented that the guidance provided in this section in the Guidelines and Technical Basis section referenced “Reliability Must Runs (RMRs)” and discussed the differences between market RMRs and what this criterion intended. The SDT points out that this is the reason it has avoided using the term “reliability must run” in the Requirement itself. However, this term has been used interchangeably in both contexts for lack of a better term, and that the meaning of the term and the reason for having these units differ depending on the context. The SDT has included an extended discussion of the underlying reason for the criterion in the Guidelines and Technical Basis, focusing on the long term remediation for BES deficiencies to avoid Adverse Reliability Impact. The SDT also made additional changes to the guidance to clarify the role of the RE in coordination and contracts.

There was a comment that the criterion is based on studies from functional entities that do not have applicability under this standard and on notifications from these entities. The SDT notes that these activities are implemented today and that there are TPL standards that require these functional entities to perform these studies. The standard also requires these planning entities to provide an action plan for remediation of identified deficiencies.

Criterion 2.4

In this section, medium impact is assigned to Transmission Facilities operated at 500kV or higher. One commenter noted that exclusion is warranted for distribution stations that are situated at the receiving end of a radial 500kV line. The commenter further noted that specific instances exist of 500/69kV stations whose only purpose is to provide distribution service. The applicability, which is section 4, stipulates applicability to BES Facilities for entities other than DPs. If the facility meets the qualification for designation as a non-BES facility under the definition of the Bulk Electric System, then it is not in scope for application of these CIP standards.

Criterion 2.5

One commenter noted that the 200kV floor specified in criterion 2.5 does not adequately consider the risk to the BES imposed by large regional areas that are predominately sub-200kV. The commenter noted the BES is defined as 100kV and above and the criterion needs to consider all of the BES in some manner. The SDT has not excluded any BES Transmission Facility in its applicability, but believes that not all BES Transmission Facilities should be protected at the medium impact level. The categorization is one that is based on impact, and the SDT believes that the inclusion of ALL BES Transmission Facilities at a single impact category is unjustified and defeats the concept of tiered levels of protection based on impact.

One commenter stated that, as currently defined, the values in the table force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. The commenter recommends the values be revised as follows: Voltage Value of a Line 200kV - 399kV - Weight Value per Line - 800; Voltage Value of a line 400kV to 499kV - Weight Value per Line - 1300. The SDT based the values in the table on values published in an engineering report, has reviewed comments from previous drafts, and believes that it has a technical basis, as described in the Guidelines and Technical Basis section, for using these values.

A commenter provided an extensive discussion of the concerns on the application of this criterion for Direct Current (DC) Facilities. The commenter argued that in the case of DC Facilities, the impact is better assessed in a wide area perspective rather than as a localized way as specified in this criterion. The commenter further commented that such studies could be conducted to provide an impact based on MW rather than the approach used in 2.5 in the case of DC Facilities. The SDT has not considered this approach for DC Facilities and any criterion that is based on a "study" (that is not currently required by any reliability standard) to determine the impact of these DC Facilities would be contrary to the bright line approach.

One commenter requested that diagrams be provided to illustrate the bullets in the Guidelines and Technical Basis. The SDT discussed providing diagrams to illustrate the bullets, but resolved that there are many configurations that can provide these illustrations and that these would raise additional questions for entities that would not be familiar with specific configurations. Entities should use their specific configuration to apply these concepts.

One commenter requested many clarifications. These are listed below with their responses:

1. Is/how is a DC line counted?
   A DC line is counted at the operating voltage for the purpose of application of criterion 2.5.

2. If you have a tie between two subs that has a transformer in series, does the line receive a weighting factor (seems to per guidance)? Do you use the higher or lower voltage? Is it the same for both ends of the line?
   If the transformer in at the site of a Transmission station or substation, it is considered as part of the Facilities of that station or substation and lines incoming and outgoing of the station or substation are considered in the application of this criterion. If the transformer is in a dedicated station, each of the stations (including the transformer station) will consider incoming and outgoing lines of the station or substation in the application of the criterion.

3. From the guidance document, it was clarified that radial facilities that only provide support for "single generation facilities" would not be included. What is the definition of a "single generation facility"? Uncertain situations might include two base load turbines aggregated on one line or wind farm collector subs which have multiple sites feeding into a single high voltage collector sub?
   These examples are all considered as a radial connection to a single generation facility.

4. From the guidance document, in the last bullet on page 27, it is not clear what the statement "In these cases" is referring to, whether the designation as a single facility or multiple facilities.
   The clause "In these cases" is qualified further by "of these transformers being within the "fence" of the substation or station": this is referring to what is considered a single facility.

5. From the guidance document, in the last bullet on page 28. How would classification of the number of substation connections be handled if two lines are parallel between the same two subs, but one has been tapped for local, non-networked load service?"
   Assuming that the tap is at the station or substation, these would be considered connections to one other substation, but both outgoing lines would be counted for the purpose of aggregate weighting. If the tap is not at the station or substation, there is not enough information to definitively make a determination without evaluating the specific facts and circumstances.

One commenter inquired during the comment period on whether the connections to other stations or substations that are considered are only those that are operating at voltage levels between 200kV and 499kV. The SDT reviewed previous drafts and clarified the criterion to ensure that the qualification of voltage levels of 200kV and higher for these connections is more explicitly stated rather than implied.

Criterion 2.6

One comment was on the obligation for the RC with respect to IROLs. RCs are required to provide to its TOPs in its RC footprint the SOLs under FAC-014-2, Requirement R5.1. In particular, it requires the RC to provide specific information related to IROLs in the sub-Requirements of 5.1. The particular agreements between RCs, TOs and TOPs to enable the proper management of IROLs in compliance with the NERC Reliability Standards are beyond the purview of the guidance. The SDT points out that the delegation of functional obligations must be considered in these Requirements.

Criterion 2.8

A commenter noted correctly that Transmission Facilities under 2.8 that do not affect Transmission, in aggregate, for generation that is less than 1500 MW do not qualify under this criterion, even if the generation facility (plant) contain cyber systems that qualify under 2.1., (provided they do not qualify under other criteria).

Another commenter noted that, in the case where the generation is not owned by the TO/TOP would be at the mercy of the Generation Owner's (GOs) application of the standard even if the TO's facilities would not otherwise be in scope. The commenter is correct in that the TOs Facilities providing the connection would be deemed to be a medium impact. This is consistent with the impact of these Transmission Facilities on the BES.

Criterion 2.9

One commenter requested clarification on what an automated switching system is. Automated switching systems refer to systems implemented in software that perform the same automated protection functions as Special Protection Systems or Remedial Action Schemes.

Criterion 2.10

One commenter stated that the guidance document specifies that the SDT "chose the term 'each' to represent that the criterion applied to a discrete System or Facility". The commenter's interpretation of this statement is that a regional UFLS program which sheds more than 300 MW and is comprised of multiple independent UFLS relays in at different substations would not be given a Medium Impact Rating at the NERC or RRO program level and that an individual relay would only be given a Medium Impact Rating if that relay shed more than 300 MW by itself. The commenter's interpretation is partially correct in that individual independent relays that are part of a UFLS system that sheds 300 MW or more in the program Requirements, but do not shed the required load by a common control system, (e.g., they individually trigger independently, even if they are configured to trigger based on the same sensed conditions) do not qualify. However, if the individual relays are all triggered automatically by a common control system that determines

that conditions warrant the action (such as a control panel that triggers a system of relays in a substation), then they are part of a load shedding system that can automatically shed more than 300 MW and therefore qualifies. The commenter's assertion that a single relay that sheds 300 MW or more does qualify is correct.

The same commenter noted the statement on ERCOT's LaaR demand/response program is not considered as qualifying under this criterion and requested more general guidance in the Guidelines and Technical Basis section for this criterion that talks to these types of programs. The SDT has included a more general statement in this section.

Criterion 2.11

There was a comment that the Guidelines and Technical Basis section on this criterion incorrectly referenced a 300 MW threshold. The SDT has made the necessary correction.

Criterion 2.12

Many comments related to the portion of criterion 2.12 of Attachment 1 that is applicable to TOP Control Centers. Commenters stated that criterion 2.12 of Attachment 1 included all TOP Control Centers, not already categorized in the high impact category, as medium impact and that many smaller TOP entities' Control Centers should be categorized as low impact in the same manner that criteria were defined for generation and balancing authority Control Centers. Many commenters proposed alternate proposals for a threshold that could provide such a criterion to be used as a candidate for categorization as low impact, such as voltage levels lower than 200 KV or using throughput indicators similar to those used in the case of transmission substations in criterion 2.5. Others provided proposals to restructure the thresholds for all three impact levels for TOP Control Centers. One commenter also proposed an exclusion clause in criterion 2.12 that would be based on engineering analysis that demonstrated minimal impact to the BES. In response, the SDT did not find any such study that would be required by an existing NERC Reliability Standard.

As part of a consolidated response to more than one entity that provided comments on draft 2's CIP-002-5, Attachment 1, criterion 2.11 (which maps to criterion 2.12 in draft 3 and draft 4), the drafting team carefully considered comments to include a threshold for TOP Control Centers, but, to reiterate previous considerations and response to the comments related to that criterion (on page 35 of consideration of comments form A), such a threshold is not supported in consideration of the functions provided by those Control Centers. The largest concentration of cyber traffic is to and from Control Centers, and loss, compromise, or misuse of cyber systems at control centers constitutes a high risk to reliability. Furthermore, criterion 2.12 applies to "Control Centers" used to perform the functional obligations of TOPs, so it is only applicable to the extent the Control Center meets the criteria of the proposed definition.

While there is clear guidance in the NERC Reliability Standards that the SDT could use to determine bright lines for generation in the wide area (such as contingency reserve Requirements), the SDT did not find any in the Transmission area to support thresholds for TOP Control Centers. The source for transmission substation bright lines, based on throughput in a Transmission station or substation according to voltage level, provided easily measureable thresholds because of their localized nature: for a given single location, the application of the threshold criteria can be easily determined. There was no bright line that the SDT could find applicable and justifiable in a wide area situation for TOP Control Centers that control many interconnected Transmission Facilities in many locations. The SDT could not find any technical guidance, either in NERC technical studies, or in existing NERC Reliability Standards Requirements, on how the loss of interconnected Transmission Facilities could be used as a basis for establishing thresholds for TOP Control Center impact. The TOPs span of control is not limited to just Transmission lines, but to a large number of diverse Transmission Facilities that relate to the reliable operation of the BES. This complexity, together with the interrelated impact from the large number of diverse Functional Entity types that impact TOP functional obligations, make it very difficult to define a justifiable threshold that can be rationalized considering all the scenarios that could impact real-time operation for a TOP Control Center.

As stated in the guidance for CIP-002-5, the reasoning and purpose for the 1500 MW threshold for generation is different:

> "By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected."
>
> The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used."

Furthermore, the SDT has an obligation to be responsive to FERC Order No. 706, which was issued after a notice of proposed rulemaking, and several points from that order were reiterated in subsequent FERC Order No. 761. The SDT has discussed this issue very significantly in several face-to-face SDT meetings. In addition to the technical reasons and differences explained above, the SDT anticipates that any threshold for TOP Control Centers will likely be met with a directive countering such threshold upon filing for approval of these standards.

The SDT based its approach in the development of this criterion in consideration of the following comments and Directive from FERC Order No. 706 approving CIP Cyber Security Standards Version 1 and FERC Order No. 761 approving CIP Cyber Security Standards Version 4.

In its Order No. 706, Para 280, FERC supports the reasoning for its subsequent Directive in paragraph 282 with the following comment:

> "...it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset…"

The SDT points out that Medium and High Impact under Version 5 translate closely to "Critical Asset" under previous versions. The Directive in FERC Order No. 706, Para 282 further states:

> "Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets."

As explained earlier, the SDT's consideration of misuse of TOP Control Centers and the role they provide, pursuant to this Directive, do not support an exclusionary threshold from medium impact in CIP-002-5, Attachment 1.

In its Order 761 approving NERC CIP Cyber Security Standards Version 4, FERC commented in paragraph 21 that:

> "...Version 4 will offer an increase in the overall protection for bulk electric system components that clearly require protection, including control centers"

In the same Order 761, Para 57, FERC further commented with the following:

> "However, we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with the Requirements of Order No. 706."

Again, in the case of Generation and BA Control Centers, the SDT used the 1500 MW threshold for consistency with the rationale used for generation bright lines. As stated, no such source can be used for wide-area transmission in the non-CIP reliability standards or other published source.

Therefore, the SDT opted to keep criterion 2.12 as it applies to TOP Control Centers (i) to ensure that all TOP Control Centers are adequately protected, in the absence of technically justifiable thresholds for lower impact TOP Control Centers, (ii) because of the critical nature of their real-time reliability functions for the interconnected Transmission systems they monitor and control, and (iii) in consideration of FERC comments and Directives expressed in Order No. 706 and reiterated in Order No. 761.

Criterion 2.13

One commenter believes that the 1500 MW minimum specified in criterion 2.13 is excessive and unreasonably excludes a significant number of BAs from meaningful participation in protecting the BES from cyber-attack and that establishing criteria effectively eliminates significant numbers of interconnected control centers fails to address the specific concerns outlined in both FERC Order No. 706 and FERC Order No. 761. The SDT considered the MW distribution of BAs and determined that the 1500 MW is consistent with generation thresholds established (and approved by FERC in Version 4) in other criteria and is appropriate in including a significant number of BAs at the medium impact category. The SDT points out low impact cyber systems are still subject to protection Requirements.

Criterion 3.1

There was a comment that criterion 3.1 should specifically state that only Generation and BA Control Centers are included. While combination of the criteria for Control Centers currently results in only Generation and BA Control Centers, this criterion is intended to catch all Control Centers that have not already met a previous criterion in section 1 and 2 (high and medium impact). The current language conveys this intent.

Criterion 3.4

One commenter stated that the use of the terms “critical” and “initial system restoration” in criterion 3.4 is problematic. The commenter noted that initial system restoration is not a defined term and registered entities have regularly argued that none of their resources are critical as they have many options from which to draw upon. The SDT has made modifications to the criterion that uses language consistent to EOP-005-2 and defined terms.

The commenter also noted that the Low Impact Rating criteria needs to include automatic Load shed systems that do not shed sufficient Load to meet criterion 2.10. All Load shedding systems that are part of the BES are included automatically as stated in the Applicability section (section 4). For DPs, Load shedding systems that meet the qualifications in section 4 are included and are all included as medium impact.

CIP-003-5

CIP Senior Manager

A commenter expressed concern on the designation of the CIP Senior Manager by a "high level official" and whether that official could be the same person as the CIP Senior Manager. The SDT notes that the language regarding "high level official" is but one example in the measure. An entity is free to determine the best way to designate a CIP Senior Manager for its unique circumstance. This could be by high level official, by committee, through authorization from a board of directors, or from any number of other options.

The SDT received a comment that there was a concern that by only requiring the identification of the CIP Senior Manager by name that the Requirement was not auditable in instances where multiple individuals have the same name at the same company. The SDT appreciates that this is a very real scenario. However, the SDT believes that this is specifically the style of auditing that it sees is incompatible with the objectives it is setting out to achieve. The SDT believes that real cyber security program leadership transcends the name on the document. Audits, instead of verifying a name on a page, should instead validate the Requirement objective that the individual identified as the CIP Senior Manager is in fact leading and managing the implementation and continuous adherence to the CIP standards.

One comment indicated that "The CIP Senior Manager relies on both the definition in the CIP Glossary and the "Responsible Entity" verbiage in every standard in section 4." The SDT does not agree. The definition of a CIP Senior Manager stands alone. However, the Requirement itself is for the Responsible Entity (the entity obligated to comply with the standard) to identify a CIP Senior Manager.

Policy Requirements

One commenter expressed concern that the SDT was too prescriptive in its language around electronic access controls in the low impact policy. The SDT does not believe this to be the case. On the contrary, the SDT has some concern that it may have left the policy up for too much interpretation. However, the SDT believed that the entity is in the best place to determine the appropriate access controls for its given situation, while still implementing an ESP of some form.

Numerous commenters expressed confusion over the applicability of the policy Requirements. The SDT considered many approaches to this issue and believes that the applicability of these requirements is clear as drafted. Requirement R1 applies to high and medium BES Cyber Systems and states as much explicitly in the Requirement. The intent of

Requirement R2 is to apply to those assets that contain low impact BES Cyber Systems and not to the BES Cyber Systems themselves. This effectively allows the entity to track implementation of the policy at a higher level of abstraction (per asset rather than per BES Cyber System), and the SDT believes this will substantially reduce the burden of evidence required by the low impact policy. The reference to CIP-002-5 is to further clarify the intended reference to asset rather than BES Cyber System. The language following the numbered list specifying that "an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required" is part of the Requirement language of Requirement R2 and should be interpreted as such. This language was explicitly included to give the industry the assurance that this Requirement would be audited (sampled) at the asset (substation, generation plant, etc.) level and not the individual Cyber Asset level. The SDT also believes that entities will be able to implement internal controls to ensure the implementation of the cyber security policy at its low impact assets. The SDT does not believe that there is any double jeopardy between Requirements R1 and R2.

One commenter suggested that the SDT modify the Requirement language for the cyber security policies to clarify that multiple policy documents could "collectively" address the topics in the Requirements. The SDT agrees and has updated the standard to reflect this change.

The SDT received comments that Requirements R1 and R2 require annual review of the policy, but never explicitly require the policy to receive updates as a result of that review. The SDT believes this is implicit in the Requirement, and updates would occur as part of an entity's ongoing compliance with the Requirement.

Requirement R2

One commenter questioned the necessity of Requirement Part 2.4 considering that entities are not required to monitor for incidents to their low impact BES Cyber Systems. The SDT appreciates this concern. This element was specifically included because the SDT strongly believes that incident response is a key component of a resilient system. Even though an entity may not be constantly monitoring for a Cyber Security Incident at its low impact BES Cyber Systems, the SDT expects that should an incident be discovered, a plan should be in place for rapid execution.

Requirement R4

The SDT received comments requesting that language be added into the Requirement clarifying that the delegation authority may itself be delegated. The SDT considered adding language to the standard to clarify this, however, the SDT believed that the Requirement was clear as is and that there was no language that prevented this delegation. The SDT included the discussion on this topic in the Guidelines and Technical Basis section specifically to clarify this issue.

One commenter pointed out that Requirement R4 as written requires that the delegations from the CIP Senior Manager be updated within 30 days of the initial delegation. The SDT agrees this is confusing and has struck this language from the Requirement.

The SDT received questions on why it included the IAC language on the Requirement to delegate authority from the CIP Senior Manager. The SDT specifically included the IAC language because it believes that in a very large organization, it is likely that changes in personnel without adequate update of delegation documentation could result in very minor deficiencies that have little or no impact on the reliability of the BES. These are precisely the types of administrative violations that the SDT is attempting to eliminate from the CIP standards. The SDT believes that, given this is all a single Requirement, the documentation required in the third sentence of Requirement R4 is part of the overall process specified in the first sentence of the Requirement; consequently, the IAC language applies to all parts of Requirement R4.

CIP-004-5

General

One commenter believes that the evidence retention for verifying access should be less than the audit cycle (which is three years for BAs, RCs and TOPs), especially if the SDT plans to keep the quarterly reviews to verify that access has been properly removed. Entities are required to demonstrate compliance with the Requirements for the entire audit period for all NERC Reliability Standards, regardless of evidence retention Requirements.

One commenter noted that within each Background section (section 5) under the heading "Applicable Systems Columns in Tables" is missing the second sentence that appears in the other standards where Medium Impact BES Cyber Systems with External Routable Connectivity is also referenced in the Background sections. The SDT confirms that it intended that phrase to be consistent wherever that applicability term was used, and the SDT has modified the background to clarify that intent.

There was a comment that within CIP-004-5, the definition of EACMS appeared inconsistent with the definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards", and that it could result in misidentification, misapplication or inconsistent application of standards. The SDT has modified the background section with respect to EACMS to provide clarification that these are examples only that support the definition.

Requirement R1

A few commenters requested that Requirement R1 include the IAC language. In response, since the Requirement may be performed at any time during the quarter, the addition of the IAC language would not be appropriate.

One commenter requested clarification on the types of materials to be provided for security awareness on a quarterly basis. The Requirement is to provide an ongoing reinforcement that cannot be provided by an annual training Requirement. The SDT has written the Requirement to allow for flexibility in implementation by the entity. The measure provides some examples of how the entity may meet this Requirement.

A few commenters considered Requirement R1 to be administrative in nature and suitable for elimination pursuant to the SAR Paragraph 81 project. While this Requirement is partly administrative, it does provide the benefit of the entity being able to timely address and make staff aware of emerging threats and vulnerabilities. This awareness can improve security for the entity.

One commenter requested that Requirement Part 1.1 be modified as, “cyber security practices and/or physical security practices.” The SDT clarified that the Requirement part applies to cyber security, which may include awareness on associated physical security.

Requirement R2

One commenter recommended that the training content Requirement Part 2.1 be moved to the measures. The SDT considered the training topics listed to be worthy of being listed as a Requirement for a minimal core competency in security practices. Entities are encouraged to add more topics as relevant to their needs.

One commenter recommended that Requirement Part 2.2 be modified to address newly registered entities. In response, the compliance dates for newly registered entities are addressed in the supplementary implementation plan provided with the Version 5 standards.

One commenter considers it is a security risk to address some of the concepts listed in Requirement Parts 2.1.1 through 2.1.9 with every single person with a need for physical or cyber access to a cyber system, regardless of his or her role. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided.

Several commenters requested clarification on the necessary training for personnel based on individual roles, functions, or responsibilities, including changes to roles, functions, or responsibilities. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided. How the training program is implemented is at the discretion of the entity.

One commenter requested that CIP Exceptional Circumstances be removed from Requirement Part 2.2, as this applies to numerous parts and is stated at the policy level. The SDT believes that, as written, the Requirement provides necessary guidance related to the Requirement without introducing the need to rely on or link to other Requirements.

One commenter requested clarification on whether the training required by Requirement R2 extends to contractors and vendor support staff. The SDT notes that, as written, the Requirement is clear that training is to be provided to anyone having authorized electronic access and authorized unescorted physical access.

One commenter requested that Requirement Part 2.1.9 be removed. The SDT considers the training topic relevant to address the vulnerabilities of internetworked systems and to address the risks of systems that are integrated and reliant upon data from other sources to perform necessary tasks (interoperability).

Requirement R3

Several commenters noted concerns regarding Requirement R3 where employee history is not available, including the identity verification necessary to perform the criminal history check, and how to comply with these instances. The Requirement provides for this, "If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed."

One commenter requested that the timeline for personnel risk assessments pursuant to Requirement R3 be modified to 10 years to align with other governmental standards and practices. The SDT is not clear if the commenter means performed every 10 years or reviewing the prior 10 years for criminal history. The SDT has kept the timing Requirement of the existing standards as approved by FERC Order No. 706.

Many commenters requested clarification for Requirement R3 that ongoing identity verification is not required. The SDT has noted in guidance and the implementation plan that identity verification is required only initially. However, the Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets their needs to confirm identity. For some, this may include performing subsequent identity verification or it could include confirmation of previous verifications.

One commenter noted grammar concerns with the Requirement R3 table parts. The SDT believes that the overarching Requirement provides the necessary context and clarity for the table.

One commenter stated Requirement Part 3.3 unclear as to whether the evaluation process includes an expectation of clearly defined evaluation criteria for approval/disapproval of the access request. The SDT has modified the Requirement to make this clearer.

Two commenters considered Requirement Part 3.4 unclear as to whether the entity is to perform the evaluation or permits the contractor or service vendor to perform the evaluation using its own criteria with an assertion to the entity of compliance and acceptability. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits their needs. The entity is responsible for ensuring that the obligations of the Requirement are met by their contractors and service vendors.

One commenter requested that the table parts for Requirement R3 be modified to require that a personnel risk assessment must be complete before granting access. The overarching Requirement R3 states that a personnel risk assessment is required in order to obtain access.

One commenter requested that Requirement Parts 3.5 and 3.6 include a clause that it is subject to applicable law and collective bargaining unit agreements. This concern is addressed in the guidance provided for Requirement R3. As written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits its needs.

Several commenters requested clarification on whose identity must be verified. As written, the Requirement is clear that personnel risk assessment is to be performed for anyone having authorized electronic access and authorized unescorted physical access. This is further defined in Requirement Part 3.4.

One commenter recommended consolidation of Requirement Parts 3.3 and 3.4 into Requirement Part 3.2. As written, the Requirement defines each individual element to be performed and that these are each elements contained within the program specified by Requirement R3.

One commenter considered Requirement Part 3.3 redundant of Requirement Part 3.2. Requirement Part 3.2 is the performance of the criminal history records check. Requirement Part 3.3 is the evaluation of the records collected under Requirement Part 3.2.

Requirement R4

A few commenters noted concerns regarding the efficacy of Requirement Part 4.2. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the

records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

One commenter recommended that Requirement Part 4.2 be removed and provide it as an example of an internal control that the Compliance Enforcement Authority (CEA) would expect to see. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

Several commenters requested clarity in Requirement Part 4.3 related to which accounts and types are subject to an annual review. Individual user accounts, user account groups or user roles are required to be reviewed on an annual basis. User account groups or user roles are to be reviewed where these are used to for role-based management of access permissions. While review of other account types (i.e.: default account) is a good security practice, it is not a Requirement under the CIP Version 5 standards.

One commenter requested clarification of Requirement R4 regarding the word "verify" and how an entity is expected to provide evidence of access control. The Requirements mandate that access is limited to only those requiring said access. It is the responsibility of the entity to determine how they can demonstrate this limitation through the use of technical or procedural controls. The SDT believes the Requirements are written to allow flexibility in implementation to allow the entity to develop a program that meets its needs. The use of access controls lists, key control processes, and log books should be considered as options.

There was a comment that the phrase "based on need, as determined by the Responsible Entity" within Requirement Part 4.1 does not add anything meaningful to the standard. The SDT added the language based on industry comment concerns to help clarify that the appropriateness is determined by the entity and not by the CEA.

One commenter stated that the concept of role-based privilege management has not been established adequately in the Requirement. The SDT believes that Requirement Part 4.1 is written with sufficient flexibility to allow the entity to implement access control processes that meet their needs. The Requirement does not preclude the use of role-based privilege management. Requirement Part 4.3 has been modified to address this concern.

One commenter requested clarity on the measures for Requirement Part 4.2. The measures are examples of how the Requirement may be met. They are not an all-inclusive list of possibilities. It would not be feasible to list all options available.

One commenter noted concerns regarding Requirement Part 4.3 related to the level of access permission review to be performed. The detailed access privileges are to be reviewed to determine if they are appropriate. This can include review of access to file systems. As noted in the guidance, "The privilege review at least once every 15 calendar months is more detailed…"

Several commenters requested clarification regarding the verification of access to information storage locations pursuant to Requirement Part 4.4. As noted in Requirement Part 4.1, there are three distinct types of access noted; (1) Electronic access, (2) Unescorted physical access into a Physical Security Perimeter (PSP), and (3) Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. The intent of Requirement Part 4.4 is the review of access to BES Cyber System Information only.

One commenter requested clarification on the scope of physical access controls for BES Cyber System Information in Requirement Part 4.1.3. Physical access control for BES Cyber System Information only pertains to the protection of hard copies of said information. The hard copies of BES Cyber System Information are not required to be within a PSP, and therefore, CIP-006-5 may not apply.

Several commenters requested clarification on the phrase "within the last seven years." In order to obtain or retain access, a person must have had a personnel risk assessment "within the last seven years" of when access was provided and ongoing. The Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets its needs. For some, this may include performing personnel risk assessments more frequently.

Requirement R5

One commenter noted that Requirement Part 5.1 does not distinguish between termination for cause and termination without cause. The SDT removed the distinction between types of terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access regardless of termination reason.

There were an abundance of commenters that noted that the time frame listed Requirement Part 5.2 is difficult to comply with and is unnecessarily short when the employee is remaining with the company if the transfer or reassignment was in the normal course of business and not for disciplinary reasons. The Requirement allows for the entity to review the access for the individual and retain access as long as necessary for transition from the prior position. The timing was determined to be necessary to meet the to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access which includes reassignment and transfer. Note that the timing is based on when the entity determines that the individual no longer needs access, which may not necessarily be the same date as the transfer or reassignment.

One commenter requested clarification for the word "removal" in Requirement Part 5.1. Removal refers to rendering the individual unable to use the access. This may be accomplished through deletion, disabling, revocation, or removal. The SDT wanted to provide flexibility in allowing any of these means to be used.

A few commenters requested clarification regarding Requirement Part 5.4 on what scenarios would fall into this category that are not covered within Requirement Parts 5.1 to 5.3. Requirement Part 5.1 is removing the person's ability for unescorted physical access and Interactive Remote Access. This can be accomplished by revoking just these elements (i.e.: RSA, VPN, Active Directory). Requirement Part 5.4 is to clean up the remaining accounts for the users, such as access to applications, databases, and other systems.

One commenter had concerns that Requirement Part 5.5 could negatively impact the reliability of the bulk electric system in cases where there is a high movement of staff between locations. In such cases the password may change so many times that it impacts people's ability to access BES Cyber Systems (they forget the password due to the high change rate). The SDT believes that due to the capabilities of these accounts, prompt changing of the password is appropriate to minimize the risk from separated employees and contractors.

One commenter requested that "termination action" be replaced with "termination" in Requirement Parts 5.1, 5.3, and 5.4. Please see the Guidelines and Technical Basis section of the standard for additional information regarding a termination action. This section addresses the concerns noted.

There was a request that the phrase "and time" be removed from Requirement Part 5.3, as it is unnecessary, given the reference to a calendar day rather than a twenty-four hour period. The SDT agrees with that clarification and has modified the Requirement to address this comment.

One commenter considers the time limits for revoking access upon terminations to be an extreme challenge. The SDT used the timeline for terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring "immediate" revocation for any person no longer needing access, including all terminations, and the SDT believes the approach reflected in the standards is a reasonable means of accomplishing the directive.

One commenter requested consideration of Requirement Parts 5.4 and 5.5 to include Physical Access Control Systems (PACS) since some cyber assets in a PACS can also have individual user and shared accounts. The SDT considers all PACS devices to be subject to the same Requirements, regardless of impact categorization. While removal of access and changing of shared account passwords on all assets is a good security practice, it is not a Requirement under the CIP version 5 standards except where noted in Requirement Parts 5.4 and 5.5.

One commenter requested that Requirement Part 5.5 be changed to 35 days for consistency with other monthly Requirements. The time parameter in this requirement is different than the periodic performance time periods in requirement parts that use the 35 calendar days period. The SDT does not consider this action to be an ongoing monthly Requirement similar to those noted in CIP-007-5.

CIP-005-5

High Water Marking

There was a comment that per the Guidelines and Technical Basis section for CIP-005-5 Requirement R1, all of the Cyber Assets and Cyber Systems, even other BES Cyber Systems of lesser impact, within the Electronic Security Perimeter (ESP) will be elevated to the level of the highest impact BES Cyber System present in the ESP. The commenter recommended that this concept be included in section 5 background of every standard, not just in CIP-005-5 guidance. The SDT considered whether to include this in the background in each standard, but determined that it was most appropriate to make clarifying changes to the Guidelines and Technical Basis section in CIP-005-5.

Background Section

One commenter suggested that to ensure consistency between the standard and the list of "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" to update this section to reflect the same definition as used in this list. In response, these do not change or modify the definitions, but provide further background and guidance information.

There was a comment in the Guidelines and Technical Basis section that stated that an ESP is required around networks even if standalone regardless of impact classification. The commenter ask the SDT to confirm the Requirement in CIP-005-5 do not imply a list of Low Impact assets is needed. In response, the SDT has added the word 'applicable' before BES Cyber Systems in the guidelines to clarify this.

A question was raised regarding the scenario where a network switch may be divided into multiple ESPs and has one port outside the ESP that provides no routing between VLANs. Furthermore, the commenter questioned the following regarding Requirement R1.5: "does two distinct machines need to be utilized, one as a fire, and one as intrusion prevention or can it be done via one device and when the EAP is segmented into multiple network where one LAN is critical and one is non-critical; and does an IDS need to be on each network segment monitoring inbound/outbound traffic on the segment or just at the EAP monitoring inbound/outbound traffic." In response, the SDT is writing Requirements for the "what's" and leaving the "how's" to the entities to implement in ways that best protect their environments while still meeting the intent of the Requirement. These standards cannot and should not be exactly prescriptive in every possible technical situation. If that were the case, they would be constantly outdated or they would actually increase our risk by presenting a monoculture to adversaries where a vulnerability in one would be the same vulnerability in all. For the VLAN question, the SDT notes that an ESP (a logical border) is required around every network

to which a BES Cyber System is connected and any external connectivity to other networks must be controlled with an Electronic Access Point (EAP). The SDT has chosen to not prescribe precisely what protective functions must reside on what devices or what the standard network architecture must be for the reasons noted above. A method for detecting malicious communication must be present at each EAP for control centers (high and medium impact).

Consideration of Data Diodes

One commenter stated that CIP-005-5 should consider data diodes which possibly would exempt systems only with a data diode connection from "external connectivity" provisions. In response, the SDT notes that the definition of 'External Routable Connectivity' includes the term 'bi-directional' in order to handle data diode situations that physically enforce a uni-directional flow. Therefore systems behind a data diode do not have External Routable Connectivity.

Requirement R1

One commenter asked what the rationale was for standalone networks that have no external connectivity to other networks to must have a defined ESP. The intent is to define the 'Associated Protected Cyber Assets (PCAs)' and the high watermarking concept. In response, in previous versions of the CIP standards, Cyber Assets on the same network (within the same ESP) with a Critical Cyber Asset had to meet the CIP-007-5 Requirements. The definition of an ESP in Version 5 is required to carry this same concept forward, as well as to handle the new issue of what level of protection is required for these Cyber Assets now that we can have multiple impact levels within the same ESP. Therefore, if a BES Cyber System is connected to a routable protocol network, even an isolated network, the ESP (which is simply the 'logical border') must be defined as that also defines the 'Associated Protected Cyber Assets'. All of these Cyber Assets within that ESP then become 'Associated PCAs' of the highest impact level BES Cyber System in the ESP.

A commenter stated that the definition of Electronic Security Perimeter allows the Responsible Entity to serially connect certain Cyber Assets to a communications processor that, in turn, communicates to other Cyber Assets using a routable protocol, and in doing so declare that the Digital Protective Control Devices do not need to reside within the ESP and therefore are not subject to CIP standards. In response, the SDT notes that connectivity is no longer a filter that kicks Cyber Assets out of scope and makes them 'no longer subject to the CIP standards'. Cyber Assets are subject to the CIP standards based on their functionality and resultant potential impact to BES reliability. It is true that certain Requirements, such as CIP-005 Requirement R1, only apply if a BES Cyber System is connected to a routable protocol network, but that is because its main point is to secure what can enter or leave routable protocol networks on which BES Cyber Systems reside. CIP-005-5 is no longer a 'scoping standard' for what is or is not in scope of the CIP standards as a whole as it has been in the past. BES Cyber Systems are in scope of the CIP standards. CIP-005-5 Requirement R1

therefore is now back to a network security Requirement that requires controlling what can enter or leave a routable protocol network.

There was a comment that requested clarification text added to the Guidelines and Technical Basis section for Requirement R1, specifically Requirement Parts 1.3 and 1.5, to remove the operational barriers that may prevent entities from implementation encryption among sites on a BES Cyber System network using either encrypted tunnels or tunnel-less encryption technologies. The commenter provided possible language to be added to CIP-005-5 Requirement Parts 1.3 and 1.5:

> "Some Entities employ encryption as a strong measure for securing communications among discrete physical sites (e.g. data centers and control centers). Encryption (either via encrypted tunnels or group encrypted transport) effectively satisfies the establishment of 'discrete Electronic Security Perimeters' as referenced in Section 4.2.3.2 of each Applicability section. Provided the termination points of the encryption are protected within Physical Security Perimeters, the Requirements for CIP-005-5 R1.3 (inbound & outbound access permissions and deny-by-default) and CIP-005-5 R1.5 (inbound & outbound malicious traffic inspection) may be achieved at central firewall(s) protecting the BES Cyber System network to which the ESPs are connected. For traffic communicating within the encrypted network, the CIP-005-5 R1.3 and CIP-005-5 R1.5 Requirements do not need to be duplicated at the encryption endpoints. This enables effective implementation of encryption, which might not otherwise be operationally feasible if traffic inspection were required inside of the protected network due to the latency and convergence delays that are introduced."

In response, The SDT believes the Requirements as written do not preclude the use of encryption. However, encryption alone does not constitute an ESP or EAP. For example, if malware is introduced via portable media to a BES Cyber System and it tries to communicate outbound to a command and control server to get further instructions or provide remote access to the BES Cyber System, the fact that there is an encrypted tunnel up to the next higher level site does not provide an EAP where the communications are inspected to determine whether they should be allowed or not. If an entity wishes to state that a wide area network of sites are within one ESP, regardless of encryption, then all Cyber Assets (which includes, e.g., all communication or networking equipment) within that very large ESP become associated PCAs and must meet the Requirements of the highest level BES Cyber System in the ESP. The standards do not preclude doing this, but there are implications that Responsible Entities should take into account.

For Requirement Part 1.2, one commenter stated that the definition of External Routable Connectivity does not anticipate a situation where serial protocol may be used over IP connectivity. The commenter provided an example, where communication between two devices may take advantage of the Ethernet ports on the devices, but run serial

protocol between the devices. Furthermore, the commenter stated that by explicitly stating, "routable protocol connection" in the definition and focusing an auditor's attention on the connection, the auditor may see the Ethernet port being used and determine noncompliance. Lastly, the commenter recommended deleting the word "connection" at the end of the definition of External Routable Connectivity. In response, the SDT disagrees. The definition is based on the type of protocol, not the transport used. Ethernet is not a routable protocol; it is a transport medium with no concept of network level addressing. It should not be assumed that transport determines protocol as routable protocols can be carried on serial lines and non-routable protocols can be carried on Ethernet. It is not a matter of transport but the protocol.

There was one suggestion in Requirement Part 1.3 that the term "permissions" can be substituted with the term "controls" to align the term with the language in the measure. In the measure, the SDT uses "access control list" as an example, and the SDT has not made a change to the Requirement language, as the use of "permissions" stems from prior versions of the CIP Cyber Security Standards. The SDT believes that the term is well-understood in this context.

One commenter had a concern with the phrase "outbound access permission" in Requirement Part 1.3 which calls for requiring inbound and outbound access permission, including the reason for granting access and denying all other access by default. The commenter furthered stated that target threat vectors to the BES Cyber Systems would be inbound to those networks and those attempts inbound into the networks need to be monitored and controlled, and that while there is the possibility that could be malicious code internal to these networks communicating, that tracking all outbound communication from one trusted network to another trusted network would more than double the monitoring that is required. In addition, the commenter stated that the CIP standards have other controls to help monitor and detect the malicious code internal to the networks. In response, the SDT does not think that having an outbound rule in an EAP that allows communication from all hosts on one internal network to all hosts on another internal network is burdensome. The benefit received of being alerted to BES Cyber Systems trying to suddenly communicate with unknown networks or hosts we believe outweighs the burden of such rules. The SDT is not prescribing the level of granularity of these rules. The intent is just that EAPs function as EAPs and don't have rule sets that allow a BES Cyber System to talk to any device in existence. The Requirement is in essence "you shall not blindly trust all hosts inside the ESP to talk to any device on earth". It is up to the entity how granular they control what the hosts inside the ESP can talk to. Some may go extremely granular and specify exactly what host can talk to what host over what port; some, due to the frequency of change or other reasons, may limit it to anything on this network can talk to anything on these other internal networks. Both are compliant. But BES Cyber Systems should probably not be able to communicate directly with all home PC's on the cable company's consumer broadband network or to any machine in unfriendly nations.

One commenter stated that Requirement Part 1.5 needed to include an explicit Requirement for real-time monitoring and/or alerting upon detection of known or suspected malicious communication. The SDT notes that monitoring and alerting is addressed in CIP-007-5, which also includes Electronic Access Control or Monitoring Systems (EACMS) (CIP-007-5, Requirement R4).

With regards to Requirement R1.5, one commenter proposed the following language: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. ESP-to-ESP communications within a discrete BES Cyber System shall be excluded." As an example, the communication links between a primary transmission control center and its backup control center shall be excluded. The SDT disagrees. If malicious code is trying to replicate itself from a primary control center to the backup Control Center, then this Requirement should be in place. Having both the primary and backup Control Centers compromised defeats the purpose. If the primary system is compromised via malware or remote control Trojans to the point that its integrity is gone and the entity needs to fail over to the backup while the primary is rebuilt, the backup needs this protection from the malware on the primary system. If the malware walked into the primary system via portable media or other means, an Intrusion Detection System (IDS)/ Intrusion Protection System (IPS) type system may save the backup system from compromise as well.

Another comment regarding Requirement Part 1.5 states that the Requirement is still geared towards implementing an IDS/IPS and that an IDS would not provide the additional protection for an ESP if a firewall failed. Also, the commenter noted that an IDS or IPS would provide no protection against an insider threat. The commenter closed by stating that “malicious” activity cannot be determined strictly by watching for an activity and that traffic to an ESP which is malicious may in fact appear to be normal. The qualification of “malicious” vs. “normal” requires knowing an actor’s intent, which cannot always be gleaned from log entries, traffic patterns or signatures. In response, the SDT has invested many hours in these very discussions and has arrived at the current Requirement. The Order makes it clear that the alternate control is also not simply another firewall. Having two firewalls in sequence would provide no value as the rule sets would be identical. The solution the SDT arrived at for an alternate control at an EAP was to detect malicious traffic (usually implemented in today’s technology via IDS/IPS as noted, but not prescribed). This would allow that if the firewall was misconfigured (e.g. an admin puts in a temporary any/any/all rule for troubleshooting and forgets to remove it after testing) then at least there would be this alternate control looking for malicious traffic and providing some means of protection which the SDT believes is the intent of the Order. As to the issue with “malicious” implying knowledge of an

actor's intent, the SDT has responded to this in previous drafts by inserting the words "known or suspected" to clarify that it is only malicious traffic that is previously known or suspected to be malicious.

Relating to requiring IDS and IPS to have firewalls, one commenter stated that it may be onerous compared to the benefit received. In response, the SDT disagrees. The SDT has already scoped this Requirement to the highest impact BES Cyber Systems which should be subject to the more stringent Requirements. The SDT believes that the benefit received from detecting malicious communications into and out of control centers far outweighs the burden.

One commenter asked for SDT clarification related to the ESP, External Routable Connectivity, and whether serially connected Cyber Assets are within scope for Requirements applicable to BES Cyber Systems with External Routable Connectivity. The SDT confirms that all BES Cyber Assets are in scope of all the CIP Version 5 standards. However, for certain Requirements, the type of connectivity limits applicability. EAPs for example, are only required around routable protocol networks to control what can get into and out of these networks. There is no EAP for a serial connection if there is no routable protocol running over it. Note that it is protocol based, not transport based. Routable protocols can run over serial transports. The same holds true for ERC – it is routable protocol based.

Requirement R1 VSLs

There was a comment that the language in the VSL should match the same language and logic as in Requirement R2. An example was provided that, the Responsible Entity should have a low VSL for not having a sub-part in its documented process, medium for not implementing one of the applicable items, high for not implementing two applicable items and severe for not implementing three applicable items, and thus, would result in a more consistent application throughout the standard. The SDT notes that it modified the VSLs for Requirement R1 in response to comments from draft 2 because of the difficulties and impracticalities of determining the measurements for graduated VSLs for Requirement R1.

Requirement R2

There was a clarification request for Requirment Part 2.2 with regards to allowing that encryption may be terminated at a firewall that protects an Intermediate Device in additoin to the Intermediate Device itself. The SDT believes that the definition of Intermediate Device provides sufficient flexibility in implementation to allow for what the commenter had requested. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. CIP-007-5 Requirement Part 5.1 refers to all user authentication; whereas CIP-005-5 Requirement Part 2 only refers to remote access.

There was a request that "where technically feasible" be added to Requirement Parts 2.2 and 2.3. The language "where technically feasible" is included in the overarching Requirement R2 to recognize that this applies to all of the Requirement Parts contained in Requirement R2, not just Requirement Parts 2.2 and 2.3.

Several commenters stated that CIP-005-5 Requirement Part 2.1 be modified to address situations where the Intermediate Device can be locally accessed (a local administrator, for example) inside the PSP. The SDT believes that, as currently written, the Requirement provides the level of protection necessary in that the Intermediate Device cannot be within an ESP and thus provides the necessary protection of the Cyber Assets within the ESP. The remaining controls for the Intermediate Device(s) provide a defense-in-depth proteciton of those systems. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter considered that CIP-005-5 Requirement Part 2.2 does not achieve the intention, which is to have traffic inspected by the IDS in an unencrypted state. The SDT notes that, as written, the Requirement and definition of Intermediate Device, collectively; provide sufficient flexibility in implementation to allow for what the commenter has noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 regarding the protections to be afforded to an "Intermediate Device". Per the definitions of Intermediate Device and Electronic Access Control or Monitoring Systems, these devices are subject to the protection of EACMS.

There was a request for clarification of CIP-005-5 Requirement Part 2.2 as to the reasonableness to include traffic between the "Intermediate Device " and device(s) within the ESP to be in scope of CIP, as it traverses an EAP. Many instances of Interactive Remote Access originate from systems that are not within a trusted network or across the

Internet. The encryption is required to terminate before going into the ESP through an EAP. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that CIP-005-5 Requirement Part 2.2 be modified as "Interactive Remote Access sessions must utilize encryption to an Intermediate Device." The SDT believes that, as written, the Requirement language achieves the same concept and result.

A recommendation was made that CIP-005-5 Requirement Part 2.3 is modified as "Interactive Remote Access sessions must utilize multifactor authentication to an Intermediate Device." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

A request for clarification was made of CIP-005-5 Requirement Part 2.2 regarding whether the "Intermediate Device" is expected to provide the encryption or if two devices are envisioned for compliance. The SDT believes that, as written, Requirement and definition of Intermediate Device, collectively, provide sufficient flexibility in implementation to allow for what the commenters have noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.3 on whether the multi-factor authentication is required for the Intermediate Device, for access to the EAP or to the individual Applicable Systems. The commenter suggested the language to read "Require multi-factor authentication for initiating all Interactive Remote Access Sessions." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 on whether VPN is an acceptable form of remote access. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There

are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

CIP-006-5

General

There were comments that CIP-006-5 does not require an entity to define a Physical Security Perimeter (PSP) and wonders if entities must assume that it is required. In response, the SDT notes that access points to the PSP must be controlled, which by definition, requires the PSP. It is not necessary to have an additional Requirement stating the existence of a PSP.

Background Section

One commenter stated that the background section includes a definition/description of "Medium Impact BES Cyber Systems with External Routable Connectivity," that notes an exclusion in the following sentence: "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." When this definition/description of Cyber Systems is used for the applicability in Requirements such as CIP-006-5 Requirement Parts 1.2, 1.4, and 1.5, it is used with the added inclusion of "and their associated...PCA." It appears the inclusive "and associated PCAs" statements in the Requirements negate the exclusion statement from the "Background," and makes the intended applicability of such physical security Requirements to specific Cyber Assets unclear for Cyber Assets without direct external connectivity which reside in the same ESP as Cyber Assets with direct external connectivity. In response, the exclusion in the background section states that it only applies to those Cyber Assets which are part of the BES Cyber System and not PCAs.

Requirement R1

One commenter stated that the deficiency correction language should not be added to CIP-006-5 Requirement R1 because it is a binary Requirement to either have a plan or not. The SDT notes that while the possession of a plan is binary, the implementation is not. Entities must document a plan with all of the applicable table parts and implement the plan at applicable BES Cyber Systems.

One commenter noted that the term "BES Cyber Systems without External Routable Connectivity" should be just "BES Cyber Systems". The SDT notes that "without External Routable Connectivity" is used to distinguish lesser obligations than those applying to "BES Cyber Systems WITH External Routable Connectivity".

Several commenters stated that CIP-006-5 Requirement R1 does not answer the question of how big an opening needs to be before it is considered an access point. In response, the SDT does not agree this question needs to be answered in a

standard's Requirement. This is an implementation-specific question. An entity may choose 96 square inches as its general measure, but that should not be the Requirement. Specifying exactly the qualifications of an access point would go beyond just the 96 square inch Requirement and likely cause significantly more confusion than currently exists.

One commenter did not agree Requirement Part 1.3 is responsive to the directive in FERC Order No. 706, Paragraph 573 to provide layered and complementary security procedures. In response, the SDT notes that in paragraph 575, the Commission specifically states it was not the intent to create an inflexible rule of redundant access control. The proposed Requirement meets the objective of having multiple physical access control measures. The Cyber Asset independence of these measures is not material to meeting the directive.

More than one commenter argued that Requirement Part 1.3 presents technical challenges without any additional security benefit. They request NERC to provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. In response, the SDT is addressing the directive in FERC Order No. 706, Paragraph 572. The SDT believes the proposed wording provides the most security benefit to the industry while still meeting the FERC directive.

One commenter suggested that for Requirement Parts 1.5 and 1.7 to remove the 15 minute maximum timeframe limit for issuing an alert. In response, the SDT notes that for physical security breaches, the threat is automatically severe and immediate and the 15 minute timeframe is necessary to provide a minimum expectation for issuing an alert.

One commenter proposed the words "of the unauthorized access" should be added to the end of Requirement Parts 1.5 and 1.7, but this would be redundant since detection is already qualified singularly in the Requirement Part.

There was a request for clarification if monitoring is needed on PACS inside a PSP according to part 1.7. In reviewing the possibility of combining Requirement Parts 1.5 and 1.7, the SDT found that monitoring and alerting Requirements applying to PACs could be interpreted to mean those inside a PSP. To clarify, the SDT notes that entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

One commenter stated that in Requirement Parts 1.5 and 1.7, BES Cyber Security Incident Response Plan is not a defined term and should not be capitalized. The SDT agrees and has made this change. Furthermore, the commenter noted that unauthorized physical access should not automatically trigger the incident response plan because the physical security

team and incident response team are often separate groups, and a single instance of a detection of unauthorized physical access is not necessarily a Cyber Security Incident. The SDT notes that an attempt to compromise the PSP is by definition a Cyber Security Incident, and the organization of physical security and incident response teams should not preclude the Requirement to identify the Cyber Security Incident. The physical security team's response to unauthorized physical access could be part of the organization's incident response plan.

Several commenters stated that Requirement Part 1.7 should be modified to require response within 15 minutes of the detection rather than the actual incident, consistent with Requirement Part 1.5. The SDT agrees and has made the clarification.

One commenter proposed that Requirement Parts 1.5 and 1.7 be combined because they use similar wording, but the SDT believes entities benefit by emphasizing the applicability to PACS outside of the PSP.

There was a comment that stated that Requirement Parts 1.6 and 1.7 should include badge readers outside of the PSP and access cannot be controlled as specified. In response, these Requirement Parts are separated because they must be monitored differently than those Cyber Assets inside a PSP. The SDT also notes that badge readers, by themselves are not necessarily considered PACS if they do not control the controlling, logging or alerting of access.

One commenter noted that a responsible entity needs to monitor each PACS system for unauthorized physical access to a PACS. However, there is no Requirement that the PACS be contained within a PSP. Therefore, a question was raised as to how does one control physical access to the PACS? In response, the SDT notes that PACS must control access according to Requirement Part 1.1, which is not the same level as Requirement Parts 1.2 through 1.5, but some form of access control must still exist for the entity.

Several commenters noted that Requirement Part 1.7 requires coordination with the incident response team, but CIP-008-5 does not apply to PACS. In response, the incident response plan does not apply to individual Cyber Assets, but compromise of a PSP and associated PACS is by definition a Cyber Security Incident affecting a BES Cyber System.

One commenter requested clarification on whether the issuance of an alert according to Requirement Parts 1.5 and 1.7 is automated, manual, or by choice. The SDT clarifies this is by choice of the entity.

There was a suggestion that there is a discrepancy between the change description stating PACS does not need to be inside a PSP and Requirement Parts 1.5 and 1.7 stating obligations for monitoring and alerting for unauthorized access to PACS. In response, Requirement Parts 1.2 through 1.5 applies to the BES Cyber System. PACS have a less stringent obligation in Requirement Part 1.1 to have a plan for restricting unauthorized access, but this is not the same obligation as having a PSP. The SDT has clarified the change rationale for Requirement Part 1.1.

One commenter stated that Requirement Part 1.8 should add "initial" before entry to align with the visitor control program. In response, the situation allowed for in the visitor control program is to avoid an escort continually signing in a visitor needing to perform a maintenance activity. This is not the same concern for authorized personnel who typically badge in each time without the overhead of an escort.

One commenter stated that Requirement Part 1.9 should be moved to data retention. In response, the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R2

There was a comment that the CIP Exceptional Circumstances should be removed since it applies globally at a policy level. In response, the CIP Exceptional Circumstance provision is controlled at a policy level but does not apply globally to all Requirements in the standard. The standards specify which Requirements the exception may apply to as a response to the FERC Order No. 706 beginning with paragraph 372, which directs additional guidance on policy exceptions.

Several comments stated that the Requirement could allow a visitor to go a long span of time without signing out. In response, the SDT notes the scenario of brief exit/entry intervals provided in comments is the purpose for allowing this provision. Specifying what timeframe constitutes the necessity of an exit sign-out goes beyond the security benefit provided by this Requirement Part.

Several commenters noted that the measure in Requirement Part 2.1 does not match the Requirement because the evidence does not demonstrate continuous access but discrete points in time. In response, the Requirement to have a program that provides continuous escorted visitor access can be measured by the program document. Evidence of compliance with the procedure requires discrete sampling to provide assurance in the implementation of the program.

One comment was that Requirement Part 2.2 would require manual or automated logging of entry and exit from the physical security perimeter and the Requirement for egress has not been explicitly defined as a Requirement. In response, egress logging has been required since CIP-006-3.

There was a comment that Requirement Part 2.3 should be moved to data retention. In response, R2.3 was not included as an evidentiary requirement. The SDT notes that the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R3

One commenter stated that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One comment was that the 24 month interval in Requirement Part 3.1 is excessive for a normally occupied control center. In response, a normally occupied control center would also receive a significant amount of testing in the operation of access control. The objective this Requirement primarily addresses field assets where access is not tested as frequently, and the timeframe is appropriate for these assets.

Guidelines and Technical Basis

Several commenters recommended modifying the section dealing with alarms to be from “immediately after” an incident to “within 15 minutes.” This better aligns with the Requirement and the SDT agrees.

CIP-007-5

General Comments

One commenter requested guidance on how to comply with CIP-007-5 Requirements on Medium BES Cyber Systems serially connected devices with regards to patching, anti-virus, etc. on a large number of programmable protective relays; and also why other measures implemented for substation assets, such as physical protection, are not adequate. In response, the SDT notes that BES Cyber Assets by definition can have an impact on BES reliability and therefore require basic cyber security protections offered by CIP-007-5 regardless of their connectivity. For patch management, the intent is that entities know about the security patches that are available for their BES Cyber Assets, what vulnerabilities they represent, and mitigate those vulnerabilities. If a security patch for a device is only exploitable over a routable protocol connection and the device is only attached serially with non-routable protocols, then that patch would be documented as not applicable. The anti-virus Requirements and guidance already mention that the entity is to document and implement how they protect against the introduction of malicious code to the BES Cyber System. For some of the devices in the example, the entity may document that there is no method to introduce malicious code.

Effective Dates

One commenter raised a concern that the effective date of the order providing applicable regulatory approval, and Requirement Part 5.2 shall become effective 12 months later, as to provide entities more time to identify and inventory all enabled default or other generic account types. In response, it is the intent of the SDT that the entity has the accounts inventoried on the effective date, not one year later. That is why there is a two to three year implementation period so that all these prerequisite activities have sufficient time to be completed so that the entity is fully compliant on the effective date. The Requirements that require periodic reviews may have their first performance take place after the effective date, but that is outlined in the implementation plan.

Requirement R1

One comment stated that a new term of “Control Center Environment” was introduced in this standard and it could potentially have a different meaning than “Control Center”. The commenter requested clarification, and in response, the SDT agrees and has changed the term to “Control Center.”

For CIP-007-5 Requirement Part 1.2, several questions were asked about the phrase, “Protect against the use of unnecessary physical input/output (I/O) ports used for network connectivity, console commands, or removable media.” Introduction of physical port protection is “assumed” to refer to logical ports only. First, a question was raised about

strong physical access controls to BES Cyber System be a compensating control here. Second, will having the BES cyber systems in locked cabinets suffice? The Requirement is not clear if the protection has to be on the individual devices. The measures indicate signage as a potential control however this would not satisfy the Requirement the way the Requirement is written. For CIP-007-5 Requirement Part 1.2, the commenter sought clarification regarding physical I/O ports that are externally accessible. For example, most servers have PCI slots, CPU slots, memory slots, etc, which are physical I/O ports. As the standard is currently written, it would seem organizations need to disable these ports. Additionally, the language "console commands" is too ambiguous. In response, the SDT notes that many of these issues are addressed in the included guidance. FERC has stated that the PSP does not meet the intent of their Order. The SDT agrees with the 'console commands' comment and has added additional guidance to address it.

For CIP-007-5 Requirement Part 1.1, several comments were made about the phrase, ""If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed." The Requirement does not provide any provisions for limiting access to those ports or services that cannot be disabled. The Requirement's measures ask for host-based protective measures. For those devices that are not capable of providing localized protective measures, such as relays, there is a question as to how this Requirement would be met. Previously, when a port or service could not be disabled, a TFE would require mitigation of the potential vulnerability. Under CIP-007-5, if the entity leaves these ports and services open they are in compliance but there is a question of whether the vulnerability of the device still remains. In response, the SDT notes that the Requirement does provide provision for those ports and services that cannot be disabled which is the phrase in question. If a device has no provision for disabling or restricting the ports, they are deemed "needed" and the Requirement only requires "unneeded" ports to be disabled. The intent is to not require TFEs for devices where the device does not allow for the Requirement to be met. The Requirements in CIP-005-5 for limiting inbound and outbound communications at the ESP is a mitigating factor for devices like this that do not allow for their "unneeded" ports to be disabled.

Requirement R2

There was one comment that stated the rationale specified a 30 day time frame while the Requirement states 35 days. The commenter requested that the rationale section be revised for consistency with the Requirement language. In response, the SDT agrees and has changed the rationale to 35 days to agree with the Requirement.

One commenter suggested adding "with External Routable Connectivity" to the Medium Impact applicability for the patch management Requirements within Requirement Parts 2.1 through 2.4. As justification, the commenter stated that they understand the comments of the SDT; however, the commenter believes that a combination of no external routable

connectivity, frequency of access to medium impact facilities, and policies reduces the risks to those facilities from the insider that would introduce threats ("thumb drives, laptops, smart phones") into the environment to an acceptable level. While devices with no external connectivity may have some physical access risks associated with the use of thumb drives, laptops, etc., the fact that they are isolated from other BES devices must be considered when addressing appropriate protections. The lack of external connectivity reduces the risks to that isolated device; therefore, the risk to the BES is minimal. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. Alternatively, a request was made that the timeframes for Requirement Parts 2.2 and 2.3 be revised to 90 days for Medium Impact BES Cyber Systems. In response, while routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means in which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable. As to the 90 day alternative, the SDT believes that a timely analysis and plan are necessary due to the nature of the environment we are in where 'Patch Tuesday' is immediately followed by 'Exploit Wednesday' as attackers quickly reverse engineer released security patches to create and release exploit code. The SDT has not put a maximum timeframe on implementation due to numerous reliability concerns, but the analysis and mitigation planning needs to occur in a timely fashion.

There was a comment that Requirement Part 2.1 requires the Responsible Entity to identify a source or sources that the entity will track for the release of cyber security patches. Furthermore, the commenter stated, *"the corresponding guidance suggests that the third-party SCADA system vendor is an appropriate source for patch availability notification. The ability of a Responsible Entity to wait until a SCADA system vendor "certifies" a patch before requiring the Responsible Entity to begin the assessment and follow-on patching process introduces unnecessary risk to the BES. There is a significant difference between assessing a patch for applicability and assessing a patch for installability. An applicable patch may be found to be incompatible with the third-party vendor's systems, would not be certified, and should not be installed. That does not mean the vulnerability being addressed by the patch should not be mitigated, rather it is incumbent upon the Responsible Entity to protect its systems in a timely manner. The Responsible Entity needs to select a patch availability source that is timely, including the original patch provider and well recognized general information providers like US-CERT, SANS @Risk, and nCircle. There is no harm in then waiting for the SCADA vendor to certify the patch before installing it, but the Responsible Entity is at least aware of the vulnerability, can assess the risk, and take*

appropriate interim action." In response, the SDT agrees with the concept; however, the SDT does not find it appropriate to prescribe in regulation certain 'timely' sources, including private firms, that must be used. Patch monitoring services can come and go. The SDT also believes that it should not use undefined terms such as 'timely' in a mandatory Requirement, nor should it define 'timely' as it refers to the seemingly unlimited number of patch sources that will exist with the significantly expanded scope of Version 5. The SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan.

For CIP-007-5 Requirement 2, part 2.1, a comment was made that the patch management process for substation or plant control systems could include security patches for Cyber Assets such as panel meters, relays, controllers, Programmable Logical Control (PLCs), and other electronic devices that are part of the BES Cyber System and do not have network connectivity. In response, the SDT agrees that any Cyber Asset that meets the definition of BES Cyber Asset is included in the CIP-007-5 patch management Requirement regardless of connectivity and that is the intent. While routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means by which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable.

One commenter requested a definition in Requirement Part 2.1 for the phrase "applicable asset," and also suggested that the phrase "Applicable Cyber Asset" should be called "Applicable System" to align with wording in the column "Applicable Systems". In response, the SDT notes that individual BES Cyber Assets have patches, not systems of Cyber Assets. A system is a logical grouping of one or more BES Cyber Assets. While the applicability is at the system level, the Requirement is to perform patch management on all of the applicable BES Cyber Assets within those applicable systems.

There was a comment made on the change from 30 days to 35 days within Requirement Part 2.2. The comment was that this change allows utilities to manage patches monthly while coinciding with vendor releases, all without running into

issues of the Requirement being less than a full month. However, the commenter stated that this should be extended to 40 days to accommodate time to review the vendor releases, and that the additional five days on top of the existing 35 days will ensure that those utilities with patch management programs are not penalized due to variations in patch release dates from month to month. In response, the intent is for a process that approximates "monthly" and the SDT has already added in at least a four period to account for holidays, weekends, and other factors. The SDT does not agree that it needs further extension. Timely analysis of security patches is the goal.

Within Requirement Parts 2.2 and 2.3, one commenter requested clarification of the use of term "mitigation plan" and how it would provide value. To clarify Requirement Part 2.2 the commenter suggested mentioning that the mitigation plan is intended as an internal document and not submitted to the RE. In response, the SDT agrees and that these plans are internal documents and not submitted to the RE. In previous drafts, these were called 'remediation plans' and the SDT received comments that this term was used for what was submitted to Regional Entities in response to violations of the standard, so the SDT changed the term to 'mitigation plan' to avoid that confusion. The SDT has added this clarification to the guidance.

There was a comment with regard to CIP-007-5 Requirement Part 2.3 that reads, "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to "create a dated mitigation plan or revise an existing mitigation plan will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to "Develop dated implementation plan" without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability." In response, the SDT notes that the 'dated mitigation plan' could simply consist of the date the entity plans to implement the security patch if beyond the initial 35 day period; therefore it is not simply a paperwork exercise that provides no reliability benefit. The intent of the Requirement is to mitigate the applicable vulnerabilities either through the installation of the patch or by some other means. Implementation of the patch is mitigation and having a record of the entity's plan to implement the patch is not seen as unnecessary paperwork.

There was a comment that Requirement Part 2.3 requires the Responsible Entity to either install the patch within 35 calendar days or simply create or update a mitigation plan. Furthermore, the commenter stated "there are no boundaries of what is acceptable in a mitigation plan, no expectation of justifying the decision, and no Requirement for

the CIP Senior Manager approval, thus allowing an entity to completely avoid the Requirement to patch a critical system by creating an illogical plan with unreasonable milestone dates. The need to wait for a scheduled outage at a field asset is well understood. Allowing an entity to determine patches will only be installed when the control center server is replaced (typically every four years), as has been seen during a CIP audit, is unreasonable and poses significant risk to the reliability of the BES. This Requirement does not require compensating measures appropriate to the vulnerability to be put into place until the patch is installed, thus furthering the potential risk. In effect, the provisions of this Requirement have the potential of creating a paper exercise with little value, with an expectation that the CIP auditor simply accept the documented plan without comment. (3) Requirement Part 2.4 furthers the inaction of the Responsible Entity by requiring the entity to follow the potentially illogical plan that the entity designed to avoid having to patch in the first place. As long as an extension of the plan is not required, there is still no CIP Senior Manager or delegate approval required." In response, the SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan. The SDT has no way to write a mandatory Requirement for a "logical" plan.

One commenter believes that the language in Requirement Part 2.4 be aligned with the language in Requirement Part 2.3. The commenter suggests that either both or neither should specify the approval Requirement of the CIP Senior Manager of delegate. The commenter recommends that the language of "…timeframe specified in Requirement Part 2.3 is approved" be added. In response, the SDT notes the CIP Senior Manager approval was added to Requirement Part 2.4 specifically to handle situations where entities might repeatedly extend their documented timeframe with no management oversight. The intent was not to have management approval of every patch in normal day-to-day processes. Entities are free to do so, but it was not the SDT's intent to make that a mandatory Requirement. Management approval of every patch on every BES Cyber Asset would tend to become a "rubber stamp" with no meaning. The SDT's intent was to have approval of exceptions so that if someone were simply moving deadlines to avoid complying with the intent of the Requirement it would be subject to management oversight.

Requirement R3

There was a comment that within Requirement Part 3.1 to consider adding the phrase "per device capability" to the beginning of the Requirement, or otherwise, if a deter posture is selected, it may be potentially in conflict with other

Requirements. In response, the Requirement is written at the system level in order to handle the device-specific issues. The SDT believes the included guidance also provides suggestions on how to handle device abilities.

With regard to CIP-007-5 Requirement 3, parts 3.1, 3.2, and 3.3, there was a comment that these three Requirement Parts do not have any timeline for action. A question was raised if an auditor will audit when the activity occurred and audit only that a process is created and executed per the registered entities process or procedure. In response, the answer to the question is yes. Malware protection is an inexact art as we are protecting against an intelligent and always changing adversary. Malware of today is quite different than malware of just a few years ago. The intent is for entities to think about the malware problem, document what they are doing about it for each BES Cyber System, and then do it. Prescribing certain technologies/tools/timeframes is not helpful in this rapidly changing area and tends to bog the industry and the regulator down in paperwork (such as TFEs) when agility in this area is required in order to protect BES reliability.

Within Requirement Part 3.2, one commenter stated that the word 'identified' is ambiguous and inconsistent with other malicious code phrases, and the commenter suggested changing the language to 'detected'. The SDT agrees with this clarification and has made the suggested change as this is how the measures and guidance were written as well.

One comment was related to the applicability section of Requirement Part 3.2. A suggestion was provided to revise this section to apply to Medium Impact assets with external routable protocol to read: "Medium Impact BES Cyber Systems with external routable protocol and their associated". In response, the SDT's intent is for the basic security protections, including malware prevention, to be applied to all BES Cyber Systems not just those with External Routable Connectivity. BES Reliability can be threatened on isolated networks of BES Cyber Systems through the introduction of malware through portable media or laptops used for support.

One commenter requested clarification on Requirement Part 3.3 which requires the anti-malware updating process to address testing of the signature or pattern file. In support of this request, the commenter stated that a number of registered entities have taken the position in the past that they address this aspect of the existing CIP Version 3 Requirement by relying upon the vendor to test before release. In response, the Requirement is taken verbatim from previous industry and FERC approved versions of the CIP standards. If the entity is obtaining tested signature updates from their control system vendor for a turnkey product, then that is compliant. The SDT does not think more prescription as to where the testing must occur is needed.

There was one comment raised that use of the term 'deter' is ambiguous and the commenter suggested replacing this language in Requirement Part 3.2. The commenter suggested replacing the language to read: "Configure the measures implemented in Requirement Part 3.1 such that it blocks or prevents access to files with potentially harmful code." This recommendation was based on the assumption that the recommendation for removal of the term "deter" is accepted in Requirement Part 3.1. In response, the SDT has purposefully added the word 'deter' so that entities are not in immediate violation of the Requirement should zero day malicious code enter the environment. There are no 100% preventions, so the SDT has added this verb to allow for that. Antivirus software tools today do deter, but do not 100% prevent.

Requirement R4

One commenter requested clarification around the last two sentences of the guidance section. The commenter also stated that currently, an entity that neglects to enable logging would be in violation. Per the Background section, a sole instance of deficiency is not grounds for a violation so long as it is adequately identified, assessed, and corrected. The statements in the guidelines seem to be relics of a previous draft which conflict with the new approach. In response, the SDT agrees and has rewritten the guidance to properly align with the Requirement.

One comment read that CIP-007-5 Requirement R4 for security event monitoring does not state any Requirements as to when the security events, particularly in Requirement Parts 4.1 (log events) and 4.2 (event alerts) are to reviewed, escalated, and mitigated. A question followed that asked if there are any Requirements for immediate action from the IT security personnel for detected failed access attempts, failed login attempts, or specific event alerts. In response, no, there are no prescriptive timeframes for response to alerts. The Requirement is to generate an alert for security events. Alerting someone to a condition is one thing, responding to the condition is dependent upon numerous variables that cannot be prescribed.

A recommendation was made to revise this Requirement to include the sentence from the guidance section, "that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment." The SDT's intent was not for the Responsible Entity to determine in totality the events to be logged, but that it must log the listed events at a minimum (subject to device capability). The Responsible Entity is free to log events above and beyond these and is encouraged to do so. However, the Responsible Entity cannot ignore the listed events.

As currently written, CIP-007-5 Requirement Part 4.1 would necessitate the logging at every Cyber Asset that is capable when there is not a network at the BES Cyber System. A suggestion was made to rewrite this Requirement to read, "for BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol, log events at the BES Cyber System Level…" In response, the SDT's intent is that if a Cyber Asset has a local log on the device, then it should be utilized. For example, a completely standalone and isolated substation relay should log security events internally if it is capable of such so that if it begins misoperating there is some log to go review on the device to see if/who/when someone has accessed it. The Requirement is not dependent on external connectivity.

In Requirement Part 4.3, one commenter suggested that this is a data retention Requirement and should not be a Requirement of the standard. In response, the SDT's intent is that this is not strictly 'data retention for the purposes of audit' Requirement, but an actual cyber security Requirement to have ready access to the past 90 days of logs for the applicable systems for quick determination of potential cyber causes of reliability-affecting events. Quickly determining whether a BES event could have had a cyber security cause is a reliability-focused Requirement and the primary way to do that is to have ready access to security event logs. Configuring a system to retain the past five minutes of security event logs is of little to no value. This is a separate issue from having evidence for audits that you maintained 90 days of logs throughout the audit period.

Within the Guidelines and Technical Basis section of CIP-007-5, Requirement R4, a question was asked if the following quotation references to NIST are the guiding principles and documentation for the development of the RSAWs and auditing of this Requirement, "Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring." In response, these guidelines are not auditable, only Requirement statements are auditable. These are provided solely for use at the discretion of Responsible Entities, several of whom have asked in previous drafts for further guidance.

One commenter requested clarification on the word "review" with regard to the statement within Requirement Part 4.4 of "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents." The commenter questioned if an automated SIEM technology solution, which monitors real-time, would satisfy the Requirement. In response, the SDT states that the intent, as per FERC Order No. 706, is to manually review the logged events in order to ensure that automated tools such as SIEM systems are tuned appropriately and are not missing security events.

One commenter stated that CIP-007-5, Requirement R4, part 4.1.2 calls out failed access attempts and failed login attempts and is unclear as to why the phrases "failed access attempts" and "failed login attempts" are separated. The

commenter requested clarification on the following two questions: Are “failed access attempts” referring to physical attempts, and are they referring to some other form of electronic access to undermine the login process? In response, the SDT notes that as outlined in the guidance, access attempts primarily occur at EAPs and involve ‘access’ across the ESP. Login attempts primarily occur at the BES Cyber Systems. The monitoring Requirement applies to both situations.

A comment was issued on Requirement Part 4.1.3 that this Requirement of malicious code prevention methods to log is already contained in Requirement Part 3.2. The commenter suggested removing this Requirement. In response, the SDT notes that logging and alerting when malicious code is detected is a separate Requirement from the actual response to the alert and the mitigation of the malicious code on the BES Cyber System. The SDT sees no duplication between these Requirements.

There was a comment that within CIP-007-5 Requirement Parts 4.2 through 4.4 the Requirements and sub Requirements have become less clear than previous CIP standards versions. The commenter stated it was unclear if Requirement Part 4.4 replaces the previous monitoring Requirements in their entirety or if it represents an additional manual sampling action that occurs outside of a primary monitoring process which may be automated. The commenter suggested to consider modifying the aforementioned Requirements to make it clear to registered entities which logging is required, how logs should be monitored, and what actions are required in the event of an interruption in logging. In response, the SDT notes that Requirement Part 4.4, as noted in the Rationale and Change Justification, is in response to FERC Order No. 706 and the Directive to require a manual review of logs to insure that automated tools are not missing events. Automated tools are only as good as their rule sets, which require periodic tuning.

One commenter noted that a clarification may be needed for Requirement Part 4.2 as to whether the alert needs to be generated real-time with automatic notification or if the alert can be generated by a long after-the-fact manual review of security event logs. In response, the SDT’s intent is, in general, for a real-time alert, but the SDT did not specify that as a timeframe in the Requirement because, for example, an after-the-fact review or analysis of logs would not require a computer-generated alert.

One commenter stated that Requirement Part 4.2 is a questionable and subjective Requirement as it states that an entity needs to generate alerts for security events that the entity determines necessary. In response, the SDT has set a minimum threshold of alerts that must be generated if the system is capable of it. All other types of alerts vary widely by the type of system in question and should not be prescribed. The alerts that can be generated by a Windows or Unix

server in a data center are quite different than what can be generated by some legacy purpose-built device in a substation.

A request was made to clarify Requirement Part 4.3 as to whether original source logs must be retained or if post-log analysis summaries are sufficient. In response, the SDT states that the language in the Requirement and measure provides the necessary level of clarity.

There were several comments on Requirement Part 4.4 that need to be clarified that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. The purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. Similarly, another comment for CIP 007-5, R4.4 read, in the Requirements column of the table, the draft language indicates a need to review logs to, "identify undetected Cyber Security Incidents." A question was raised if this is intended to be "identify detected Cyber Security Incidents?" Also for CIP-007-5 Requirement Part 4.4, a recommendation was made to change "undetected" to "potential". In response to the aforementioned comments, the SDT notes the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

One comment read that in Requirement Part 4.4, to be consistent with other Requirements, that the phrase "15 days" be changed to "15 calendar days." In response, the SDT agrees with this clarification and has made the change.

A recommendation was provided to change the language in Requirement Part 4.2 to read "Detected failed login attempts from part 4.1." In response, the SDTs intent is that alerts be generated when it is detected that event logging has failed.

One commenter raised an issue that in Requirement Part 4.4 the words "summarization" and "sampling" components are too broad. In support of this, the commenter encouraged specificity in all measures. Additionally, the term "undetected" is unclear and confusing. The commenter stated that clarification, such as "logged but not previously selected for alerting or alarming" could be helpful. In response, the SDT has chosen to not provide further prescription but to use the words from FERC Order No. 706 to allow entities to meet the intent without prescribing exactly how to summarize or sample

the logs. Sufficient summaries or samples are dependent on many variables and do not lend themselves to a one-size-fits-all approach.

A comment was made with regard to Requirement Part 4.4 that a manual log review is a labor intensive and outdated approach. The technical guidance should allow for use of network behavior analysis or other automated review processes for this Requirement. The commenter believes that this Requirement is ambiguous. The commenter further stated that the Requirement to review 'undetected' Cyber Security Incidents is essentially a Requirement to perform manual reviews. By requiring a manual review, the entities are encouraged to record the absolute minimum event types as to minimize the burden of the manual review. Further, the Requirement to perform manual reviews would incentivize entities to not invest in systems that can perform automated log analysis and event correlation. In response, the SDT has added this Requirement in response to a directive in a FERC Order. The intent is to ensure that such automated tools are continually tuned and are not missing events that should be caught and alerted on.

A request was made to clarify Requirement Part 4.4 that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. Furthermore, the commenter stated that the purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. With regards to the Requirement column of the table for Requirement Part 4.4, the draft language indicates a need to review logs to "identify undetected Cyber Security Incidents". Is this intended to "identify detected Cyber Security Incidents"? One last comment was a suggestion to change the word "undetected" to "potential". In response, the SDT states that the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

Requirement R5

There was a comment that the TFE language in CIP-007-5 Requirement Part 5.6 is unnecessary since technical or procedural controls can be used and that the phrase "per Cyber Asset capability" be used instead. In response, since many Cyber Assets used today utilize shared accounts and have no capability for individual accounts, periodically changing passwords is necessary. The SDT is aware that some systems have passwords that cannot be changed, or that if changed will break the system's functionality. Therefore, the SDT allowed for TFE's since the entity may not be able to

change the password either technically or procedurally. The SDT chose not to use the 'per Cyber Asset capability' as this is an instance where documenting and implementing some alternative control is necessary.

Within the Rationale section of CIP-007-5 Requirement R5, there was a suggestion to add the phrase “mimic display” to the second paragraph which outlines what is not included in interactive user access. In response, the SDT disagrees because the definition agreed to by the SDT is very clear and by adding another example with a non-widely used term would not add further clarity.

One commenter asked how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. The commenter stated that both appear to require authentication of Interactive Remote Access sessions. In response, CIP-007-5 Requirement Part 5.1 refers to any user access, including local access while physically present at the device. CIP-005-5 Requirement Part 2.3 refers to remote access.

A commenter believes that including specific password Requirements within a standard is contrary to new and safer technologies by the industry. In response, the SDT notes that the password Requirements have been worded in such a way that they only apply if passwords are used for authentication. If other, stronger means of authentication are used (tokens, biometrics, etc.) then the password Requirements do not apply. The Requirements are only “for password only authentication”.

One commenter stated that the term “generic account types” used in Requirement Part 5.2 is not defined and has not been well understood by entities to date. In response, the SDT notes that the term is now “default or generic” and the guidance provides some further explanation. The SDT does not believe that there is a sufficient definition of “generic” that will add any value beyond its normal dictionary definition.

One commenter suggested that within Requirement Part 5.2, alternate wording be provided to specify “known” enabled default or other generic account types. In response, the SDT agrees and has made the recommended clarification. The SDT notes this concept was already included in Requirement Part 5.4 and has included it here in Requirement Part 5.2 as well.

One commenter stated that Requirement Part 5.4 needs to be clarified that it pertains to active user accounts. The comments stated that there is no value to changing a password for an inactive or disabled user account until such time as the account is enabled. The commenter requested that the Requirement should also be clarified to require the initial

password change prior to placing the BES Cyber Asset into service. In response, the SDT disagrees. A known, published password should be changed even if the account is disabled. If the account is accidentally re-enabled, the password would be widely known. The SDT agrees that it would be a good practice to not only change the default password but also disable the default accounts if feasible, but it is not a Requirement.

There was a comment with regard to Requirement Part 5.4 that the word 'known' is ambiguous. For clarity, the commenter suggested changing the phrase "known default passwords" to "knowable default passwords". In response, the SDT disagrees that changing "known" to "knowable" solves the issue. The Requirement applies to the Responsible Entity, therefore it is "known to the Responsible Entity". Some vendors include "back door" user accounts in devices that are known only to the vendor and not the Responsible Entities. The Requirement is for the Responsible Entity to document only those that they know of.

A commenter suggested that Requirement Part 5.5's limitation to "password only" authentication is too narrow in scope and needs to include any use of a password for interactive access, even if part of a multi-factor authentication. The commenter also stated that this would need to include user accounts that are capable of being used interactively even if the intended use is only programmatic (e.g., an FTP account). Another comment to Requirement Part 5.5 was that the first paragraph uses the phrase "interactive user access" and that this is not a defined term. However, it is similar to the CIP Version 5 definitions defined term. The commenter questions whether the phrase "interactive user access" should be defined or clarified in the Guidelines and Technical Basis section. The SDT has added language clarifying "interactive user access" from the rationale for Requirement R5 to the Guidelines and Technical Basis section for Requirement Part 5.5.

One commenter recommended that the phrase "…at least once every 15 calendar months" be replaced with "at least once each calendar year." In response, and as described earlier, the SDT disagrees as it has standardized throughout the CIP standards that the original use of the word 'annual' be replaced with 'once every 15 calendar months.'

With regard to Requirement Part 5.7, one commenter requested a clarification to establish an upper bound (or maximum number of attempts) to generate an alert or initiate an account lockout. In response, the SDT disagrees that a prescriptive number of attempts is warranted. The entities will be in a better position to determine how many attempts in what time interval are needed for the particular situation. There may be widely varying circumstances to take into account such as is the login used by a process that is vital and will locking it out or slowing the interval between tries affect reliability.

CIP-008-5

General

One commenter stated that both CIP-008-5 and CIP-009-5 have plan update Requirements and should be considered for removal. In response, the SDT does not agree these should be removed in this version because we address multiple Directives in FERC Order No. 706 related to the update of plan documents.

Requirement R1

One commenter suggested adding "assess" to the required processes in Requirement Part 1.1. The SDT does not agree there is a need to include "assess" in the Requirement Part.

One commenter recommended increasing the one hour reporting threshold in Requirement Part 1.2. In response, the SDT uses this timeframe to respond to a directive in FERC Order No. 706, Paragraphs 673 and 676. The one hour also refers to the preliminary reporting required from the point at which the entity has determined an incident is a Reportable Cyber Security Incident.

Several commenters suggested that the obligation to report to the ES-ISAC in Requirement Part 1.2 may not be acceptable for some Canadians, but the SDT is unaware of any ES-ISAC reporting restrictions for Canadians. However, the SDT has clarified that such reporting to ES-ISAC is only required, unless prohibited by law, to account for scenarios where federal or provincial laws may prohibit such action.

Several commenters stated that notification of the ES-ISAC occurs only after a Cyber Security Incident is determined to be reportable and the one hour timeframe should start at the determination of the incident as being Reportable. The SDT has modified the Requirement to clarify the one hour timeframe is from determination rather than identification.

One commenter requested clarification on the term "preliminary notice." In response, we quote from the Technical Guidelines section of CIP-008-5, "This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."

There was a comment that the one hour timestamp in Requirement Part 1.2 would require a paperwork intensive burden on the entity that may qualify for removal according to Paragraph 81 of FERC's Order on the Find, Fix, and Track process.

In response, while additional documentation may be necessary to demonstrate compliance with the timeline, the objective this Requirement goes beyond an administrative function.

One commenter suggested changing the one hour reporting threshold of Requirement Part 1.2 to 24 hours to align with EOP-004-2. In response, the one hour threshold is directed as a change in FERC Order No. 706;the SDTs for both CIP Version 5 and EOP-004-2 agrees this obligation was best left in the context of CIP-008-5.

One commenter stated that the roles and responsibilities of the incident response plans specified in Requirement Part 1.3 should be left to the Responsible Entity. They expressed concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective incident response plan.

Requirement R2

One comment read that Requirement R2 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R2 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter proposed Requirement Part 2.1 needs clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be a disincentive. Regardless, it is best left to the entity to determine how to test its plan.

There was a suggestion that the testing periodicity in Requirement Part 2.1 is inconsistent from the period used across other standards. The SDT agrees and has made this modification.

One commenter proposed adding wording to confirm a single incident response plan is sufficient for all High and Medium Impact BES Cyber Systems. In response, the Requirement Part does not preclude having a single plan, and the rationale in Requirement R1 suggests doing so.

One commenter suggested that documentation of a Reportable Cyber Security Incident suffers a “catch-22” in that one of the steps is a determination of whether or not an incident is Reportable. In response, the documentation of a Reportable

Cyber Security Incident can be performed after-the-fact. This is not a Requirement to document each step contemporaneously with each action.

One commenter recommended removing the documentation of deviations in Requirement Part 2.2 since it is mostly captured in the lessons learned. In response, the lessons learned activity likely will use documentation captured from the Cyber Security Incident, but there is no obligation to document the use of the plan. The SDT chose to use documentation of deviations because this is a much less documentation-centric activity than documenting how the plan was used.

Several commenters stated that Requirement Part 2.3 should be moved to data retention. In response, the retention of this information serves the purpose of supporting follow-up incident analysis and correlation activates. There is otherwise no obligation to retain this information.

Requirement R3

There was a comment that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter stated that CIP-008-5 Requirement R3 should allow deficiency correction. In response, the SDT does not agree this Requirement meets the criteria to be considered as high frequency, zero tolerance obligations as are the other Requirements that allow for deficiency correction.

There was a comment that in Requirement Part 3.1.2, lessons learned do not always trigger a plan update and that a qualifier “as applicable” should be added. The SDT agrees and has added the clarification, “lessons learned associated with the plan.” Corresponding changes have also been made in CIP-009-5.

There was a proposal that the timeframe in Requirement Part 3.2 could be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

One commenter proposed removing Requirement Part 3.2 or specifying only the affected roles and responsibilities. In response, the SDT notes that notification of all individuals is necessary for communication during a Cyber Security Incident.

One commenter stated for Requirement Parts 3.1 and 3.2, the wording needs to be rearranged to read better - the phrase 'no later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this change.

CIP-009-5

Requirement R1

One commenter stated that the roles and responsibilities of the recovery plans specified in Requirement Part 1.2 should be left to the Responsible Entity. They express concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective recovery plan.

There was a comment that Requirement Part 1.2 discusses responders without any additional clarification of who fits into this category. In response, this language has been carried forward from previous versions and the SDT has not received any additional comments supporting modification. The SDT agrees additional guidance would be helpful and has added clarification in the Technical Guidelines section of CIP-009-5.

There was one comment that stated that there should be more consistency in the applicability column of the tables and requests clarity on what applies if a Medium Impact BES Cyber System does not have a connectivity qualifier. In response, the lack of a qualifier only means that all Medium Impact BES Cyber Systems are applicable.

One commenter requested clarity on the intended frequency of performing Requirement Part 1.4. In response, the frequency is determined by the Responsible Entity. Some cyber systems may require a daily backup while other cyber systems, for example, at a power plant, may only require backups after major changes to the system.

One commenter suggested removing “and to address backup failures” from Requirement Part 1.4 because it may lead the reader to the notion of having another pre-determined plan to account for unknown issues during the backup. In response, the SDT notes that addressing backup failures meets the objective of the Requirement and purpose for verifying the successful completion of backups. Without this obligation, an entity could simply perform validation testing without performing any corrective action on the backup process.

Several commenters proposed changing Requirement Part 1.5 to “One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery.” However, the rephrasing has a subtle change in meaning. The per device capability exception applies to the preservation of data and not the procedure itself.

One commenter stated that Requirement Part 1.5 can lead to delay in recovery operations, particularly in a Control Center. In response, the SDT notes the provision of the Requirement that data preservation should not impede recovery.

One commenter requested clarification of Requirement Part 1.5. They state that it would seem the activity would delay recovery. In response, planning to preserve evidence could include additional individuals assisting in the recovery or retaining failed Cyber Asset equipment during recovery operation.

One commenter suggested adding a CIP Exceptional Circumstance qualifier to Requirement Part 1.5. In response, the SDT removed this qualifier based on industry comments because an event triggering recovery could most likely be a CIP Exceptional Circumstance, and thus nullify the Requirement. However, Requirement Part 1.5 achieves the same objective in having a qualifier to avoid the disruption of restoration activities. The commenter also expressed concern about the intent of Requirement Part 1.5 and suggests moving this to CIP-008-5. In response, the objective is to have this performed in any recovery operation and not just Cyber Security Incidents.

There was a comment for Requirement Part 1.5 suggesting that the Requirements could put the registered entity into a "catch-22" scenario where it could try to comply with the Requirement by saving logs, which might impede recovery. In response, the plan should address the issue where saving information impedes recovery as indicated in the Requirement Part.

One commenter stated that in Requirement Part 1.5, the device capability should be worded to clearly qualify the preservation of data. The SDT agrees and has made this change. They also suggested the measure be updated to include the device capability qualifier. However, the qualifier itself only applies to the Requirement and does not need to have inclusion in the measure.

Requirement R2

There was one comment that the words 'between tests of the plan' are not needed. The SDT agrees and has made this clarification.

One commenter requested clarification on how an entity tests a representative sample of information if, per Requirement Part 2.1, they performed a paper drill. In response, the SDT notes that the test in Requirement Part 2.2 is not necessarily the same test performed in Requirement Part 2.1.

One commenter proposed Requirement Parts 2.1 and 2.3 need clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be disincentive. Regardless, it is best left to the entity to determine how best to test their plan.

There was a request for clarification on the difference between 2.1 and 2.3 and for additional guidance on what types of operational exercise the SDT considers meeting the Requirement. In response, the SDT refers to the Technical Guidelines section of CIP-009-5, which states "The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, '[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims).'"

One commenter suggested that Requirement Part 2.2 needs to provide additional clarification for a "representative sample" of information used to recover BES Cyber System functionality. In response, the SDT does not think it provides a benefit to further specify a representative sample of information in this Requirement. Otherwise, this Requirement becomes focused on the sample of information rather than the recovery of information. As specified in the rationale, "Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information."

A clarification request was made on Requirement Part 2.2 regarding a representative sample. The representative sample must be determined by the Responsible Entity. It could be a test of all the most recent backup tapes or it could be a single representative test for multiple instances of the same system.

Requirement R3

There was a comment that this Requirement should include language that would allow an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter suggested that a lessons learned activity should not be required for every failure of equipment in the field. In response, failure of equipment in the field does not indicate a recovery operation in all cases.

There was a proposal that the timeframe in Requirement Part 3.2 be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

There were several comments on parts 3.1 and 3.2 that the wording needed to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this clarification.

Guidelines and Technical Basis

One entity commented that the guidelines state that recovery plan information is BES Cyber System Information, which is not consistent with the definition of BES Cyber System Information. The SDT agrees and has modified the guidance to state that recovery plan information may be considered BES Cyber System Information.

CIP-010-1

Timeframes for Configuration Control Activities

The SDT received comments that the timeframes for configuration control activities are inconsistent. The SDT believes that the timeframes specified are consistent and are reflective of a reasonable configuration change control process.

Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls

Comments expressed concern over the cross-reference to CIP-005-5 and CIP-007-5 as it related to the controls that could potentially be impacted by a change. The commenter recommended that the Requirement be broadened to include any control rather than simply those included in CIP-005-5 and CIP-007-5. The SDT appreciates the concern expressed in this comment and wrestled with this issue itself. After changes to this issue during multiple rounds of industry comment, the SDT believes that bounding the controls that need to be assessed is the most auditable approach.

The SDT received comments regarding a concern over double jeopardy between CIP-005-5, CIP-007-5, and CIP-010-1, specifically as it relates to the documentation of logical network accessible ports. The SDT does not believe this is a double jeopardy situation. CIP-005-5 and CIP-007-5 specify how ports are to be configured whereas CIP-010-1 specifies that they be documented.

Requirement R1

The SDT received numerous comments to add the “external routable connectivity” qualifier to the applicability section in Requirement R1. The SDT appreciates the concern regarding the amount of effort involved in maintaining baseline documentation for disconnected Cyber Assets. However, since these devices are disconnected, the point in time at which the device is interacted with is the only time that the configuration may actually be validated. Given this, the SDT believes it is worthwhile to formalize the configuration change management process for these systems such that an understanding of the current configuration of the device is assured at all times.

One commenter identified confusion as it relates to comma usage in CIP-010-1 Requirement Part 1.5.1. The SDT has clarified the Requirement and removed the incorrect comma.

One commenter asked for clarification that the items in the baseline are “current” and not historical. The SDT confirms that it expects that the baseline is a current representation of the configuration and that this should be kept up to date by Requirement Part 1.3.

One comment from industry asked for clarification as it relates to Requirement Part 1.4.2 and whether this verification that security controls are in place was to be performed on the production system itself. The SDT clarifies that this is the case. The intent of the Requirement is to ensure that the production system is properly protected following a change that affected its baseline configuration.

Several commenters asked for clarification on the use of TFEs in Requirement Part 1.5 (testing of changes) and whether the SDT actually meant CIP Exceptional Circumstances. The SDT envisioned that operational issues may prevent the ability to test a change prior to its implementation. The SDT believes that the TFE process provides the protection necessary to ensure that violations are not issued for a wide range of circumstances, including but not limited to those operational issues contemplated in the CIP Exceptional Circumstances definition.

Requirement R2

Comments expressed that the IAC language should be removed from CIP-010-5 Requirement Part 2.1 because this Requirement was itself an internal control. The SDT agrees that the Requirement represents a control; however it believes that, particularly given the required periodicity, that there could be deficiencies identified in the control itself and it therefore warranted the IAC language.

Requirement R3

One commenter recommended that the language in Requirement Part 3.3 be modified to add the word applicable ("Prior to adding a new applicable Cyber Asset...") in order to clarify that this Requirement did not apply to those systems that are temporarily connected for less than 30 days. The SDT agrees that this is consistent with the intent of the language and has modified the language accordingly.

The SDT received concerns regarding the performance of active vulnerability assessment prior to the deployment of new BES Cyber Assets. The SDT agrees that these assessments may be imperfect and that there may be some applications that will not properly function outside of a full production environment. However, the SDT continues to believe that since this is the only time when active scans may be safely performed on future production equipment that it is in the best interest of the BES for an active vulnerability assessment to be performed.

The SDT received comments preferring additional specificity as to what to validate during a vulnerability assessment. The SDT appreciates these concerns, but believes that a vulnerability assessment for an EMS system may look substantially

different from an assessment of a PLC. The SDT believes that the best approach is to allow the entity to define an appropriate assessment methodology for their environment, which may then be evaluated by an auditor.

The SDT received comments that questioned the technical feasibility of monitoring for changes to the baseline configuration. The SDT originally had intended for this monitoring to occur on a more frequent basis, potentially real-time monitoring. However, it was persuaded that there are some systems for which real-time monitoring would be infeasible. The SDT does believe that given the relatively high level items included in the baseline, that periodic monitoring every 35 days is a reasonable method to ensure that changes are not taking place outside of an entity's change control program.

Numerous commenters expressed concern about the Requirement to document the differences between the test and production environments. The SDT reminds the industry that this Requirement was the result of a FERC directive. Additionally, the SDT reminds the industry that it believes that for a relatively stable testing environment, that this documentation could be done once and utilized for multiple changes or testing cycles.

Commenters asked questions about the multiple timeframes for the vulnerability assessments for high impact BES Cyber Systems. The SDT confirms that these time frames are intended. Effectively, this requires an annual paper or active vulnerability assessment, but an active vulnerability assessment must be performed at least every three years. The SDT believes that the confusion raised by the question is due to the reader not considering the entire table as itself a single Requirement.

One commenter expressed confusion on the applicability of CIP-010-1 to access points. The SDT clarifies that since access points are the point at which access is controlled, they are included in the definition of EACMS and as such are applicable to CIP-010-1.

One commenter asked for clarification that the test environment did not have to be an exact mirror of the production environment. The SDT confirms that this was the intent of using the phrase "models the baseline configuration."

CIP-011-1

Requirement R1

Commenters requested that Requirement Parts 1.1 and 1.2 of CIP-011-1 Requirement R1 be clarified to indicate that a single method or procedure was sufficient. The SDT agrees that this is the intent and has clarified the standard as requested.

Commenters suggested that CIP-011-1 Requirement Part 1.2 should contain a measure that indicates "repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program." The SDT does not see how a repository is evidence of a procedure to protect and securely handle BES Cyber System Information. The SDT agrees that an information repository may be used effectively to meet this Requirement, but it is only a component of the evidence based upon a particular manner of implementation.

Requirement R2

One commenter requested that Requirement R2 of CIP-011-1 be moved to CIP-010-1 as it could be considered part of a change control process. The SDT believes that the objective of this Requirement is the protection of the information in a BES Cyber System and therefore believes it is appropriate to include in CIP-011-1.

Commenters identified a typographical error in the measure of Requirement Part 2.2. The SDT appreciates this correction and has updated the standard.

Implementation Plan

Effective Date

Several commenters had questions or concerns about the Version 3 to Version 4 to Version 5 transition within the standards' implementation plan. Some questioned whether extending Version 3 to the effective date of Version 5, and superseding Version 4, is still possible, while others asked for a deadline for accomplishing such a transition plan. The SDT appreciates these concerns, as they are issues of efficiency, planning, effort, and cost for all of the industry. However, the SDT also acknowledges that not all entities are situated exactly the same. As such, the SDT is hesitant to provide a "deadline" or other trigger for FERC action that would serve to foreclose the opportunity for the implementation language to be adopted in time to implement moving directly from Version 3 to Version 5. The SDT expects that the filing will address this issue in a manner such that certainty about the issue may come as soon as possible, and that the filing and other coordination between NERC and FERC is the appropriate venue for supporting the implementation plan after industry approval. In the meantime, it is reasonable to expect that some entities may need to make a risk-informed judgment to proceed with Version 4 implementation by a certain date if the proposal in the implementation plan is not approved expediently. Some entities may be able to wait longer than others into 2013 before making that determination. The SDT has communicated directly with NERC to underscore the importance of coordination of this effort, and the SDT believes that having an approved set of standards, definitions, and implementation plan before the end of 2012 continues to provide a reasonable timeline to consider the implementation plan proposal.

There was one comment that 36 months to comply with CIP-003-5 Requirement R2 is excessively long since it only requires documentation of a few policies. The SDT notes that CIP-003-5 Requirement R2 requires implementation, and not just documentation of policies. This expands to a significantly large number of the overall reported BES Cyber Systems, which warrants such a timeline.

One commenter suggested that it misleads entities to allow the provision suspending compliance with Version 4. The SDT does not agree this is misleading. The SDT has been careful to communicate the risk in awaiting this order to begin planning compliance with Version 4. Furthermore, the FERC approving this provision, even if it is closer to the Version 4 Effective Date, still spares entities and auditors alike untold expenses of a compliance monitoring program for Version 4.

A few commenters asked about audits in 2015 during the expected transition window to Version 5's effective date. That is outside the scope of the SDT, but the SDT has tried to account for a smooth transition within the implementation plan,

to include specifications for initial required performances of periodic events. In response to this question and the issue of transition from Version 3 to Version 5, the SDT understands that NERC is preparing information to assist in the smooth transition among CIP standards versions, and that such information will be coordinated upon certainty that Version 5 has been approved by the industry and is no longer subject to change.

One commenter stated that the effective date language should be qualified with a statement that sufficient time should be given for completion of CIP-002-5 R2 to comply with CIP-003 through CIP-011. The SDT believes this is already well understood and ongoing communication and training will provide entities further guidance to categorize BES Cyber Systems with sufficient time to comply with CIP-003 through CIP-011.

Several entities comment that NERC and the drafting team should request FERC to suspend compliance with Version 4 and allow entities to transition from Version 3 to Version 5 on the effective date. In response, the proposed effective date does bypass Version 4 and provides the FERC the opportunity to issue an order approving this provision. In effect, this is the industry and SDT communication to the FERC requesting the bypass of Version 4.

There was a comment that suggested extending Version 3 until Version 5 becomes effective could not be accomplished in Canada through an implementation plan. In response, the SDT notes that Canadian jurisdictions would be subject to the second provision for "those jurisdictions where no regulatory approval is required." The commenter is correct that the proposal in the Implementation Plan, if approved, would supersede any other Order to the contrary. In all cases of reliability standards, the Implementation Plan is subject to regulatory or other applicable federal approval.

A few commenters noted that CIP-003-5 is dependent upon CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1 passing. The SDT confirms the commenters' understanding and notes that the implementation plan conditions all standards passing before any of them become effective.

One commenter expressed concern that the implementation of CIP-004 through CIP-011 should be combined into those standards. The SDT points out that the implementation of security procedures in CIP-004 through CIP-011 is included in those Requirements that have actions associated with them. The entity should refer to the high level Requirement for the implementation language.

Initial Performance of Certain Periodic Requirements

Several commenters stated some confusion with the initial performance of periodic Requirements section or suggested that it is unnecessary and, if retained, should be in guidance. The SDT notes this section was incorporated from industry comments, and moving this section to guidance would be misleading because the additional time for compliance with periodic Requirements would not be enforceable in guidance.

There was a comment that no provision for CIP Exceptional Circumstances exists for some periodic Requirements and that an entity should be allowed to track instances of non-compliance in CIP Exceptional Circumstances rather than self-report. In response, the SDT has indicated where exceptions may occur to the standards in defined CIP Exceptional Circumstances. Most of the periodic Requirements should have enough lag time built in to avoid the need for self-reporting in emergency situations. Otherwise, it is not envisioned all compliance activities should cease in a CIP Exceptional Circumstance, but only the ones indicated in the Requirements.

One commenter proposed revisions to the following initial periodic Requirements, and the SDT responds in order:

- CIP-004-5 Requirement Parts 4.2 through 4.4 should be required on or before the effective date to preclude record-keeping errors. The SDT notes that record-keeping errors, while not the most efficient, are not violations of the standard.
- CIP-006-5 Requirement Part 3.2 should tie to the previous testing interval and allow 24 months for the newly in-scope Cyber Assets. In response, tying the interval to previously in-scope Critical Cyber Assets would cause more confusion than is necessary for this Requirement, and the SDT believes the 12 calendar months are appropriate timeframes for testing PACS.
- CIP-008-5 Requirement Part 3.1 and CIP-009-5 Requirement Part 3.1 should not be included in the initial performance of periodic requirements section since they are not periodic, but are performed in response to a test. The SDT agrees.
- CIP-010-1 Requirement Parts 3.1 and 3.2 should not be included because it would be similar to part 3.3 in adding a new Cyber Asset to the BES Cyber System. In response, the SDT retains the additional timeframe because strict compliance would suggest this periodic timeframe be performed immediately on the effective dates for all BES Cyber Systems in scope, which would be infeasible for most all entities.
- CIP-009-5 Requirement Part 2.3 is included in both groups 6 and 7. The SDT notes this is not the case.

- Group 8 of the periodic Requirements dealing with the continued effectiveness of previous personnel risk assessments is already incorporated in the Requirement language. In response, strict compliance with the Requirement would otherwise suggest immediate compliance with this Requirement on the effective date.

One commenter suggested that NERC imposing Requirements before the effective date goes beyond NERC's legal authority. In response, the implementation plan does not modify the effective date of any Requirement but makes clear when the initial performance must occur for certain Requirements. By stating a Requirement can be performed prior to the effective date does not impose a different effective date. Rather, this clarifies that on the effective date, the entity has complied with the Requirement by performance of a past activity.

There was an observation that CIP-006-5 Requirement Part 3.1 and the Requirements specified in section 7 have periodicities longer than the initial performance. This is correct and intended by the SDT because even though the periodicity is longer, the benefit achieved by the initial performance puts it closer to the effective date.

Previous Identity Verification

One commenter noted an incorrect reference to CIP-004-5 Requirement Part 4.1, and the SDT expresses their gratitude for uncovering this error.

Planned or Unplanned Changes Resulting in a Higher Categorization

Several commenters suggested that the distinction between planned and unplanned changes is not clear and the timeframe for planned changes should be extended to 18-24 months. In response, the SDT carries forward this language that has been in effect since Version 2. The 12 months is also carried forward as the time entities with existing CCAs have to implement CIP Requirements on new CCAs. The SDT does not consider this 12 month timeframe unreasonable and notes in the example given that updates to a generation facility would be considered a planned change and compliance would be part of the maintenance performed during the outage.

One commenter stated that the addition of time for initial performance of periodic Requirements muddles the timeline for compliance. In response, the implementation plan would not preclude an entity from complying earlier to benefit the entity with a consistent compliance schedule, but without this provision, the periodic Requirements would need to be performed prior to the 12 month period, and this is neither reasonable nor appropriate. This language was added since the last posting in response to multiple entities' request.

There was a comment that suggested the last scenario in unplanned changes be clarified as the first high or medium impact BES Cyber System overall rather than at a facility. The SDT has made this clarification by providing a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

There was a request for clarification on the use of Effective Date in the table heading "Scenario of Unplanned Changes After the Effective Date". In response, the SDT notes that this is the effective date specified in each standard for Version 5 of the CIP Cyber Security Standards.

Applicability Reference Tables

One commenter proposed revisions to the Requirement applicability, and the SDT responds in order:

- CIP-004-5 Requirements R4 and R5 should apply to Protected Cyber Assets. In response, we have addressed most of the risk by authorizing and revoking access associated with the BES Cyber System. We carry forward the precedent of applicability in this case from previous standards, and do not find a justification for adding them to the applicability of these Requirement Parts.
- CIP-005-5 Requirement R1 should apply to PACS as it does in the current standard.
- CIP-005-5 R1 should apply to PACS as it does in the current standard. In previous versions, CIP-005 R2 applied but not R1. The SDT received significant industry feedback that this applicability was confusing and resulted in multiple interpretations. The SDT addresses access control at the device level in CIP-007-5 and avoids the confusion around the disconnect between applicability in CIP-005-4 R1 and R2, and for this reason, CIP-005-5, Requirement R1 does not apply to PACS.

There was a comment that CIP-005-5 Requirement R2 should apply to EACMS. In response, the EACMS are referenced as part of the Requirement. The confusion of recursive Requirements is not worth the reliability and security benefit gained by their inclusion.

Definitions

BES Cyber Asset

One entity commented that the definition should reference "the items in Attachment 1" instead of "Facilities, systems, or equipment," because "Facilities, systems, or equipment" is subjective and lends itself to differing interpretations, and Attachment 1 provides greater clarity and guidance on the criteria to define BES Cyber Assets. The SDT points out that a definition is used in a standard and cannot reference a part of the standard. The term "Facilities, systems or equipment" has been used as part of the definition of Critical Assets for Versions 1, 2, 3 and 4.

BES Cyber System

One commenter wrote that the definition uses the word logically that may be mistakenly interpreted to mean networked instead of validly grouped. The SDT believes that the rest of the definition of the BES Cyber System in relation to the performance of reliability functions provides clarity to the meaning used here.

BES Cyber System Information Responses

The SDT received a concern regarding the phrase "not publicly available" in that if BES Cyber System Information was made public, it would then be outside the scope of the standard. The SDT appreciates this concern; however, it believes that the meaning is ultimately clear as to the intent.

CIP Exceptional Circumstance Responses

The SDT received a request to clarify the punctuation in the definition of CIP Exceptional Circumstances. The SDT has updated the punctuation as requested.

One commenter expressed concern about the ability to declare a CIP Exceptional Circumstance for hardware, software or equipment failure. The concern of the commenter was that this could open the door to bypassing Requirements for minor issues. The SDT did not envision this as a free for all and believes that the obligation to have policy around the declaration and response to CIP Exceptional Circumstances should minimize any abuse of this definition.

CIP Senior Manager Responses

One commenter requested that the SDT address the accepted interpretation request in RFI Project 2012-INT-06. While the SDT has an obligation to incorporate existing interpretations, the response to the interpretation that was highlighted has not been posted and therefore the SDT would risk contradicting a pending standards interpretation action.

Additionally, since that interpretation has not been approved by industry, there is no way for the SDT to determine whether it reflects a level of consensus of the industry. As such, the SDT believes that this would be too large of a change to incorporate at this point in the development process.

Control Center

Many entities requested clarification on the term “associated data centers” in the definition of Control Centers and asked whether these are the "data centers" that service/support a control center”. Comments were also made that “data center” is not a defined term. The SDT believes that the term “data center” is a commonly understood term of practice and that a specific glossary definition is not required. The intent of including “associated data centers” in the definition of Control Centers is to include only those systems that are associated with the Control Center Cyber Assets and directly support the functions of the functional entities defined. These will be the BES Cyber Systems that directly provide monitoring and control functions for the Control Center operators’ use in the performance of their real-time functions, and to ensure that this does not include certain types of field data aggregating or processing assets that are associated with field transmission or generation assets. Control Center data centers do not necessarily reside in the same facility where operators are hosted, but may extend the Control Center to include facilities hosting these cyber systems outside of the facility hosting the Control Center operators.

One entity requested clarification on the meaning of “location” in the definition. The NERC Guideline for Critical Asset identification has an extensive discussion of control rooms and Control Centers. In general, a location is delineated by a physical boundary that hosts a set of BES Facilities.

One entity suggested the addition of “CIP” to the term or some indication that this is only a definition used in the CIP context. The SDT is proposing the term to be included in the NERC Glossary. The convention is that when the term is used in its capitalized form (initial letter of each word), then it is used as the NERC Glossary defined meaning of the term. Otherwise, it is used in the undefined, generic meaning. This does not have any effect on other standards that do not use the term in its capitalized form. Other standards which wish to use the NERC Glossary term as defined (or wish to amend it through the development process) can use the capitalized form.

Cyber Asset

One entity commented that the inclusion of “hardware, software and data” in the definition of Cyber Asset was redundant and proposed a simplified definition of “Entity programmable electronic devices”. The SDT’s approach to existing definitions is to make only the modifications necessary for additional clarity or intent. This definition is based on

the previous definition of Cyber Asset. The SDT believes that removing the terms "hardware, software and data" would not provide additional clarity and that the addition of "Entity" in the qualification of "programmable" would inappropriately limit the general scope of the definition of cyber asset. The protection Requirements in the standards include those necessary to ensure that proper processes are included for protection from inappropriate modification or misuse of programs not directly modified by the entity.

Another entity commented that the proposed definition could be interpreted to require utilities to demonstrate consideration of - in addition to hardware - all software and data on each programmable electronic device, which would be impracticable and overly burdensome. The entity recommends changing the definition to "Programmable electronic device." The SDT points out that the inclusion of these qualifications has been part of the definition of cyber assets since Versions 1, 2, 3 and 4 and that the modifications to the previous definition ensures that the definition includes the data when it is on these devices.

One entity commented that the inclusion in voice communication for a Control Center operator to implement operating actions in the execution of a Control Center functional obligation would include many smaller entities as Control Centers. The determination of whether a facility is considered a Control Center is dependent on whether it meets the definition, not on size or on how it performs its functional obligations. The manner in which it implements its functional obligations will determine what are qualified BES Cyber Assets. For example, in the environment that the commenter describes, there may be many BES Cyber Assets that provide monitoring and alarming information on which the operator will initiate a real-time operation for the BES. The impact of such monitoring and alarming systems on the real-time operation of the BES warrants the protection commensurate with its function.

Cyber Security Incident

One commenter suggested modifying the definition of Cyber Security Incident to eliminate attempts of compromise or disruption because such a definition is broad enough to include any erroneous traffic. The SDT disagrees. Attempts of compromise imply intent far beyond erroneous traffic and should be analyzed and recorded as part of the CIP-008-5 incident response plan.

There was a comment that the definition of Cyber Security Incident should also apply to PCAs, EACMS and PACS. In response, the definition has no applicability, and an incident occurring on PCAs, EACMS and PACS already meets the definition of having the potential to impact the BES Cyber System.

There was a comment suggesting that it is difficult to determine the intent of an attacker, and the commenter further suggested that "suspicious" is vague. In response, the SDT intends that such determination is best left to the entity. Without the qualifiers of suspicious and malicious, it could be interpreted that many nominal events would be considered Cyber Security Incidents.

Electronic Access Control and Monitoring System

One commenter stated that the definition of EACMS is inconsistent with the definition used in the background section of Version 5 CIP Standards. In response, the guidance provided in the background section is not a definition. It only provides example EACMS for the purpose of adding context for the reader.

Intermediate Device (now "Intermediate System")

A recommendation was made that the definition of Intermediate Device be modified to remove the phrase "or collection of Cyber Assets", as they consider this limiting the scope. The SDT used "A Cyber Asset or collection of Cyber Assets" to allow for flexibility so that an entity could use one or more devices to perform the noted functional Requirements. The scope of the definition and Requirements is limited to only Interactive Remote Access to BES Cyber Systems. Further, it was noted in prior comments that entities may not be able to implement a single device that provides encryption and multifactor authentication. As a result of comments, the definition has been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards.

One commenter requested clarification on the definition of Intermediate Device. The SDT has worked the definition to allow for flexibility in the selection and implementation of technology to meet their needs. The definition does not prevent an entity from having an Intermediate Device within an ESP, just not the ESP containing the BES Cyber Systems being remotely accessed. The definition term (not the definition's meaning) has also been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested more clarity regarding the types of devices that would qualify as intermediate devices, beyond the Requirements that they must support encryption for any interactive sessions and multifactor-authentication for access to any interactive sessions. Additional references are available in the *Guidance for Secure Interactive Remote*

Access document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Interactive Remote Access

One commenter suggested that, as written, the definition appears to require that entities declare each of their internal networks as an ESP, including their corporate networks. The commenter discussed that many entities monitor their corporate network in much the same manner as their ESPs, and that requiring encryption within their corporate networks would introduce an unacceptable security risk by rendering their monitoring capabilities ineffective. The commenter requested appropriate clarifications or that the definition be modified to specify that Interactive Remote Access and the associated technical controls be required when traffic is traversing an untrusted or public network only. In response, the SDT notes that it is not necessary to declare the encryption termination point as a part of the ESP. It is allowable to have the termination point reside outside of the ESP, such as a corporate firewall to allow for corporate boundary systems to monitor network traffic as described. In this scenario, the corporate firewall would be considered and protected as an EACMS but still not considered to define an ESP.

There was a recommendation to remove the second sentence of the Interactive Remote Access definition. The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

One comment suggested that the definition of Interactive Remote Access be modified to remove the sentence, "Remote access can be initiated from: ... contractors and consultants." The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

There was one request that the definition be modified as "access is likely initiated…" The SDT used "may be initiated" to allow for flexibility rather than using words such as "shall be initiated" or "will be initiated" which are far more restrictive and align to the concern noted.

There was a suggestion that the definition of Interactive Remote Access be modified to remove Requirement language within the definition. The SDT considers all parts of the definition to be clarification of what is and is not Interactive Remote Access. The Requirements are the technical controls to be implemented.

Reportable Cyber Security Incident

There was a comment suggesting that the definition of Reportable Cyber Security Incident is too broad and should specifically state that a malware infection of an in-scope Cyber Asset should be reported. In response, the SDT provides additional guidance in the context of CIP-008-5 that would generally ensure the proper reporting of a malware infection. However, a malware infection itself would cause additional uncertainty in the definition. Moreover, entities would be left to wonder if a contained malware infection was reportable or not. For these reasons, the SDT does not agree with the recommendation to further specify Reportable Cyber Security Incident.

One commenter said that this definition should be removed and addressed solely within the standard. In response, the SDT believes there is sufficient consensus for the definition and moving this term to a local definition in CIP-008-5 would be a significant change and potentially cause uncertainty in the enforceability of this definition.