Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Note: On September 14, 2012, NERC was alerted that the reference to CIP-002-5 in Requirement R2 of CIP-003-5 was incorrect.

This revised draft corrects the reference from "CIP-002-5, Requirement R2, Part R1.3" to "CIP-002-5, Requirement R1, Part R1.3." It is clear by the reference's context that it should be Requirement R1.

No other changes were made to this standard or any of the other CIP V5 standards currently posted.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).
4. Second posting for 40-day formal comment period and concurrent ballot (April 2012).

Description of Current Draft

This is the ~~second~~third posting of Version 5 of the CIP Cyber Security Standards for a ~~40~~30-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5, which reverted to the original organization of the standards with some changes, was posted in November 2011 for a 60-day comment period and ~~first~~ ballot. ~~–~~ A second posting of Version 5 ~~reverts to the original organization of the standards with some changes and~~was posted in April 2012 for a 40-day comment period and ballot. Version 5 addresses the balance of the FERC directives in its Order No. 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the ~~first~~second posting and ballot.

Anticipated Actions	Anticipated Date
~~40~~30-day Formal Comment Period with Parallel Successive Ballot	~~April~~September 2012
Recirculation ballot	~~June~~November 2012
BOT adoption	~~June~~December 2012

Effective Dates

1. **24 Months Minimum** – ~~The Version 5~~ CIP ~~Cyber Security Standards~~ 003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. ~~Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.~~[1]

2. In those jurisdictions where no regulatory approval is required, ~~the Version~~ CIP-003-5 ~~CIP Cyber Security Standards~~, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	~~Update version from "3" to "4".~~ Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of ~~Functional Entities~~functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific ~~Functional Entity~~functional entity or subset of ~~Functional Entities~~functional entities are the applicable entity or entities, the ~~Functional Entity~~functional entity or ~~Entities~~entities are specified explicitly.

4.1.1 Balancing Authority

~~**4.1.2 Distribution Provider** that owns **Facilities described in 4.2.2**~~

~~**4.1.3 Generator Operator**~~

~~**4.1.4 Generator Owner**~~

~~**4.1.5 Interchange Coordinator**~~

~~**4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1**~~

~~**4.1.7 Reliability Coordinator**~~

~~**4.1.8 Transmission Operator**~~

~~**4.1.9 Transmission Owner**~~

~~**4.2. Facilities:**~~

~~**4.2.1 Load Serving Entity:** One~~one or more of the ~~UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard~~following Facilities, systems, and ~~that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.~~

~~**4.2.2**~~4.1.2 ~~**Distribution Provider**: One or more of the Systems or programs designed, installed, and operated~~equipment for the protection or restoration of the BES:

4.1.2.1 ~~A~~ Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS ~~System~~) system that~~:~~

4.1.2.1.1 is part of a Load shedding program ~~required by~~that is subject to one or more requirements in a NERC or Regional Reliability Standard; and ~~that~~

- **4.1.2.1.2** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

- **4.1.2.2** ~~A~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is ~~required by~~subject to one or more requirements in a NERC or Regional Reliability Standard.

- **4.1.2.3** ~~A~~Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is ~~required by~~ subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~•~~**4.2.1.4** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4.2.3**~~**4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers ~~and Load-Serving Entities:~~** : ~~All BES Facilities.~~

All BES Facilities.

~~**4.2.4**~~**4.2.3 Exemptions:** The following are exempt from Standard CIP-~~002~~003-5:

~~**4.2.4.1**~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.2.4.2**~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.2.4.3**~~**4.2.3.3** ~~In nuclear plants, the Systems~~The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4 -For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

~~Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.~~ The SDT has incorporated within this standard 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. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

~~These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as ~~they feel~~it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the ~~table~~preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

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.

B. Requirements and Measures

Rationale – R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall ~~implement~~review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Personnel ~~security;~~& training (CIP-004);

~~**1.2**~~ Electronic Security Perimeters~~;~~

~~**1.3**~~**1.2** (CIP-005) including Interactive Remote Access;

~~**1.4**~~**1.3** Physical security~~;~~ of BES Cyber Systems (CIP-006);

~~**1.5**~~**1.4** System security~~;~~ management (CIP-007);

~~**1.6**~~**1.5** Incident reporting and response~~;~~ planning (CIP-008);

~~**1.7**~~**1.6** Recovery plans~~;~~ for BES Cyber Systems (CIP-009);

~~**1.8**~~**1.7** Configuration change management~~;~~ and vulnerability assessments (CIP-010);

~~**1.9**~~**1.8** Information protection~~;~~ (CIP-011); and

~~**1.10**~~**1.9** ~~Provisions for declaring~~Declaring and responding to CIP Exceptional Circumstances.

~~**M1.** Evidence must include~~**M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Rationale – R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge 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. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics~~.~~; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

~~**R2.** For BES Cyber Systems not identified as high impact or medium impact, each Responsible Entity shall implement one or more documented cyber security policies that address the following topics: *[Violation Risk Factor: Low] [Time Horizon: Operations Planning]*~~

~~**2.1** Cyber security awareness;~~

~~**2.2** Physical access control;~~

~~**2.3** Electronic access control; and~~

~~**2.4** Incident response to a BES Cyber Security Incident.~~

~~An inventory, list, or discrete identification of BES Cyber Systems is not required.~~

~~**M2.** Evidence must include one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics.~~

Rationale – R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests that the SDT consider whether the single senior manager should be a corporate officer or equivalent. ~~The SDT believes that the requirement that the senior manager have~~ As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name~~.~~ and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. ~~Evidence~~ An example of evidence may include, but is not limited to~~:~~

- ~~A~~, a dated and ~~signed~~approved document from a high level official designating the name of the individual identified as the CIP Senior Manager~~; or~~.

- ~~A dated organizational chart designating the name of the individual identified as the CIP Senior Manager.~~

Rationale – R4:

~~Annual review and approval~~The intent of the ~~cyber~~requirement is to ensure clear accountability within an organization for certain security ~~policy~~matters. It also ensures that ~~the policy is~~ delegations are kept up-to-date and ~~periodically reaffirms management's commitment to~~ that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the ~~protection of its BES Cyber Systems.~~ 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With

~~**R4.** 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. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

~~**M4.** Evidence may include, but is not limited to:~~

1. ~~Revision history, records of review, or workflow evidence from a document management system that indicate annual review of each cyber security policy; and~~
2. ~~A dated signature by the CIP Senior Manager for each cyber security policy that indicates annual approval.~~

~~**Rationale – R5:**~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

~~**R5.**~~

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. 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, the specific actions delegated, and the date of the delegation~~, and~~; approved by the CIP Senior Manager; and updated within 30 days of the initial delegation and any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~**M5.** Evidence~~**M4.** An example of evidence may include, but is not limited to, a dated document, ~~signed~~approved by the CIP Senior Manager, listing ~~named personnel~~individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

~~**Rationale – R6:**~~

~~The intent of the requirement is to ensure that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~**R6.** 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. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

~~**M6.** Evidence may include, but is not limited to, dated documentation that includes the name of the CIP Senior Manager or documentation that includes the names or titles of any delegations, that is current to within 30 days with the name or title of anyone who performed a required approval or authorization.~~

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~entity~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain ~~data or~~ evidence ~~for~~of each requirement in this standard for three calendar years ~~or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer~~.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the ~~duration~~time specified above, whichever is longer.
- ~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	N/A	N/A	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 1.1 to 1.10.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 1.1 to 1.10.
R2	Operations Planning	Medium	N/A	N/A	The Responsible Entity has implemented at least one cyber security policy, but has failed to address one of the required Parts 2.1 to 2.4.	The Responsible Entity has not implemented any cyber security policy, Or The Responsible Entity has implemented at least one policy but has failed to address two or more of the required Parts 2.1 to 2.4.
R3	Operations	Medium	N/A	N/A	N/A	The Responsible Entity has not identified, by

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning					name, a single senior management official ("the CIP Senior Manager") with overall authority and responsibility for leading and managing implementation of the requirements within the CIP group of standards.
R4	Operations Planning	Lower	N/A	N/A	The Responsible Entity has reviewed its cyber security policy or policies, but not all of them have been approved by the CIP Senior Manager within the required time period.	The Responsible Entity has not reviewed the cyber security policy or policies and the CIP Senior Manager has not approved all of them within the required time period.
R5	Operations Planning	Lower	N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by title or name of the delegate) as required.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R6	Operations Planning	Lower	N/A	NA	Change to one delegation was not documented within 30 calendar days of the effective date.	A change to the CIP Senior Manager, Or more than one delegation was not documented within 30 calendar days of the effective date.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the ~~10~~nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel ~~Security~~& training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account ~~Management~~management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points

~~1.3. Remote Access~~

- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating ~~system~~systems and applications used to initiate ~~the Interactive Remote Access before initiating~~ Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

~~1.4~~1.3 Physical ~~Security~~security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress ~~and egress~~

~~1.5~~1.4 System ~~Security~~security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

~~1.6~~1.5 Incident ~~Response~~reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.~~7~~6 Recovery ~~Plans~~plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.~~8~~7 Configuration ~~Change Management~~change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.~~9~~8 Information ~~Protection~~protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

~~1.10 Provisions for~~1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a ~~compliance~~reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

~~Requirement~~ In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the ~~4~~four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the

audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not necessary. The SDT also notes that in ~~topics 2.2 and~~topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

~~In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~**Requirement R5**~~The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement ~~R5~~R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the ~~Standard Drafting Team~~SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. ~~As detailed in the examples provided in the Measure, a~~ A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

~~**Requirement R6:**~~

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.