NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form A
CIP-002 and CIP-003 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 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

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated

In response to draft 2 of the Version 5 CIP Cyber Security Standards, the Standards Drafting Team (SDT) received significant input from a wide variety of perspectives. All of that input greatly helped the team to refine the standards and associated documents, and the set of standards now posted reflects all of that combined input. There were several varied perspectives in the comments, and the SDT attempted to address each comment as responsively as possible.

There were several changes that reflected careful consideration of several comments that affected the standards on a global basis, whether in format, style, or substance. In addition, there were several comments the SDT considered that were repeated across multiple questions, sometimes submitted by the same entity to each or to many of the questions. Rather than explaining in detail the global changes in response to each question, and rather than responding separately to the frequently repeated comments in each question, the SDT addresses those global issues and general comments in this section.

Many comments related to specific language suggestions or to specific compliance concerns. The SDT has responded to those comments in each of the individual questions summaries that follow this section. Those comments were thorough and varied, and they reflected diverse perspectives and topics. The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan. The SDT believes this posting package addresses all of the substantive issues received from the previous two iterations of comments and various other inputs.

Change in labeling of the applicability columns in the tables to "Applicable Systems"
After posting draft 1 of CIP Version 5, commenters expressed concern that merely using "Applicability" as the title of the applicability columns in the Requirement tables (in CIP-004 through CIP-011) created confusion with the actual "Applicability" section of the standards. In response, for draft 2, the SDT added specificity and labeled those columns "Applicable BES Cyber Systems and associated Cyber Assets." In response to that change in draft 2, commenters expressed concern with the length and suggested that the SDT label the applicability column "Applicability." Therefore, the SDT is proposing to label these columns, "Applicable Systems." This should eliminate any confusion with the applicability section of the standards themselves while also providing appropriate brevity.
Handling of "associated" Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCA) (and the associated change to their use in the "Applicable Systems" column of the requirement tables)
In previous drafts, in the applicability columns (now "applicable systems" columns), the standards used a term "Associated Protected Cyber Assets," "Associated Electronic Access Control or Monitoring

Systems," and "Associated Physical Access Control Systems" where it intended that the requirement part be applicable to not only the applicable high or medium impact BES Cyber Systems, but also to other Cyber Assets or systems, as specified, associated with those BES Cyber Systems. Also, for Protected Cyber Assets, the requirement applied to Cyber Assets or lower impact BES Cyber Systems that were in the same ESP as the applicable BES Cyber System. There was confusion the precise meaning or application of the "associated" systems, and the SDT has made the link more explicit in this draft. One of the fundamental concepts of CIP Version 5 is that it is adopting a systems approach, and those "associated" systems should be more closely connected with the applicable subject of the requirement. Therefore the SDT has moved the associated systems to follow immediately after the subject of the requirement and clarified that they are "associated with" that specify type of BES Cyber System or other applicable system. Mitigation for the associated systems may be accomplished through other applicable systems.

High Watermarking Concept

The CIP Version 5 Standards use a term "Protected Cyber Assets" to refer to those Cyber Assets that are within the ESP, which in previous versions of the standards were "other (non-critical) Cyber Assets within the ESP" (see CIP-005-4, Requirement R1, Part 1.4, and CIP-007-4). Additionally, in Version 5, a Protected Cyber Asset can also be a BES Cyber System of a lower impact classification if it is within the same ESP as a higher impact BES Cyber System.

For example, CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in

the ESP. The standard accomplishes this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

Measures: "but not limited to"

Many commenters expressed concern about or questioned the meaning of the use of "but not limited to" in the previous draft and asked for it to be removed from the measures. The concern as the SDT understood it was that "but not limited to" could be used to request evidence beyond that which is specified in the measure even if the entity has otherwise provided what the measure describes. With respect to "but not limited to," the SDT specifically inserted that phrase to assist the Responsible Entity, particularly in light of technologies that may change. It is not intended to be used as a mechanism to request additional evidence beyond that which is required to demonstrate compliance. The SDT is concerned that removing "but not limited to" opens the same question (albeit in slightly different context) as the CIP Interpretation Drafting Team just answered with respect to the interpretation of CIP-002 (versions 1 through 4) for Duke Energy (NERC Standards Development Project 2010-INT-05). Namely, are the measures listed exhaustive/prescriptive or are they illustrative? By including a qualifier such as "but not limited to," as is common in statutory drafting and in other legal contexts, the SDT intends to signal that the measures are not exhaustive. It provides flexibility to the Responsible Entity on what is acceptable. For example and for purposes of illustration, if one said "evidence may include an orange, a lime, or a lemon," one could expect that perhaps only an orange, a lime, or a lemon would be appropriate. However, if one said, "evidence may include, but is not limited to, an orange, a lime, or a lemon," one could just as reliably expect that an orange, a lime, or a lemon would be appropriate, but it would also be reasonable that something not explicitly enumerated by the list, but similar in nature to items on the list, such as a tangerine, may also be acceptable. Importantly, that is not the same as additionally requiring a tangerine even though one already has an orange; however, that is the concern manifested in the comments. To address the commenters' concerns, however, the SDT has made a slight change in support of signaling in all measures that they are examples and that the list of examples is not exhaustive. The SDT believes that it is providing sufficient flexibility in this manner—and for the Responsible Entities' benefit—in clarifying that measures are not prescriptive lists while also attempting to allay fears that "but not limited to" will be used in a manner that expands the requirement. Rather than stating "Evidence may include, but is not limited to, . . ." the SDT has added the "example" concept to precede "evidence" (e.g., "**An example of** evidence may include, but is not limited to, . . ." or "**Examples of** evidence may include, but are not limited to, . . .").

Movement to focus on correcting deficiencies in certain requirements:
In response to several comments, 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. Where used, the requirements incorporate the forward-looking language into the main requirement, which ties in with CIP Version 5's use of accompanying tables. It is presented in those requirements as follows:

> "Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table]."

The SDT also considered several alternatives and additions to this language. For example, some alternatives proposed modifying "process" (or program, etc.), while others suggested to add language specifying certain things that are not violations in addition to the requirement language. Many of the ideas or suggestions presented concepts that the team agrees with, but they are more appropriate for other aspects of monitoring compliance with the standards, not for inclusion within the standards themselves. Language indicating what is not a violation is more appropriate for compliance tools such as the RSAW. The SDT also notes that the VSLs will reflect this approach where the approach is used, and the SDT is actively working with NERC Compliance Operations to prepare the RSAWs for the CIP Version 5 standards. Furthermore, the SDT expects continued participation by industry in providing input into the RSAW development following approval of the standards, and the SDT notes that a draft RSAW for part of CIP-006-5 is posted for comment and for illustrative purposes.

The SDT is charged with writing straightforward requirements stating the desired behavior that will maximize reliability of the BES. The CIP requirements are written to require documented processes that must address the elements in the tables that accompany the requirements. These tables therefore set the parameters for the processes. There are no issues with documenting the processes – the entity must have the processes and they must have the parameters as outlined in the requirement tables.

The compliance concerns, especially those related to zero tolerance for deficiencies, is not related to the documenting of the processes, but in the implementation of the processes. The process should have numerous 'bright line' parameters that outline the goal the industry striving towards. A concern applies when implementing the processes in a world of tens of thousands of people and hundreds of

thousands of Cyber Assets. In certain cases, absolute perfection forever is not reasonable, even if it is desirable.

In light of the direction toward a risk-based approach to compliance monitoring by NERC, The CIP SDT had an opportunity to do to address this issue in certain requirements within the standards themselves. As described above, the SDT included a phrase to modify the verb 'implement' in several (but not all) of the requirements in CIP V5. Entities are to have the processes; the processes must meet the requirements in the tables; and the entities shall implement those processes in a manner that identifies, assesses, and corrects deficiencies.
The emphasis of the self-correcting language is on the implementation of the processes. The processes themselves cannot miss required parts or parameters as outlined in the tables.

Implementation Plan proposal to extend Version 3 until Version 5 remains unchanged in this draft
In light of the order approving the CIP Version 4 standards (FERC Order No. 761), several commenters asked about the drafting team's proposal in the implementation plan to extend Version 3 until the effective date of Version 5. The SDT's proposal, if approved—and its intent for Version 5 to supersede Version 4 and to extend the effectiveness of Version 3 until Version 5 goes into effect—remains unchanged.
In the implementation plan for the CIP Version 5 standards, the SDT has previously proposed to extend Version 3 until the effective date of Version 5. In doing so, the effective date proposes that Version 4 will be superseded by Version 5 and not go into effect. Even though Version 4 has been approved by order, the SDT always contemplated such approval during the development of the implementation plan language. That order does not change the SDT's proposal. The expectation that there would be an order in early to mid 2012 is why the SDT included language in the implementation plan's effective date to specify that the extension of Version 3 until Version 5, and that Version 4 would not go into effect, would occur "notwithstanding any order to the contrary." There is no change in the SDT's intent and proposal to extend Version 3 until Version 5, and for Version 5 to supersede Version 4, notwithstanding the recent order approving Version 4. The SDT also understands, as is the case for any standards proposal by the industry, that the proposal is subject to approval by regulatory authorities.

Stakeholders will notice that within the individual standards for CIP Version 5, the effective dates have been modified so that they are specific to the particular standard. In doing so, the reference to extending Version 3 and superseding Version 4 has been removed, as the Implementation Plan is the appropriate place for that language (where it remains, as described above). Thus, while there is no change to the SDT's proposal, the individual, standard-by-standard effective dates have been modified to comport with the style and form of other NERC Reliability Standards.

Annual v. 15 calendar months
Several commenters expressed dissatisfaction with the standards' use of the phrase ". . . at least once every calendar year, but not to exceed 15 calendar months . . ." for describing the required frequency

of performance on some requirements. Some entities expressed a desire to simply use "annual," while others suggested changing the "but" to an "or." The SDT has discussed alternative approaches and is using the term ". . . at least once every 15 months . . ." to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. As explained in the global comment section of the response to comments for draft 2, simply using "once per calendar year" creates a potential for bi-annual bookending that the SDT does not intend. Similarly, the SDT understands that the use of both "calendar year" and "15 calendar months" was unnecessarily complicated. The SDT acknowledges that there is a CAN that addresses "annual," but that applies where the standard does not make clear what it means in its use of the term. In CIP Version 5, there is an opportunity and an obligation to unambiguously reference the periodic time parameter. Furthermore, one of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify an audit interpretation. Instead, the SDT used specific language to clarify a time parameter that approximates one year in time while also accounting for operational realities that make a 15 month parameter more reasonable. The term "annual" is no longer used in these CIP standards for periodic requirements, and, therefore, the CAN on the word "annual" can no longer apply.

TFE v. Per Cyber Asset Capability

Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a technical feasibility exception ("TFE") in instances where a device could not meet the required parameter. The SDT has spent considerable time reviewing each use of TFE language in CIP Version 5 where it is necessary.

The SDT has also determined that there are some requirement parts that should not require a TFE, as certain parameters are not essential themselves, but should apply if a device is capable of the parameter. This is distinct from the reasoning for requirements with TFE language. In the latter requirements, a certain performance or parameter is required, regardless of technology, device, etc. By using "per (device/system) capability," the SDT does not intend that the specific parameter or performance is required regardless of capability, but only applicable on devices that have that capability. For example, proposed CIP-007-5, Requirement R4, Part 4.1 requires "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents . . ." Here, the SDT does not intend to require event logging. However, if a Responsible Entity is using a device that can log events, it is required to enable event logging to the extent the device is capable.
The phrase "where technically feasible" indicates that the standard requires strict compliance without a TFE. As mentioned above, the drafting team does not intend for some requirements to be TFE-triggering. The underlying rationale for a TFE is that there is legacy equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern.[2] Under such circumstances, the responsible entity must file a TFE that demonstrates strict compliance with an

[2] Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, Paragraph 3

applicable requirement is not technically possible and that there is an alternative course of action that will protect the reliability of the Bulk-Power System to an equal or greater degree than strict compliance.[3]

While a TFE requires an entity to show why strict compliance with an applicable requirement is not technically possible, "per device capability" clarifies that the requirement is only applicable to the devices for which compliance with a particular requirement is possible in the first instance. This provides reasonable flexibility to the industry while also retaining the TFE concept where necessary. Thus, the "per device capability" alternative reduces the need for TFEs and will be less onerous on entities. The SDT does not intend to eliminate TFEs altogether, but proposes to use the "per device capability" as an alternative that is effective in protecting the reliability of the Bulk-Power System.

VSLs

In previous drafts of the Version 5 CIP Cyber Security Standards, VSLs were posted concurrent with each standard. For this posting, the VSLs are presented in one document. They will continue to be prepared for posting for non-binding poll during the recirculation ballot. The VSLs should not be a basis for a ballot determination, and the SDT will continue to refine them as necessary.

Applicability Section of the standards (Introduction - Section 4 – Applicability)

There were several comments about the Applicability section of the standards in various comments related to specific standards. The SDT has reviewed those suggestions and made several changes to the applicability sections of each standard.

Several commenters stated that in part 4.2 of section 4, the criteria for qualified Distribution Providers and Load Serving Entities for UVLS/UFLS systems remain unclear. Specifically, the language was not clear on whether the 300 MW of load referred to the DPs and LSEs' share or to the total load shed. In addition, they also noted that the language for Transmission Protection systems is unclear and needs clarification to more precisely describe the protection systems that are in scope. They also suggested that these should be moved to Low Impact because there is no justification for small entities to be subjected to the requirements for Low and Medium entities. The SDT has proposed modified language to clarify the qualifications for UFLS and UVLS systems that specifies that they are those UFLS or UVLS systems that are part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard and that perform automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. With regard to the impact classification, the SDT believes that because of the function that UVLS and UFLS systems play in last ditch efforts to stabilize the BES, the 300 MW threshold provides a measure of impact that justifies the classification as medium impact systems: lower impact systems have already been removed from the scope and are not subject to these standards.

[3] Id, Paragraphs 5 and 8

Many references in the applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Several comments indicated that LSEs should not be included in section 4 since the NERC Functional Model does not include any tasks related to the implementation and operation of load shedding systems. The SDT reviewed the LSEs tasks in the NERC Functional Model and has removed LSEs from the applicability of the CIP standards.

Several commenters suggested that the following language be added to the end of the criterion for Protection Systems: "and where the Protection System is connected to a supervisory control system providing remote operation capability." The SDT has reviewed the proposed addition to section 4.2.2 for Protection Systems and does not believe that the additional language to restrict the scope to only those Protection Systems that are remotely operated is intended or justified in the scope of section 4.2.2. The SDT notes that the proposed addition makes the assumption that all cyber vulnerabilities are based on remote operation capability. This would provide an incomplete mitigation for cyber threats that do not rely on remote operation for execution.

Several commenters stated that the inclusion of the glossary term "Systems" does not apply to DPs as used in section 4.2.2. One comment also pointed out that this is true in many other places where the term is used, while others' comments pointed out inconsistencies in the use of the term. The SDT notes that the terms Facilities, systems and equipment is always used in combination in the context of this application. The SDT has considered the intent of the terms in its uses and agrees that the glossary term "Systems" does not reflect the intent, and the SDT has made those changes where appropriate. In addition, the SDT believes that the issue is relieved with the changes made to refer to "assets" when referring to a group of Facilities, systems or equipment at a given location.

One comment stated that the statement at the beginning of the guideline and technical basis section that refers to applicability to DPs that refer to EOP-005 should be deleted since section 4.2.2 scopes more than EOP-005. In response, the SDT notes that the paragraph also includes reference to the registration criteria, in addition to EOP-005. The SDT believes the reference is appropriate.

One comment noted that in section 4, part 4.2.2, all single points of failure in the cranking paths should be protected and that where the Blackstart Resource is outside of the Responsible Entity's ownership, that the part of the cranking path that is the injection point to the cranking path to the unit to be

started should be specified. The SDT notes that Section 4.2.2 is not the criterion for determining the protection of the cranking path, but rather defines which part of a DPs equipment is in scope.

One comment suggested additional qualification in section 4 to ensure that the exemption section covers all facilities covered under a cyber security plan under the Nuclear Regulatory Commission (NRC) regulations. The SDT agrees with the clarification and has included the suggestion in the language in section 4 that covers nuclear facilities. The language has been added to section 4.2.4.3 to read: "In nuclear plants, the Systems, structures, and components that are regulated by the NRC under a cyber security plan pursuant to 10 C.F.R. Section 73.54."

One comment discussed the use of the phrase "required by a NERC standard" in section 4 and instances of affected Facilities, systems and equipment where there is no requirement to implement them by a NERC standard. The SDT agrees with the discussion and has made modifications to the language to more accurately reflect the intent.

One comment stated that section 4.2.4.2 attempts to define exemptions for communication links, but fails to include the exclusion of end points to those circuits (see CIP-005/R1.3). The SDT notes that end-points of circuits that are access points are included by the definition of Electronic Access Points (i.e. they are not "between" ESPs).

Reason for CIP Version 5

Some commenters inquired in their comments why CIP Version 5 was necessary, or they expressed a preference to continue under existing versions of the CIP Standards. To facilitate understanding of the reasons for Version 5 as part of the obligation to address the remaining directives in FERC Order No. 706, the SDT offers the following explanation and review of the previous versions of the NERC CIP Reliability Standards.

The NERC Board of Trustees adopted the first version of the CIP Reliability Standards on May 2, 2006. On August 28, 2006, NERC submitted to FERC for approval the Version 1 CIP Reliability Standards. On January 18, 2008, FERC issued its Order No. 706. In this order, FERC approved the Version 1 CIP Reliability Standards and issued more than 100 directives to NERC that included modifying the standards. An SDT began a phased-in approach to respond to the directives in FERC Order No. 706. As part of that phased-in approach, the SDT addressed the directives in the order that it could respond to quickly, and it developed a plan to address the remaining directives.

Version 2 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on May 6, 2009. On May 22, 2009, NERC submitted to FERC for approval the Version 2 CIP Reliability Standards. On September 30, 2009 FERC issued its Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing. In this Order FERC approved the Version 2 CIP Reliability Standards and issued four additional directives to NERC that included modifying the

standards, with a required response in 90 days. At that time the SDT had to abandon it plan for addressing the outstanding directives in Order No. 706 and had to immediately address the newly issued directives.

Version 3 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on December 16, 2009. On December 29, 2009, NERC submitted to FERC for approval the Version 3 CIP Reliability Standards. On March 31, 2010 FERC issued its Order on Compliance. In this Order FERC approved the Version 3 CIP Reliability Standards.

Version 4 of the CIP Reliability Standards (CIP-002-4 through CIP-009-4) was developed as an interim step to address the more immediate concerns from FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period. The Commission approved Version 4 on April 18, 2012.

Work has continued on further improvements to the standards, including responses to the remaining Commission directives from FERC Order No. 706, and it is these further enhanced standards that will be submitted to the Commission as Version 5. The next version of the CIP Reliability Standards will build on the Version 4 standards' establishment of uniform criteria for the identification of Critical Assets.

Version 5 of the CIP Reliability Standards provides a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

The changes in Version 5 also present many strategic advantages. Chiefly, a significant deliverable is to close out FERC Order No. 706. More importantly, Version 5 aligns to essential reliability functions and provides significant flexibility to entities in adapting requirements to individual operations.

Version 5 represents a systems-based approach to standards, which provides an opportunity to implement solutions and tailor security based on function, connectivity, risk, and impact. That flexibility represents a significant transition from the "in or out" demarcation for applying requirements in Versions 1 through 4 of the standards, as the drafting team has been able to structure Version 5 in a way that more finely tunes the applicability of each requirement based on connectivity, impact, and other characteristics.

Version 5 is also an experience-based set of standards. It is the first opportunity for the industry to evaluate, consider and incorporate lessons learned from implementation and audit of Versions 1 through 3, and the requirements aim to provide clearer emphasis on the required results. Collectively, the Version 5 standards support continued improvement in support of protecting against compromises that could lead to misoperation or instability in the Bulk Electric System.

NERC Quality Review

In addition to the changes that were made in response to comments, the SDT also submitted the set of standards to NERC for a quality review (QR). In response to the QR, the SDT made several changes for clarity, most of which related to style and form, grammar, word choice, etc.

The Applicability section was modified in response to QR to add "Interchange Authority" to the list of functional entities. The NERC Functional Model lists "Interchange Coordinator" while the registration criteria list "Interchange Authority," and they are not yet synchronized. Until that occurs, the SDT specifies that the standards apply to "Interchange Coordinator or Interchange Authority."
The SDT removed CIP-004-5, Requirement R4, Part R4.2. In previous drafts of the CIP standards (which was Requirement R6), the standard required designation of "one or more individuals" to authorize access, followed by a second requirement part for that individual to authorize based on need. The SDT has determined that the designation of one or more individuals is administrative in nature and is something that should be addressed by the Responsible Entity's plan, not by a requirement part. The performance required is now addressed through one requirement part.

The SDT also removed CIP-006, Requirement R3, Part R3.2, which required that Responsible Entities document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months. This requirement was a documentation requirement, and the SDT, in adding the modifying language to "identify, assess, and correct deficiencies" to Requirement R1, determined that the documentation requirement to log outages was not necessary.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10

7.	Rick Crinklaw	Lane Electric Cooperative	WECC	3
8.	Annie Terracciano	Northern Lights Inc.	WECC	3
9.	Aleka Scott	PNGC	WECC	4
10.	Heber Carpenter	Raft River Electric Cooperative	WECC	3
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC	1, 3
12.	Marc Farmer	West Oregon Electric Cooperative	WECC	4
13.	Margaret Ryan	PNGC	WECC	8

12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14.	Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	M & A Electric Power Cooperative	SERC	1, 3	
4.	Northeast Missouri Electric Power Cooperative	SERC	1, 3	
5.	N.W. Electric Power Cooperative, Inc.	SERC	1, 3	
6.	Sho-Me Power Electric Cooperative	SERC	1, 3	

15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Oglethorpe Power Corporation		SERC	5
2.	Georgia Transmission Corporation		SERC	1

16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWERENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
8.	SCOTT NICKELS	RPU	MRO	4
9.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
10.	MARIE KNOX	MISO	MRO	2
11.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
12.	SCOTT BOS	MPW	MRO	6, 1, 3, 5
13.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
14.	THERESA ALLARD	MPC	MRO	1, 3, 5, 6

17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2.	James Howard	Lakeland Electric	FRCC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Joe Stonecipher	Beaches Energy Services	FRCC	1
6.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7.	Randy Hahn	Ocala Utility Services	FRCC	3

19.	Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Darl Shimko	MGE	MRO	3
2.	Joseph DePoorter	MGE	MRO	4
3.	Steve Schultz	MGE	MRO	5
4.	Jeff Keebler	MGE	MRO	6

20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Jones	Pepco	RFC	1

21.	Group	Rick Terrill	Luminant					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6
9.	Brenda Hampton	Luminant Energy Company LLC		

22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Smith	BANC	WECC	1

23.	Group	Scott Brame	NCEMC	X				X					

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Rayburn Country Electric Cooperative		SPP	
2. Empire District Electric		SPP	1
3. City Utilities of Springfield		SPP	4
4. Westar Energy		SPP	1, 3, 5, 6
5. Cleco Power		SPP	1, 3, 5, 6

25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						

Additional Member	Additional Organization	Region	Segment Selection
1. Pawel Krupa		WECC	1
2. Dana Wheelock		WECC	3
3. Hao Li		WECC	4

27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					

Additional Member	Additional Organization	Region	Segment Selection
1. Denise Lietz	Puget Sound Energy	WECC	1
2. Erin Apperson	Puget Sound Energy	WECC	3

28.	Group	Michael Mertz	PNM Resources	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1. Laurie Williams	Public Service Co. of New Mexico	WECC	1
2. Michael Mertz	Public Service Co. of New Mexico	WECC	3

29.	Group	Sasa Maljukan	Hydro One	X									

Additional Member	Additional Organization	Region	Segment Selection
1. David Kiguel	Hydro One	NPCC	1

30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION A3 – CIP-002-5:

If you disagree with the changes made to CIP-002-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, the SDT made significant changes to attachment 1 and provided clarity to the requirements and associated rationales and measures. The explanations below describe the modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity in language.

Introduction - Section 4 – Applicability
There were several comments on this section in response to question A3, but the issues and responses relate generally to all of the standards. The discussion and response to comments on this section is provided earlier in this document in the Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated section.

Requirement R1
Substantial changes were made to both the structure and the approach in Requirement R1: while the end result is a categorized list of high and medium impact BES Cyber Systems, there were many changes made to address concerns related to Low Impact assets and an asset based approach to deriving BES Cyber Systems. Many comments suggested a more prescriptive approach to the methodology used to arrive at the objective lists, including suggestions to add a flow-chart to the requirement: the SDT made a number of changes to address the "what" instead of the "how", and added substantive qualifications to better define the assets affected.

In particular, several commenters stated that the requirement to review and update the categorization on every change to the BES was an onerous burden in a company with a large number of constantly changing BES Facility configuration. The SDT has reviewed comments and is persuaded by the arguments presented. The SDT also considers that an annual review and update for BES Facilities, given the long term implementation of BES Facility changes, together with the requirements for BES Cyber Systems change control, provide a framework that provides the controls necessary.

Several commenters stated that the requirements for identification in Requirement R1 of CIP-002-5 be modified to require reference to “BES Sites” rather than Facilities, systems and equipment. One comment also suggested that inventories for Low Impact would allow requirements for low impact to be at the site level. Many comments suggested a Facilities impact-based approach to the derivation of the impact of BES Cyber Systems. The SDT has considered the suggestion and made modifications to the current CIP-002-5 requirements to incorporate the concepts using language already used in the criteria and Version 4 approved standards. While the terms Facilities, systems and equipment are precisely the same terms used in the definition of Critical Assets in prior versions, the SDT has made modifications to the proposed language to use the term “assets”, a term familiar to the industry in compliance activities for prior versions.

In response to numerous comments on the issue of asset-based derivation of cyber system impact, the SDT made substantive changes to Requirement R1s language and structure to include this approach. While Requirement R1 is ultimately intended to result in categorized BES Cyber Systems for the application of cyber security requirements, the SDT has made changes to the language and contents of Requirement R1 as well as the criteria in attachment 1 in consideration of comments received.

Several commenters commented on the use of the capitalized term Bulk Power in the rationale for Requirement R1. The paragraph has been deleted and the term is no longer used in the rationale.

One commenter suggested that a bullet is not required in requirement part 1.3 of Requirement R1. The comment also suggested an inconsistency between Requirement R1 and the associated VSL. The SDT has redrafted Requirement R1 in consideration of comments and the bulleted clause is now in the applicable part of the requirement. The inconsistency in the VSL has been corrected.

One commenter suggested that the SDT continues to insist there is no need to identify the low impact BES Cyber Systems and their associated Cyber Assets (e.g., R1.3) and that this causes an auditability issue. The SDT believes that an “asset” based approach in the revised draft and the requirement for the list of assets containing Low Impact BES Cyber Systems provides relief to the auditing issue.

Several commenters requested an explanation of the values used in the VSLs for Requirement R1. The SDT notes that the values are based on FERC Guidelines for VSLs that use percentages. Many entities commented on the need for absolute values for smaller entities since percentages would provide an unfair bias for small entities that would more easily reach percent based thresholds.

One comment stated that the SDT should consider reusing lists generated by other standards. The SDT notes that evidence used for other reliability standards can be presented for these CIP standards as long as they provide the evidence required to demonstrate compliance to the CIP requirement.

One commenter suggested that requirement parts 1.1, 1.2 and 1.3 should also include documentation as part of the requirement and that requirement part 1.4 should require the update prior to commissioning. The SDT's approach to requirement definition focuses on results and believes that a requirement to "document" does not directly result in the reliable operation of the BES. The SDT has defined the required functional result that directly contributes to the reliable operation of the BES. Requirement R1.4 has been removed by SDT in consideration of comments received.

One commenter suggested that by specifying requirements for Low Impact, CIP-002-5 implies a list of BES Cyber Systems. The commenter further suggested either requiring a list of Low Impact Cyber Systems or removing Low Impact altogether. The SDT notes that requirements must be explicit and that CIP-002-5 has made it clear and explicit that a list of Low Impact BES Cyber Systems is not required. However, in the new draft, a list of Low Impact assets is required to facilitate the application of policy requirements to Low Impact assets.

Several commenters suggested many editorial changes to the language used in Requirement R1. The SDT has made fundamental structural and language changes to Requirement R1 to address comments received.

Requirement R2

One commenter suggested that the rationale for Requirement R2 does not include approval of the lists. The SDT notes that the last sentence in the rationale refers to the approval process.

One commenter made many remarks on inconsistencies between the Requirement R2 language, the measure and the VSLs. The SDT has made modifications to R2 and its measures and VSLs for consistency.

Many commenters suggested alternative language, or reverting to the use of the term annual for the clause describing the annual review and approval. One commenter also inquired as to whether the clause supersedes an entity's definition of annual. The SDT has discussed alternative approaches and is using the term "at least once every 15 months" to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. The SDT has intentionally not used the word "annual". This term is no longer used in these CIP standards for periodic requirements

and therefore, the CAN on the word annual can no longer apply in this requirement. One of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify audit interpretation. Instead, the SDT used specific language that implements its intent. This topic is also discussed in greater detail in the introductory, global section of these comment responses.

Attachment 1

Section 1 - High Impact Control Centers

One commenter stated that criteria for control centers fail to consider inter-Control Center connectivity and that the concept of mutual distrust does not work because of trusted paths. The SDT has included consideration of connectivity in the application of requirements. The applicability of mutual distrust depends on specific considerations of network configuration. A blanket statement based on an assumed configuration does not support the generalized comment. The SDT believes that requirements in the standards for protection of BES Cyber Systems provide a basis for Responsible Entities to implement the necessary protection in their network and system design.

Several commenters stated that the introductory text in High and Medium Impact criteria should be deleted or modified due to the change in approach for facilities based impact. The SDT notes that Requirement R1 still requires, ultimately, the categorization of BES Cyber Systems for the application of requirements. The SDT believes that the introductory text in the criteria for High and Medium is still required to express this result.

One commenter suggested on the inclusion of “associated data centers” in the control center criteria and argued that the BES Cyber Systems in these “data centers” would already be included. The SDT has made revisions to the definition of Control Centers, has now included data centers in the definition, and removed the phrase from attachment 1.

Many comments were received on the relationship of TO Control Centers and the functional obligations of TOPs. There was also a comment on the section in the guidance that pertains to TO Control Centers that perform the functional obligations of the TOP. In particular, one comment suggested removal of the guidance, citing ownership issues and issues with NERC Functional Entity registration. The SDT believes that the criterion in question is used to determine the impact of the BES Cyber Systems, and that, irrespective of registration issues, if these Cyber Systems perform a function that is relevant to the functional obligation of a TOP, and that this is formally delegated, then the impact should be appropriately assessed as such. The issue of ownership is a non-issue since the responsibility for compliance to the applicable requirements resides with the owner of the identified BES Cyber Systems that provide that function.

Several commenters suggested that the language used in criterion 1.3 with respect to TOP Control Centers needed clarification and that the guidance for this criterion should explicitly say that TO Control Centers that do not perform the functional obligation of the TOP should be classified as Medium. The SDT has inserted additional guidance to clarify this point. A TO facility that does not perform or does not have an obligation to perform any of the reliability tasks of a BA, TOP or GOP does not meet the definition of a Control Center and the BES Cyber Systems should be evaluated according to the criteria in attachment 1. TOs should review the functional tasks of a TOP and those of a TO and ensure they are not delegated any of these functional tasks through an agreement or a contract. In particular, TOs should note that the functional model does not list real-time operational tasks for that entity.

One commenter asked whether a TO Control Center that performs an operation under the direction of a TOP is performing a functional obligation of a TOP. The NERC Functional Model does not include operation of BES Facilities under the tasks or obligations of a TO, but does include them under the obligations of a TOP. If the TO has an obligation (contractually or because of some other formal agreement) to operate BES assets, whether it is in an emergency or in normal operational circumstances, under the direction of a TOP, then that Cyber System is used to perform the functional obligation of a TOP. The functional obligation of operational control of the BES asset has been delegated to the TO.

One commenter also asked whether a TO data center that collects data and then processes that data for transmission to the TOP is performing a functional obligation of the TOP. The SDT has moved the data center association to the definition of a Control Center and associates it with the facility hosting the operating personnel. In the scenario described, the TO data center is not associated with the BES Cyber Systems owned by the TOP. The “data center” described is analogous to field data aggregating facilities and are evaluated as BES Cyber Systems necessary for providing situation awareness for real-time operations, and should not be evaluated as TOP Control Center “data centers”.

One commenter suggested a number of modifications to the criteria aimed at better stratifying the distinction of Medium from High Impact, especially in the case of BA and TOP Control Centers. The SDT considered the suggestions and has made a number of modifications to address the comments. On another suggestion of increasing the threshold for High Impact BA and GOP Control Centers to 3000 MW, the SDT notes that the stratification of the High Impact from Medium Impact is mostly based on impact due to the wide area reliability tasks of the Functional Entities. However, the SDT has included modifications that provide some stratification of the levels for BA, TOP and GOP Control Centers which are consistent with thresholds approved in Version 4. On the subject of UFLS thresholds, the SDT reviewed recent developments in Regional Standards for UFLS and the tolerances specified in these standards as a basis for evaluation of

the current threshold: the SDT concluded that the current threshold represents a reasonable representation of the level of tolerance in these standards so far.

Several commenters suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

One commenter suggested that the word "control" in the definition of Control Center requires more explanation and that the situation awareness section of the guidelines on BES Reliability Operating Services could include cyber systems used in collecting data for management and engineering analysis. The SDT has provided, in the guideline, the type of operations included in the use of the word. The definition provides further qualification in the context of the Control Center. The word "control" is used in several other standards and is a well understood concept in the BES environment. The intent of the situation awareness section in the guideline on BES Reliability Operating Services is to broadly define a reliability function and is not meant to be used solely for the qualification of applicable BES Cyber Systems: it is intended to be a first step in qualifying a population of Cyber Systems for further application of additional qualifications in the definition of BES Cyber Systems, applicable assets and the impact criteria in attachment 1.

One commenter stated that criteria 1.2 and 1.4 in attachment 1 qualify assets affected as "generation assets" and pointed out that not all assets in scope are strictly "generation assets". The SDT agrees and has made the suggested modification.

One commenter requested clarification on whether the 1500 MW in requirement parts 1.2 and 1.4 of attachment 1 referred to criterion 2.1. The SDT responds that the 1500 MW refers to total aggregate generation of 1500 MW, and is not tied to criterion 2.1.

Section 2 - Medium Impact

Several commenters stated that the 15 minute criterion in requirement part 2.1 of attachment 1 is unnecessary and redundant. Another commenter stated that this 15 minute clause was contrary to the "bright-line" concept. One commenter also stated that the inclusion of the 15 minute qualification in the criteria was inappropriate because the criteria define BES asset impact. The addition of this qualification resulted from previous comments and sought to

provide clarity in the scope of BES Cyber Systems to be included in consideration of this criterion. Where the qualification is included, the language makes it clear that it applies to the effect of the BES Cyber System.

There was a comment that the 15 minute in criterion 2.1 and 2.2 is going to be difficult to prove in an audit and suggested the term "that operate the reactive resource" instead in 2.2. As stated in the guideline, the intent of the 15 minute is to provide a boundary to the impact to real-time operations. The alternative use of the term "real-time" does not provide a useful defined term. The SDT believes that the commenter's suggestion to use the term "that operate" in criterion 2.2 restricts the full scope of cyber systems that affect the real-time operation of the BES for reactive resources.

The commenter further suggested that criterion 2.1 should consider regional operational conditions and requested clarification on the 1000 MVAR threshold for 2.2. For 2.1, the SDT considered regional variations in determining this threshold and notes that this is the approved Version 4 criterion. For 2.2, the SDT consulted with operational and planning experts during the development of this criterion in Version 4.

One commenter stated that the commas around the words "as necessary" in criterion 2.3 were confusing. The SDT has reviewed the criterion and agrees that the commas are misplaced and have altered the intent of the criterion. The SDT has made changes to the placement of the commas to clarify the intent.

One commenter requested clarification on the use of the phrase "long term planning horizon" in criterion 2.3. The SDT notes that criterion 2.3 of attachment 1 does not use the phrase "long term planning horizon" but uses a specified one year or more near-term timeframe. The SDT notes the intent is to avoid the identification of generation facilities that could be used to remediate short term reliability issues.

Two commenters requested additional clarification in the notifications to asset owners in criteria 2.3 and 2.6. For 2.3, the notification is affected as part of the execution of a contract. For 2.6, the applicable IROL reliability standards require that the asset owners be notified. These standards do not specify how the notification is to be done, but that notification must be performed.

One commenter suggested that in requirement part 2.2 of attachment 1, the nameplate value should be qualified to account for ranges. The SDT has included a qualification of "maximum" in the criterion.

One commenter stated that criterion 2.3 references the long term planning horizon, contrary to the real-time operations aspect of the CIP standards. In addition, the commenter suggested that additional guidance be provided as to the notification of such obligations. Also, the commenter requested similar clarification in the guideline for criterion 2.8. The SDT points out that the criterion states that the designation of the asset is performed as part of a planning activity that has a time horizon of one year or more (near-term) by the Planning Coordinator or Transmission Planner, but the impact of a compromise of an affected BES Cyber System would meet the qualification for real-time operations. Additional clarification on notifications has been added to the guideline for criteria 2.3 and 2.8.

One commenter stated that the guidance section that refers to the category D contingency of TPL standards in the discussion of criterion 2.3 is unlikely and suggests removing it. The SDT has removed the reference in the guideline.

One commenter suggested using the phrase "generation interconnection facility" instead of "Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems Transmission Facilities" in criterion 2.8, citing the term used in Project 2010-07. Another commenter suggested on the exclusion of generation plant collector buses in criterion 2.4 and 2.5 in the guidance and suggested an explicit exclusion in the requirement. The SDT reviewed the standards in Project 2010-07 and has not found "generation interconnection facility" as a defined term in the NERC Glossary. The term is however used in the PRC standard in the project. The SDT intends that the application of this criterion to Transmission Owner/Transmission Operator owned and generator owned Transmission Facilities that provide this interconnection of generator output to the Transmission system. However, for clarity and to address the exclusion of these facilities in criteria 2.4 and 2.5 that one comment stated, the SDT has added this term as an inclusion in 2.8.

One commenter suggested alternative language for criterion 2.5 to clarify the application of the aggregate rating. The SDT made modifications to the language in 2.5 to clarify the application of the aggregate to the sum of applicable Transmission facilities at the station.

Many commenters suggested using, for criterion 2.6, the same language used in criteria 2.8 and 2.9. The SDT notes that in criterion 2.6, the criterion refers directly to the Facilities that make up the IROL and has used the exact language used in the IROL standards that require the identification of these specific Facilities. Criteria 2.8 and 2.9 apply to Facilities that could indirectly cause a violation or reduction of the IROLs.

Several comments were on the reasons for the removal of the WECC specific qualifications for those criteria that are based on IROLs. The SDT understands that the commenter has reconsidered its position on IROLs and that other changes in attachment 1 negate the need for any WECC specific qualification.

Several commenters requested information on the standards that require notification of asset owners for IROLs in criterion 2.6. One commenter also stated that the term Control Center is not a NERC defined term and to organize the guidelines by transmission, generation, etc. The SDT notes that the guidelines for criterion 2.6 provides information on the NERC Reliability Standard that contains these requirements (FAC-014) that require identification of these assets and notification to applicable owning Functional Entities. The term Control Center is a proposed defined term in this CIP standards package and the guidelines for criteria are organized by generation and transmission.

One commenter inquired as to why all facilities necessary for the NIPR (not just Transmission Facilities) are not included in criterion 2.7 (Nuclear Interface facilities). The SDT notes that the scope of applicability in NUC-001 is limited to transmission entities listed, which consists of registered entities.

One commenter requested clarification in the application guideline on how, in criterion 2.8, the TO would obtain information on whether generation it does not own or operate meets criterion 2.3. The SDT included additional guidance in the application guideline section.

One commenter stated that the UVLS/UFLS in criterion 2.10 that refers to the 300 MW threshold should specify the lowest rating in the last 12 months. Several commenters stated that the use of the highest MW rating in the guidelines and technical basis on UVLS/UFLS should be changed to “hourly integrated load”. The SDT has not specified the methodology used to determine the 300 MW and has deferred to the requirements of the applicable regional UFLS/UVLS standards.

One commenter stated that criterion 2.10 might imply that individual unconnected relays in a load shedding program under a common trip point would be included and suggested excluding these. The SDT believes that the qualification of a common control system addresses this concern and believes that the exclusion language has the unintended consequence of excluding individual relays irrespective of their impact.

One commenter stated that the language in criterion 2.10 which specifies “regional load shedding programs” is problematic since there is no such requirement and pointed out that PRC standards place the responsibility for

establishing UFLS programs on the Planning Coordinator. The SDT has made modifications to section 4 that pertains to load shedding and criterion 2.10 to more accurately reflect the requirements of the PRC standards.

There was a comment that for criterion 2.10, the language suggests that any compromised component that make up SPS, RAS or automated switching system is required to be protected regardless of if it has an effect on the IROL or not. The SDT notes that the current language does not imply this requirement. The current language only applies if the compromise, whether of one or more components of the SPS, RAS or automated switching system, would cause a violation of one or more IROLs or "cause a reduction of one or more IROLs".

One commenter suggested setting a threshold for Special Protection Systems for applicability of these CIP standards. The SDT notes that all Special Protection Systems, irrespective of any threshold, are designated as Critical Assets under Version 4. The SDT notes that this has been the case because of the critical function provided by Special Protection Systems in the reliable operation of the BES.

Numerous commenters stated that in part 2.11 of attachment 1, the threshold for generation Control Centers should be changed to 1500 MW for consistency with the generation threshold in other criteria in Medium Impact. One commenter also pointed out an inconsistent term in the flow chart in the guidelines and technical basis section. In the same area, another commenter commented that part 2.11 should be removed and that the specific hydro situation should be handled in the definition. The SDT's intent in 2.11 is to include as Medium all the remaining Control Centers not already classified as High, because of the functions provided by Control Centers. In defining a 300 MW threshold for generation Control Centers in 2.11, the SDT was attempting to address a situation specific to hydro-electric generation Facilities. The SDT has removed this artificial threshold in view of changes made to this criterion. Further, the SDT made modifications in the threshold in the criterion for generation Control Centers to address these comments. The inconsistency of terms used in the flowchart has been corrected.

Several entities commented on the removal in draft two of criteria for restoration resources (blackstart units and cranking paths) from the Medium category. Some were in favor of this removal while others were not. Specifically, one commenter made several comments regarding generation and cranking path restoration resources. One comment read that restoration resources should be rated as Medium Impact. In contrast, another commenter suggested that restoration resources should not be included in the scope of the application of the CIP standards because of the absence of the need for remote data communication in the event of a restoration and the exclusion of cranking path from the definition of the BES. In response, in addition to the justification provided as part of the draft two materials, the SDT has

further considered industry input and comments in the consideration of these criteria with respect to their effect on overall reliable operation of the BES and has now removed them from High or Medium Impact criteria. In response, the SDT notes that the assumption that remote access through data communications is necessary for the realization of cyber security threats represents an incomplete mitigation approach, and that the CIP standards are aimed at protecting cyber systems that would impact the real-time operation of the BES, not solely those that directly operate elements of the BES. NERC Reliability Standards that govern the operation of load shedding programs and the protection of the BES elements are other examples of such approaches.

Section 3 – Low Impact

One commenter noted that the criteria in section 3 of attachment 1 should include the phrase "not included in high or medium". The SDT has made the necessary clarification.

General Comments

One commenter suggested that the footnote regarding the effective date of Version 5 and the effective date of Version 4 should be moved to the main text of the effective date. The SDT considered moving this footnote, but believes that movement of the footnote could cause unnecessary confusion, since the effect would not be different. The footnote simply clarifies the effective language that Version 4 does not go into effect and is superseded by Version 5.

There was a comment that the varying language regarding the phrase "destroyed, degraded, or otherwise rendered unavailable" and its variations needs to be consistent. In addition, Southern Company provided additional clarification language for the cranking path criterion in Low Impact. The SDT has reviewed the uses of the term and has ensured consistency when referencing Facilities or BES Cyber Systems. The main difference is the addition of "destroyed" and "otherwise rendered unavailable" in the case of Facilities. The SDT has added the suggested clarification in criterion 3.3.

One comment was on the use of the word "would" instead of "could" in the standards and recommended the use of the prospective word "could". The SDT believes that the use of the word "would" is appropriate to describe the certain impact of a compromise due to an exploitation of vulnerability.

One commenter stated that the last paragraph on page seven leaves it up to the registered entity to determine the level of granularity when identifying the BES Cyber Systems and instructs the registered entity to take into consideration the operational environment and scope of management and raised questions of auditability in the text. The SDT notes that the background and guideline sections are only providing context to the standards. The only auditable parts of the

standards are the applicable definitions and requirements. The SDT directs the commenter to the definition of BES Cyber System for effective application of the requirements.

There was a comment on the examples for Electronic Access Control and Monitoring Systems in the background section, specifically the use of certificate authorities, security event monitoring systems and intrusion detection systems. The SDT uses the term "Certificate Authorities" as an example of the type of cyber assets owned by the Responsible Entity that would be subject to the CIP standards if it relates to a function that is used within the scope of a BES Cyber System. The SDT has used the generic term "security event monitoring systems" as a generic functional term and has specifically avoided the use of the various acronyms used to include this function. This is also true of the term "intrusion detection systems": the SDT is providing an example of the function, and the term "intrusion prevention systems" includes functions that are not within the scope of the requirements. The SDT acknowledges that intrusion prevention systems necessarily include an intrusion detection function.

One commenter suggested the inclusion of network attached storage and storage area networks in the examples for Protected Cyber Assets. Examples provided are not intended to be exhaustive lists, but are intended to provide some examples of the types of systems that could meet the requirements for the definition of Protected Cyber Assets. They are not intended to mean that all of these types of systems are necessarily Protected Cyber Assets, but are examples of systems that could be Protected Cyber Assets if they meet the definition.
SPP suggested footnoting the time horizon reference in requirements. Time Horizons are standard designations used in all requirements and is a standard requirement for all NERC standards requirements. They are required characteristics of each requirement in the same way that Violation Risk Factors are. The SDT believes that footnotes for these are not required as they are generically defined in other NERC documents.

One commenter requested clarification of the general use of transmission facility and its scope. In using terms such as "Facility" in the criteria, the SDT has made substantial changes to Requirement R1 that provides flexibility to the Responsible Entity to define what the term includes within the definition of the requirement. Requirement R1 now includes a listing of the types of assets to be considered that provides a more defined scope to the applicability of CIP-002-5 and the CIP cyber security standards. Within these, Responsible Entities have flexibility in defining the sets within these considerations for application of the criteria.

One commenter requested clarification on entities that have coordination responsibilities. The SDT notes that the table in the guidance provides guidance on those entities that have responsibilities for inter-entity coordination. In a

restoration scenario, those Responsible Entities that require inter-entity coordination to perform their functions that require such coordination have responsibility for this coordination.

One commenter pointed to an inconsistency between the title of the standard and the heading of the document. The SDT corrected the inconsistency.

One commenter stated that the NERC Functional Model does not define Functional Entities. The SDT notes that the current version of the Functional Model (Version 5) defines both Reliability Functions and the Functional Entity that performs the tasks. In addition, there are further responsibilities defined under Functional Entities which are specifically defined in relation with other Functional Entities.

A commenter requested additional guidance in the concept of BES Cyber System. The SDT has made several modifications to the guidance for the overall concept of BES Cyber System, including additional peripheral terms related to BES Cyber Systems, such as Protected Cyber Assets. The SDT believes these additional clarifications provide the additional guidance on the concepts.

There was a comment on the guidance on BES Reliability Operating Services provided for optional use by entities as an aid to scope BES Cyber Systems in the guideline section of the standards. One commenter also suggested removing the designation of Functional Entities for the BES Reliability Operating Services to minimize differing opinions. The SDT made several modifications to this section in consideration of these comments where appropriate. With respect to comments on voltage control and Distribution Providers, the Functional Model clearly lists voltage reduction in its tasks. The designation of Functional Entities is provided as guidance and resulted from comments from previous drafts. The SDT believes that this information provides additional guidance for some Responsible Entities in scoping their BES Cyber Systems.

One commenter suggested that the format of the standard is different and suggested moving the background to the end together with the guideline. The SDT has used the standard template for results based standards and is the recommended standards development format and approach.

There was a suggestion that the rationale should not be part of the standard. The rationale statements will be removed from the official filing and included as information, together with the guidance information.

Several comments were on the use of bright lines and the problem with a one size fits all approach without provisions for studies and engineering analysis and the requirement to require at least some protection for all BES assets. The SDT notes that the objective of Version 5 of the CIP standards is to provide some level of protection to all BES Cyber Systems according to the impact to the real-time operation of the BES assets they are supporting. The bright line based approach was approved by industry stakeholders and FERC as part of Version 4.

One commenter suggested the use of a more definitive term "prevent" in qualifying impact on functions in the reliable operation of the BES. In addition, there was a suggestion for an explanation of the use of the 15 minute window in the definition of BES Cyber Asset. The SDT believes that the word "prevent" does not provide a qualification for the full scope of applicability, but a subset. The intent of the SDT is to ensure that impacts also cover impairment as well as outright "prevention". An explanation of the 15 minute window is in the background section of the standard under real-time operations.

One comment suggested that the stipulation of ownership for compliance responsibility is inconsistent with PRC standards that also stipulate "operate". The SDT has consistently maintained that responsibility for compliance is the asset owner's.

There was a general comment on the application of FISMA and the NIST framework in relation to the CIP standards. The SDT notes that CIP V5 considered the NIST framework as one of the inputs to the drafting of these standards in response to FERC Order 706. The SDT did not consider FISMA requirements, but rather the NIST Risk management framework as directed by Order 706. The SDT also considered input from several other frameworks and has used those inputs in the drafting of standards that are subject to compulsory compliance and enforcement. The NIST 800-53 series is characterized as guidelines for controls, not compliance requirements.

QUESTION A10 – CIP-003-5:

If you disagree with the changes made to CIP-003-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major issues identified through the comment form with CIP-003-5 included (1) the list of low impact BES Cyber Systems for Requirement R2, (2) demonstration of policy implementation, (3) clarity of policy topics in Requirement R2, and (4) the reliability benefit of the annual review/approval of the cyber security policies as well as maintaining documentation of changes to the CIP Senior Manager and delegates.

List of Low Impact BES Cyber Systems for Requirement R2

Numerous commenters identified concerns that while the SDT intended to provide protection from discrete identification of Low Impact BES Cyber Systems, there was still significant concern that this would still be required in order to demonstrate compliance with the requirement. Additionally, commenters suggested that the object of the policy for Low Impact BES Cyber Systems should be on the facilities (or "sites") themselves and not specifically the Low Impact BES Cyber Systems. The SDT continues to believe that the identification of low impact BES Cyber Systems would not be required in order to comply with CIP-003-5 R2. However, the SDT also agrees with commenters that a facilities based approach to the low impact policy comes with a number of benefits. Among these being the creation of a reasonable level of abstraction (the facility) of which to refer to the low impact BES Cyber Systems, thus facilitating any necessary sampling during an audit, without explicitly needing a list of these cyber systems themselves. Consequently, CIP-003-5 R2 has leveraged a reference to CIP-002-5 where facilities with low impact BES Cyber Systems are identified. The SDT believes this approach will provide consistency of application of the policy for low impact BES Cyber Systems, provide a reasonable approach for audit oversight, and create additional clarity on the evidentiary expectations.

Policy Implementation

There were a number of comments that expressed issues with ambiguity in the use of the term "implement" as it relates to the cyber security policies in both CIP-003-5 R1 and R2. In reviewing this comment, the SDT noted that the obligation to "implement" the cyber security policy has existed since version 1 of the CIP standards. Additionally, FERC directed the ERO in Order 706 to "to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards." While this directive did not specifically direct changes to the cyber security policy, as this policy already had the obligation to implement in version 1, the SDT is cognizant that any change to the contrary would require reasonable justification.

As it relates to the CIP-003-5 R1 cyber security policy for medium impact and high impact BES Cyber Systems, the SDT believes there is sufficient justification to make a modification to the language of the requirement in order to provide the clarity that the industry desires around the obligation to "implement." The SDT strongly believes that it has not lessened the obligation to implement the cyber security policy. However, given the required scope of the CIP-003-5 R1 cyber security policies, the SDT believes that implementation of these cyber security policies is effectively demonstrated through compliance with CIP-004-5 through CIP-011-1. Therefore, the SDT has chosen to remove the term "implement" from CIP-003-5 R1. The SDT believes that this should provide clarity as to the expectation of implementation as well as to relieve concerns of double jeopardy between CIP-003-5 R1 and the entire body of CIP-004-5 though CIP-011-1.

The SDT has handled this concern differently for the low impact cyber security policies in CIP-003-5 R2. As there are no corresponding requirements in CIP-004-5 through CIP-011-1 that require explicit implementation of areas addressed by the low impact policy, there are no double jeopardy concerns. The SDT has attempted to provide structure around the obligation to implement the cyber security policies through the global modifications that provide for continuous improvement and the identification, assessment, and correction of deficiencies. The expectation of the SDT is that entities will define cyber security policies that address the four required areas and put these policies in effect using an overall framework that provides reasonable assurance that the policies are applied through methods that identify, assess, and correct any deficiencies.

Policy Topic Clarity for Low Impact Policy

In addition to ambiguity over the implementation of the cyber security policy for low impact BES Cyber Systems, commenters expressed concern over the clarity of the individual policy topics for low impact BES Cyber Systems. The SDT appreciates these comments and has made some modifications to the topic language. However, the SDT understands that these modifications do not completely alleviate the concerns around individual topical clarity. The SDT has modified the topic "Physical access controls" to "Physical security controls" and "Electronic access controls" to "Electronic access controls for external routable protocol connections and Dial-up Connectivity." The SDT chose to not add too much additional detail to these policy topics in recognition of the wide range of environmental, geographic, technical, operational, and logistical differences that may exist amongst the set of low impact BES Cyber Systems. As such, the SDT's intent is to allow Responsible Entities to have flexibility to design and implement the most efficacious security program possible for their particular set of low impact BES Cyber Systems. The modification to physical security controls over physical access controls acknowledges this approach. "Physical security controls" gives great discretion to the Responsible Entity to choose controls that are effective. The SDT believes the paradigm shifts in NERC CIP Reliability

standards allowing for multiple levels of security (high, medium, and low) and creating an atmosphere of continuous improvements through the identification, assessment, and correction of deficiencies will address the concerns of compliance risk that are driving the need for more prescriptiveness in requirements language. Additionally, the SDT added the language to R2.3 "…for external routable protocol connections and Dial-up Connectivity" to address the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact.

Reliability Benefit and Double Jeopardy Concerns of Requirements R3, R5, and R6

Numerous commenters also raised questions about either the reliability benefit or double jeopardy of requirements R3, R5, and R6. Often, these questions were tied to work going on in NERC standards related to Paragraph 81 of the FERC Order approving the FFT process. The comments about their reliability benefit sometimes hinged on them being a requirement in and of themselves, rather than a component of the requirements for R1, R2, and R4 in draft two. The double jeopardy concerns also raised similar questions as to whether a violation of R3, R5, and R6 in draft two would also constitute a violation of R1, R2, and R4 of draft two. The SDT agreed with these concerns. The SDT believes that the same reliability and security objectives will be reached, while alleviating unnecessary compliance concerns, by combining these requirements. As such, the review and approval for each of the cyber security policies has been added as an obligation in the security policy requirements (R1 and R2) themselves. Additionally, the obligation to keep the CIP Senior Manager and delegation documentation up-to-date has been added to those requirements (now R3 and R4), respectively.

Modify Signature to Approval in Measures

Several commenters mentioned the use of "signature" in the measures when the requirement called for "approval." The SDT had never intended to imply that a wet ink signature was the only acceptable form of evidence of approval. Language in the guidelines and technical basis section further clarified that hardcopy or electronic approvals were acceptable. The SDT has modified all instances of "signature" in the measures in CIP-003-5 to "approval' to prevent any confusion and better align with the language in the requirement itself.

Minority Comments

The SDT also received a number of different comments that asked various questions or raised assorted concerns about the topics that were included in Requirement R1. Among other things, these comments mentioned confusion about the guidance related to terms used in the policy topics, inclusion of Interactive Remote Access separate from ESPs, and the relationship between these topics and CIP-004-5 through CIP-011-1. The intention of the SDT was for these policy items

to individually reference each of the standards CIP-004-5 through CIP-011-1. As such, the SDT has chosen to align the policy topics with the title of the other CIP standards (with some exceptions) and include a specific reference to the standards itself in order to clarify that alignment. As mentioned in the discussion of policy implementation above, the SDT's expectation is that implementation of the cyber security policy for medium and high impact BES Cyber Systems will be demonstrated through compliance with CIP-004-5 through CIP-011-1.

Typographical Errors

Several commenters also noted a typographical error where the VRF for CIP-003-5 R2 was listed as low in the requirement and medium in the VSL table. The SDT appreciates commenters pointing this out. The intention of the SDT was for the VRF of CIP-003-5 R1 for medium and high impact BES Cyber Systems to be medium, consistent with CIP-003-4 R1 and for the VRF of CIP-003-5 R2 to be low due to the lesser risk associated with low impact BES Cyber Systems. The SDT has corrected this mistake.

VSL Comments not responded to:

One comment suggested that Requirement R6 should have four VSLs based on days late. The SDT has removed the requirement because the addition of language to identify, assess, and correct deficiencies in what is now Requirement R4 covers the documentation of delegations.

One comment stated to start missing discrete elements of a program as low VSLs in Requirement R2. The SDT has made this change.

One comment suggested to use Lower/Moderate VSLs for Requirement R2 instead. In response, the VSLs only address the degree to which entities can violate a requirement and not the risk power to the BES from said violations.

For the Requirement R4 VSLs, there was a comment that the VSL should read: Lower/Medium – Lack of Review High/Severe – Lack of Approval. This requirement has been removed because the annual review is already accomplished in Requirement R1 and the need to have a CIP Senior Manager sign the policy is administrative in nature.

There was a comment that the VSL for Requirement R3 is more detailed than the requirement itself. The SDT has updated the VSL to match the requirement.

Questions with Votes Only:

1. **Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1?**

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
BC Hydro	No
IRC Standards Review Committee	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No

Organization	Yes or No
Duke Energy	No
Dominion	No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	No
MRO NSRF	No
Florida Municipal Power Agency	No
Madison Gas and Electric Company	No
Luminant	No
SMUD & BANC	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
Western Electricity Coordinating Council	No
CenterPoint Energy	No
Tri-State G&T - Transmission	No
PacifiCorp	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Western Area Power Administration	No
Utility Services Inc.	No
Consumers Energy Company	No
Muscatine Power and Water	No
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	No
NIPSCO	No
Portland General Electric	No
TransAlta Centralia Generation LLC	No
Trans Bay Cable	No
National Grid	No
Hydro-Quebec TransEnergie	No
LCEC	No

Organization	Yes or No
Pacific Gas and Electric Company	No
Ingleside Cogeneration LP	No
Manitoba Hydro	No
Niagara Mohawk (dba National Grid)	No
PSEG	No
Bonneville Power Administration	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
Wisconsin Electric Power Company	No
The Empire District Electric Company	No

Organization	Yes or No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
Nebraska Public Power District	No
City of Austin dba Austin Energy	No
ISO New England	No
Network & Security Technologies, Inc.	No
City Utilities of Springfield, MO	No
American Public Power Association	No
Alliant Energy	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No

Organization	Yes or No
Indiana Municipal Power Agency	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Puget Sound Energy, Inc.	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Tennessee Valley Authority	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
PJM Interconnection	Yes
Kansas City Power & Light	Yes
MEAG Power	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
BC Hydro	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
SMUD & BANC	No
Progress Energy	No
PacifiCorp	No
Utility Services Inc.	No

Organization	Yes or No
NIPSCO	No
LCEC	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
ISO New England	No

Organization	Yes or No
Kansas City Power & Light	No
Indiana Municipal Power Agency	No
Brazos Electric Power Cooperative	No
PPL Corporation NERC Registered Affiliates	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Luminant	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	Yes
Portland General Electric	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Ameren	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
PJM Interconnection	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Duke Energy	No
Progress Energy	No
NCEMC	No
PNM Resources	No
AEP Standards based SME list	No
Xcel Energy	No
MidAmerican Energy Company	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Kansas City Power & Light	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Southwest Power Pool Regional Entity	Yes
NRG Companies	Yes
PNGC Comment Group	Yes

Organization	Yes or No
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Florida Municipal Power Agency	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
New York Power Authority	Yes
Tampa Electric Company	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

5. CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
MRO NSRF	No
Florida Municipal Power Agency	No

Organization	Yes or No
Madison Gas and Electric Company	No
Pepco Holdings Inc & Affiliates	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
AEP Standards based SME list	No
Snohomish County PUD	No
Edison Mission Marketing & Trading	No
Consumers Energy Company	No
Muscatine Power and Water	No
Lower Colorado River Authority	No
LCEC	No

Organization	Yes or No
LCRA Transmission Services Corporation	No
Ingleside Cogeneration LP	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service	No

Organization	Yes or No
Corporation and Upper Pennisula Power Company	
Nebraska Public Power District	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
MEAG Power	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
BC Hydro	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
PNM Resources	Yes
Hydro One	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
NIPSCO	Yes
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
New York Power Authority	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
ISO New England	Yes
City Utilities of Springfield, MO	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
ACES Power Marketing	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Southern Company Services, Inc.	No
Independent Electricity System Operator	No

Organization	Yes or No
Lakeland Electric	No
Tampa Electric Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
American Public Power Association	No

Organization	Yes or No
Tucson Electric Power	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
City of Palo Alto	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
New York Power Authority	Yes
Tennessee Valley Authority	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
ISO New England	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

7. **CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4?**

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Edison Mission Marketing & Trading	No
Independent Electricity System Operator	No

Organization	Yes or No
Pattern	No
United Illuminating Company	No
Lakeland Electric	No
Tampa Electric Company	No
Tennessee Valley Authority	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
New York Power Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
US Bureau of Reclamation	Yes

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
Florida Municipal Power Agency	No
Progress Energy	No
Hydro One	No

Organization	Yes or No
Independent Electricity System Operator	No
Xcel Energy	No
Flathead Electric Co-op	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper	No

Organization	Yes or No
Pennisula Power Company	
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
American Public Power Association	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes

Organization	Yes or No
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes

Organization	Yes or No
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Kansas City Power & Light	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
Progress Energy	No
Portland General Electric	No
Independent Electricity System Operator	No
Flathead Electric Co-op	No

Organization	Yes or No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (JRO00088, NCR01177)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes

Organization	Yes or No
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Trans Bay Cable	Yes

Organization	Yes or No
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes

Organization	Yes or No
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT