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).

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-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. This version (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.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the 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 standards shall become effective on the first day of the seventh 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 Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Configuration Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: Standard CIP-010-1 requires that Responsible Entities have minimum configuration management and vulnerability assessment controls in place to protect BES Cyber Assets and BES Cyber Systems.

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 that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-010-1

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.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

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*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

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 specific elements required 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 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 infer any 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.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the 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.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization processes. 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.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as Medium 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.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems** – Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. 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 or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points** – Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

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	**Applicability**	**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 of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels.	Evidence may include, but is not limited to: • A spreadsheet identifying the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System; • A record in an asset management system that identifies the required items of the baseline configuration for each BES Cyber Asset in the BES Cyber System.
Reference to prior version: *New Requirement*		**Change Rationale:** *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.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**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	Authorization, by the CIP Senior Manager or delegate, and document changes to the BES Cyber System that deviate from the existing baseline configuration.	Evidence may include, but is not limited to: • A change request record and associated electronic approval (performed by the individual with the authority to authorize the change) in a change management system for each change; • A record of each change performed along with the minutes of a "change advisory board" meeting (that indicate authorization of the change) where an individual with the authority to authorize the change was in attendance.
Reference to prior version: *CIP-007-3 R9* *CIP-003-3 R6*		**Change Rationale:** *The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3 R6.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
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	Update the baseline configuration and other documentation required by a NERC CIP Standard, including identification and categorization of the BES Cyber Systems, as necessary within 30 calendar days of completing the change.	Evidence may include, but is not limited to: • For changes that impacted the categorization of a BES Cyber System, dated categorization documents, with a date that is within 30 days of the date of the completion of the change; • For changes that impacted the CIP-009-required recovery plan of a BES Cyber System, a dated recovery plan, 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*		**Change Rationale:** *Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**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 to the BES Cyber System that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls that could be impacted by the change; 1.4.2. Following the change, verify these required controls and the BES Cyber System availability are not adversely affected; and 1.4.3. Document the results of the verification.	Evidence includes, but is not limited to a list of security controls verified or tested along with the dated test results.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *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.*	

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicability**	**Requirements**	**Measures**
1.5	High Impact BES Cyber System	For each change that deviates from the existing baseline configuration for Control Centers: 1.5.1. Prior to implementing any change in the production environment, test the changes to the BES Cyber System in a test environment that models the baseline configuration of the BES Cyber System to ensure that required cyber security controls are not adversely affected; and 1.5.2. Document the results of the testing and 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 includes, but is not limited to, a list of 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.
Reference to prior version: *CIP-007-3 R1*		**Change Rationale:** *This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.* *This change addresses FERC Order ,paragraphs 397, 609, 610, and 611*	

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	**Applicability**	**Requirements**	**Measures**
2.1	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	Where technically feasible, monitor for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1) and document and investigate the detection of any 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: *New Requirement*		**Change Rationale:** *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.* *This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order 706, paragraph 397.DHS Catalog & addresses FERC Order 706, paragraph 397.*	

Rationale – R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of 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: 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	**Applicability**	**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	Initially upon the effective date of the standard and at least every calendar year thereafter, not to exceed 15 calendar months between assessments, conduct a paper or active assessment of the security controls to determine the extent to which the controls are implemented correctly and operating as designed.	Evidence may include, but is not limited to: • A document listing the date of the assessment (performed at least each 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; • 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 and CIP-007-4, R8*		**Change Rationale:** *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Initially upon the effective date of the standard and at least once every 3 calendar years thereafter, not to exceed 39 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment. 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 within 39 calendar months of the previous assessment), 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: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547* *As suggested in FERC Order 706 paragraph 644, the details for what should be included in the assessment are left to guidance.*	
3.3	High Impact BES Cyber Systems Associated Electronic Access Control or Monitoring Systems	Except for CIP Exceptional Circumstances, prior to adding a new Cyber Asset to a BES Cyber System or Electronic Access Control or Monitoring System, perform an active vulnerability assessment of the 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 BES Cyber Asset) and the output of the tools used to perform the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicability**	**Requirements**	**Measures**
Reference to prior version: *New Requirement*		**Change Rationale:** *FERC Order 706 p. 541, 542, 544, 547*	
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 that action plan.	Evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items with proposed dates of completion, 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: *CIP-005-3 R4.5* *CIP-007-3 R8.4*		**Change Rationale:** *Added a requirement for an entity planned date of completion as per the FERC directive in Order 706, paragraph 643.*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

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 complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for since the last completed audit or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant 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**	**Lower**	**N/A**	The Responsible Entity updated the baseline configuration, but failed to update the required documentation within 30-days of the change being completed.	The Responsible Entity has established a configuration management program, but failed to establish a documented baseline. OR The Responsible Entity has established a configuration management program, but failed to have the CIP Senior Manager or delegate authorize any changes to the baseline configuration and to document those changes. OR The Responsible Entity has established a configuration management program, but with respect to the	The Responsible Entity has not established any configuration management programs. OR Did not implement a configuration management program.

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 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**	**Lower**	**N/A**	**N/A**	The Responsible Entity has established a configuration monitoring process for changes to the baseline but failed to document a detected unauthorized change.	The Responsible Entity has not established a configuration monitoring process for changes to the baseline. OR The Responsible Entity has not investigated a detected unauthorized change to the baseline configuration.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**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 BES 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	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 The Responsible Entity has not established any vulnerability assessment processes for one of its applicable BES Cyber Systems.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				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.		OR 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 that models the baseline 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

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						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.

Guidelines and Technical Basis

Requirement R1:

The physical location referred to in the baseline configuration is geographically where the BES Cyber Asset is located (e.g. Pine Valley Control Room, Generator X, Substation Y) and should be used to ensure that BES Cyber Systems receive the controls that are applicable to the environment in which the components are located (e.g. control center, transmission facility, generation facility). The physical location is not intended to be a specific floor plan location (e.g., panel A, rack B). As such, the physical location of virtual component should identify where the virtual components are being executed (e.g. Pine Valley Control Room, Generator X, Substation Y).

The Control Center test environment 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, patch level, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple.

Additionally, the entity should note that wherever a test environment 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 control center BES Cyber System which may not be able to be replicated such as 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:

It should be understood that the intent of R2 is to require automated monitoring of the BES Cyber System. However, the Standards Drafting Team understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). It is for this reason that automated technical monitoring was not explicitly required and an entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should not that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well documented in the initial NOPR from FERC as well as FERC Order 706. 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

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.