

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.

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).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-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 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

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

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, 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 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	TBD	Developed to define the configuration management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.	

Definitions of Terms Used in 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 — Configuration Management and Vulnerability Assessments
2. **Number:** CIP-010-1
3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration management and vulnerability assessment requirements in support of protecting BES Cyber Systems from 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 will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or 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 or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.
 - 4.2.2 **Distribution Provider:** One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:
 - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that

performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- 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 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

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

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

4.2.4.3 In nuclear plants, 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.

5. Background:

Standard CIP-010-1 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*.

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for a common subject matter.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. 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.

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 particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

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.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.

- **Associated Physical Access Control Systems** – Applies to each Physical Access Control System associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity in the applicability column.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale – R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

- R1.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management*. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*].
- M1.** Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Develop a baseline configuration, which shall include the following for each Cyber Asset identified, individually or by group: <ul style="list-style-type: none"> 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed on the BES Cyber Asset; 1.1.3. Any custom software developed for the entity; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches. 	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset.
Reference to prior version: <i>New Requirement</i>		Change Rationale: <i>The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.</i>	

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Authorize and document changes that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.
Reference to prior version: CIP-007-3, R9; CIP-003-3, R6		Change Rationale: <i>The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.</i>	
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change that deviates from the existing baseline configuration, update the baseline configuration and other documentation required by CIP-005 and CIP-007 as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to, updated baseline documentation for changes that impacted CIP-005 or CIP-007 documentation, and relevant CIP-005 or CIP-007 documentation, with a date that is within 30 days of the date of the completion of the change.
Reference to prior version: CIP-007-3, R9; CIP-005-3, R5		Change Rationale: <i>Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.</i>	

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify these required controls determined in 1.4.1 and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
Reference to prior version: CIP-007-3, R1		Change Rationale: <i>The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.</i>	

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
1.5	High Impact BES Cyber System	<p>Where technically feasible, for each change that deviates from the existing baseline configuration:</p> <p>1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration to ensure that required cyber security controls are not adversely affected; and</p> <p>1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.</p>	<p>Evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.</p>

CIP-010-1 Table R1 – Configuration Change Management			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
	<p>Reference to prior version: <i>CIP-007-3, R1</i></p>	<p>Change Rationale: <i>This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.</i></p> <p><i>This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.</i></p>	

Rationale – R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

- R2.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring*. [*Violation Risk Factor: Lower*] [*Time Horizon: Operations Planning*].
- M2.** Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
2.1	High Impact BES Cyber Systems Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Where technically feasible, monitor continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate detected unauthorized changes.	Evidence may include, but is not limited to, logs from a system that is monitoring the configuration of the BES Cyber System along with records of investigation for any unauthorized changes that were detected by the system.
Reference to prior version: <i>New Requirement</i>		Change Rationale: <i>The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.</i> <i>This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.</i> <i>Thirty-five Calendar days allows for a “once-a-month” frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.</i>	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

- R3.** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3– Vulnerability Assessments*. [*Violation Risk Factor: Medium*] [*Time Horizon: Long-term Planning and Operations Planning*]
- M3.** Evidence must include each of the applicable documented processes that collectively include each of the applicable items in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	At least once every calendar year, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed.	Evidence may include, but is not limited to: <ul style="list-style-type: none"> • A document listing the date of the assessment (performed at least once every calendar year, not to exceed 15 calendar months between assessments), the controls assessed for each BES Cyber System along with the method of assessment, and the individuals who performed the assessment; or • A document listing the date of the assessment and the output of the tools used to perform the assessment.
Reference to prior version: CIP-005-4, R4; CIP-007-4, R8		Change Rationale: <i>As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.</i>	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months between assessments), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
Reference to prior version: <i>New Requirement</i>		Change Rationale: <i>FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.</i> <i>As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.</i>	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	Applicable BES Cyber Systems and associated Cyber Assets	Requirements	Measures
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset), prior to adding a new Cyber Asset perform an active vulnerability assessment of the new Cyber Asset.	Evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of the tools used to perform the assessment.
Reference to prior version: <i>New Requirement</i>		Change Rationale: <i>FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.</i>	
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems. Associated Physical Access Control Systems Associated Electronic Access Control or Monitoring Systems Associated Protected Cyber Assets	Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).
Reference to prior version: <i>CIP-005-3, R4.5; CIP-007-3, R8.4</i>		Change Rationale: <i>Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.</i>	

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 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 may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for 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 specified above, whichever is longer.
- The Compliance Enforcement Authority 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	<p>The Responsible Entity has established a configuration management program, but failed to authorize any changes to the baseline configuration and to document those changes.</p> <p>OR</p> <p>The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.</p>	<p>The Responsible Entity has not established any configuration management programs.</p> <p>OR</p> <p>The Responsible Entity did not implement a configuration management program</p> <p>OR</p> <p>The Responsible Entity has established a configuration management program, but failed to establish a documented baseline</p> <p>OR</p> <p>The Responsible Entity has established a configuration management program, but with respect to the</p>

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes in the baseline configuration, did not determine the required cyber security controls identified in CIP-005, CIP-006, and CIP-007 that could be impacted by the changes; or did not verify that the controls were not adversely affected when the change was implemented.
R2	Operations Planning	Medium	N/A	N/A	N/A	<p>The Responsible Entity has not established a configuration monitoring process for changes to the baseline.</p> <p>OR</p> <p>The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.</p>

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.
R3	Long-term Planning and Operations Planning	Medium	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not performed an active vulnerability assessment on a new Cyber Asset prior to adding it to an applicable BES Cyber System. OR	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems.	The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. OR

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems.</p>		<p>The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems.</p> <p>OR</p> <p>The Responsible Entity has established and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but failed to perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline</p>

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						configuration of its applicable BES Cyber Systems. OR The Responsible Entity has established one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, and the execution status of the mitigation plans.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Application Guidelines

Guidelines and Technical Basis

Requirement R1:

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their Vulnerability Assessment processes, Responsible Entities are strongly encouraged to include at least the following elements:

Paper Vulnerability Assessment

1. Network Discovery - A review of all Electronic Access Points to the Electronic Security Perimeter
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications

Application Guidelines

Active Vulnerability Assessment

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.