NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2014-02 - Cyber Security - Order No. 791 Identify, Assess, and Correct; Low Impact; Transient Devices; and Communication Networks Directives

Violation Risk Factor and Violation Severity Level Justifications

The tables in this document provide a working draft of the analysis and justification for each Violation Risk Factor (VRF) and Violation Severity Level (VSL) for each requirement in the CIP Cyber Security Standards revisions that address the Order No. 791 identify, assess, and correct; low impact; transient devices; and communication networks directives.

Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines.

The CIP Version 5 Revisions Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria – VRFs

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC VRF Guidelines

Guideline (1) — Consistency with the Conclusions of the Final Blackout Report

The Commission seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System.

In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

Emergency operations

Vegetation management

Operator personnel training

Protection systems and their coordination

Operating tools and backup facilities

Reactive power and voltage control

System modeling and data exchange

Communication protocol and facilities

Requirements to determine equipment ratings

Synchronized data recorders

Clearer criteria for operationally critical facilities

Appropriate use of transmission loading relief

Guideline (2) — Consistency within a Reliability Standard

The Commission expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) — Consistency among Reliability Standards

The Commission expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) — Consistency with NERC's Definition of the VRF Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) — Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria - VSLs

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on the guidelines shown in the table below:

Lower	Moderate	High	Severe
Missing a minor element (or a small percentage) of the required performance The performance or product measured has significant value as it almost meets the full intent of the requirement.	Missing at least one significant element (or a moderate percentage) of the required performance. The performance or product measured still has significant value in meeting the intent of the requirement.	Missing more than one significant element (or is missing a high percentage) of the required performance or is missing a single vital Component. The performance or product has limited value in meeting the intent of the requirement.	Missing most or all of the significant elements (or a significant percentage) of the required performance. The performance measured does not meet the intent of the requirement or the product delivered cannot be used in meeting the intent of the requirement.

FERC Orders on VSLs

In its June 19, 2008 Order on VSLs, FERC indicated it would use the following four guidelines for determining whether to approve VSLs:

Guideline 1: VSL Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

- Compare the VSLs to any prior Levels of Non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when Levels of Non-compliance were used.

Guideline 2: VSL Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

- Guideline 2a: A violation of a "binary" type requirement must be a "Severe" VSL.
- Guideline 2b: Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline 3: VSL Assignment Should Be Consistent with the Corresponding Requirement

- VSLs should not expand on what is required in the requirement.

Guideline 4: VSL Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

. . . unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

In its March 18, 2010 Order Addressing VSL Assignments in CIP Standards, FERC offered the following additional guidance relative to VSLs for CIP requirements:

Guideline 5: Requirements Where Single Lapse in Protection Result in Compromised Computer Network Security

Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary rather than gradated Violation Severity Levels.

Guideline 6: VSLs Should Account for Interdependent Tasks

Violation Severity Levels for cyber security Requirements containing interdependent tasks of documentation and implementation should account for their interdependence.

VRF and VSL Justifications – CIP-003-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Security policies enable effective implementation of the CIP 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. Periodic 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. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. Failure to provide clear governance may lead to ineffective controls, which could compromise security; and, therefore, the integrity of the Bulk Electric System. Consequently, a VRF of Medium was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security policy that contains certain elements specified in the requirement. The VRF is only applied at the requirement level, and the requirement parts are treated in aggregate. While the requirement specifies a number of elements, not necessarily parts, that must be included in the cyber security policy, the VRF is reflective of the policy as a whole. Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards.

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-003-6, R1</th></tr>
<tr><td></td><td colspan="3">This requirement maps from CIP-003-5, R1, which has an approved VRF of Medium; therefore, the proposed VRF remains consistent.</td></tr>
<tr><td>FERC VRF G4 Discussion</td><td colspan="3">Guideline 4- Consistency with NERC Definitions of VRFs.
Failure to properly implement the cyber security policy is unlikely, under Emergency, abnormal, or restoration conditions anticipated by the preparations to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Therefore, this requirement was assigned a Medium VRF.</td></tr>
<tr><td>FERC VRF G5 Discussion</td><td colspan="3">Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.
The cyber security policy requirement encompasses a number of policy domains. The VRF is identified at the risk level represented by all of the policy domains in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.</td></tr>
<tr><th colspan="4">Proposed VSLs</th></tr>
<tr><th>Lower</th><th>Moderate</th><th>High</th><th>Severe</th></tr>
<tr><td>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1.1)
OR
The Responsible Entity did not complete its review of the one</td><td>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1.1)
OR
The Responsible Entity did not complete its review of the one</td><td>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1.1)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security</td><td>The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1.1)
OR
The Responsible Entity did not have any documented cyber security policies for its high impact</td></tr>
</table>

VRF and VSL Justifications – CIP-003-6, R1			
or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.1) OR	or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.1) OR	policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but	and medium impact BES Cyber Systems as required by R1. (R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing

VRF and VSL Justifications – CIP-003-6, R1			
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address one of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the	The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but did not address two of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the	did not address three of the four topics required by R1. (R1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal	low impact BES Cyber Systems, but did not address any of the four topics required by R1. (R1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

VRF and VSL Justifications – CIP-003-6, R1			
one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1.2)	one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1.2)	to 18 calendar months of the previous approval. (R1.2)	

VRF and VSL Justifications – CIP-003-6, R1	
NERC VSL Guidelines	Meets NERC’s VSL Guidelines—There is an incremental aspect to a violation of this requirement, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to previously approved requirements CIP-003-5 R1 and CIP-003-5 R1.2. The VSLs were combined for these requirements using a gradated methodology. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-003-6, R1	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement; and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.

VRF and VSL Justifications – CIP-003-6, R1	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required topics. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-6, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements for low impact BES Cyber Systems. The purpose of plans is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan,

VRF and VSL Justifications – CIP-003-6, R2	
	Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in the Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-5, R1, which has an approved VRF of Lower but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security plan would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VRF and VSL Justifications – CIP-003-6, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented one or more Cyber	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 1. (R2) OR The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to CIP-003-	The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-	The Responsible Entity failed to document or implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1. (R2)

VRF and VSL Justifications – CIP-003-6, R2			
Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to CIP-003-6, Requirement R2, Attachment 1, Section 4. (R2)	6, Requirement R2, Attachment 1, Section 4. (R2) (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) according to CIP-003-6, Requirement R2, Attachment 1, Section 4. OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems,	003-6, Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity documented and implemented electronic access controls for LERC, but failed to implement a LEAP or permit inbound and outbound access according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity documented and implemented electronic access controls for its assets containing low impact BES Cyber Systems, but failed to document and implement authentication of all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)	

VRF and VSL Justifications – CIP-003-6, R2			
	but failed to document physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to CIP-003-6, Requirement R2, Attachment 1, Section 3. (R2)	OR The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to CIP-003-6, Requirement R2, Attachment 1, Section 2. (R2)	

VRF and VSL Justifications – CIP-003-6, R2	
NERC VSL Guidelines	Meets NERC’s VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented its cyber security plan(s) but fails to address one or more of the required sections of the cyber security plan(s). The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-003-5 R2. The proposed VSLs removed the “identify, assess, and correct” concept and incorporated the elements of the Attachment 1 but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-003-6, R2	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.

VRF and VSL Justifications – CIP-003-6, R2	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-6, R4	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability purpose of this requirement is to ensure clear lines of authority and ownership for security matters that could impact the stability and integrity of the Bulk Electric System, that delegations are kept up-to-date, and that individuals do not assume undocumented authority. As this requirement is only a part of the overall governance structure of a cyber security program, which includes additional leadership and policy, a VRF of Lower was assigned to this requirement.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement directs that the CIP Senior Manager is responsible for all approval and authorizations, but also grants the CIP Senior Manager with the ability to delegate this authority. The Requirement also calls for changes to the CIP Senior Manager and any delegations to be documented within 30 calendar days. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The requirement does not contain parts and are, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-003-5, R4, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to show clear authorization for actions taken back to the CIP Senior Manager would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The obligation of this requirement is to demonstrate that the CIP Senior Manager is ultimately responsible for all approvals and authorizations required in the CIP Standards. This requirement allows for delegation, but also obligates the Responsible Entity to document these delegations. The VRF was chosen based upon the highest reliability risk objective, which is the clear line of authority to the CIP Senior Manager and are, therefore, consistent with VRF Guideline 5.

VRF and VSL Justifications – CIP-003-6, R4			
Proposed VSLs			
Lower	Moderate	High	Severe
The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

VRF and VSL Justifications – CIP-003-6, R4	
NERC VSL Guidelines	Meets NERC’s VSL Guidelines—There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. There is a single element upon which severity may be gradated; as such, gradated VSLs were assigned.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-003-5 R4. The proposed VSLs removed the “identify, assess, and correct” concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-003-6, R4	
Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The requirement contains interdependent tasks of documentation and implementation. The VSL requirement presumes that the only way to demonstrate compliance is through documentation; as such, the VSLs are based upon the documentation measure, and implementation is assumed with documentation, therefore accounting for the interdependence in these tasks.

VRF and VSL Justifications – CIP-004-6, R2

Proposed VRF	LOWER
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective would not have adverse effect on the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-5.1, R2, which has an approved VRF of Lower.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a training program would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.

Proposed VSLs

Lower	Moderate	High	Severe
The Responsible Entity implemented a cyber security training program but failed to include one of	The Responsible Entity implemented a cyber security training program but failed to include two of the training	The Responsible Entity implemented a cyber security training program but failed to include three of the training	The Responsible Entity did not implement a cyber security training program appropriate to

VRF and VSL Justifications – CIP-004-6, R2			
the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-004-6, R2</th></tr>
<tr><td></td><td></td><td></td><td>with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)</td></tr>
</table>

VRF and VSL Justifications – CIP-004-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.

VRF and VSL Justifications – CIP-004-6, R2	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation,	The VSLs are based on a single violation and not cumulative violations.

VRF and VSL Justifications – CIP-004-6, R2	
Not on A Cumulative Number of Violations	
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This VSL accounts for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation.

VRF and VSL Justifications – CIP-004-6, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.

VRF and VSL Justifications – CIP-004-6, R3	
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for implementing a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the Requirement level and the requirement parts are treated equally. Each Requirement Part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-5.1, R2, which has an approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a security training program could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining

VRF and VSL Justifications – CIP-004-6, R3			
physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR	physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical	authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR

VRF and VSL Justifications – CIP-004-6, R3			
The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or

VRF and VSL Justifications – CIP-004-6, R3			
			more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)

VRF and VSL Justifications – CIP-004-6, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R3. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations. The requirement is to implement a training program and failure for a single individual to have training does not necessarily imply a single violation. An overall view of the training program must consider the number of individuals who failed to receive training for a given period.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security. Although failure to implement a training program could associatively affect the ways in which computer network security applies, it does not, by itself, indicate a failure of computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This Requirement pertains to implementing the cyber security program and does not require procedural documentation.

VRF and VSL Justifications – CIP-004-6, R4	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have received a personnel risk assessment. Failure to meet this objective could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for a personnel risk assessment program for individuals needing or having access to a BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement's VRF is consistent with similar security requirements with similar risks in the other CIP standards.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a personnel risk assessment program could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that documentation a personnel risk assessment is developed for individuals with access to BES Cyber Systems and, therefore, does not co-mingle more than one obligation.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter	The Responsible Entity did not implement any documented program(s) for access management. (R4)

VRF and VSL Justifications – CIP-004-6, R4			
during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and	during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and	but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 10%	OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

VRF and VSL Justifications – CIP-004-6, R4			
necessary within 15 calendar months of the previous verification but for 5% or less of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of itsBES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	but less than (or equal to) 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber Systems, privileges were incorrect or unnecessary. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BES Cyber System Information storage locations, privileges were incorrect or unnecessary. (4.4)

VRF and VSL Justifications – CIP-004-6, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R4. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document or implement all required documented program(s) has a binary Severe VSL. Other Requirement Parts associated with the required processes do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-004-6, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Failure to revoke access to BES Cyber Systems and BES Cyber System Information within the required time frame is an administrative requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to revoke access to BES Cyber Systems and BES Cyber System Information when individuals no longer need access. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. Each Requirement row contributes to the objective of this Requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-5.1, R5, which has an approved VRF of Medium. Therefore, the proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to revoke access to BES Cyber Systems and BES Cyber System Information may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this Requirement, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Requirement R5 requires prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Each part of Requirement R5 specifies the obligations to revoke access in various situations when an individual no longer needs such access.

VRF and VSL Justifications – CIP-004-6, R5			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.4) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following

VRF and VSL Justifications – CIP-004-6, R5			
The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.5) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.5)	day following the predetermined date. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (5.3)	reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)

VRF and VSL Justifications – CIP-004-6, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-004-5.1 R5. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-004-6, R5	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to implement programs for access revocation has a binary Severe VSL. A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-006-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this Requirement. The requirement specifies that each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. Failure to restrict physical access to BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets could result in unauthorized access, which could directly affect the ability to monitor or control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-5, R1, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-6, R1 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-006-6, Requirement R1 requires the implementation of documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. A failure to implement these documented plans may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this requirement,

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-006-6, R1</th></tr>
<tr><td></td><td colspan="3">if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.</td></tr>
<tr><td>FERC VRF G5 Discussion</td><td colspan="3">Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.
The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets and, therefore, does not co-mingle more than one obligation.</td></tr>
<tr><th colspan="4">Proposed VSLs</th></tr>
<tr><th>Lower</th><th>Moderate</th><th>High</th><th>Severe</th></tr>
<tr><td>N/A</td><td>N/A</td><td>N/A</td><td>The Responsible Entity did not document or implement physical security plans. (R1)
OR
The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1)
OR
The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2)</td></tr>
</table>

VRF and VSL Justifications – CIP-006-6, R1			
			OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each

VRF and VSL Justifications – CIP-006-6, R1			
			Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9) OR

VRF and VSL Justifications – CIP-006-6, R1			
			The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-006-5 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary in the "Severe" category and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.

VRF and VSL Justifications – CIP-006-6, R1	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

VRF and VSL Justifications – CIP-006-6, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. This Requirement calls for one or more documented visitor control programs. Failure to implement a visitor control program is not expected to directly affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented visitor control programs. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-5, R2, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-6, R2 is consistent.

VRF and VSL Justifications – CIP-006-6, R2			
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a documented visitor control program is an administrative requirement, and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented visitor control programs and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor’s name, and the point of contact. (2.2) OR

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-006-6, R2</th></tr>
<tr><td></td><td></td><td></td><td>The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)</td></tr>
</table>

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are binary in the “Severe” category and therefore do not lower the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary in the “Severe” category and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the ‘weakest link’ characteristic, should apply binary VSLs	The proposed VSL is binary and assigns a “Severe” category for the violation of the Requirement.

VRF and VSL Justifications – CIP-006-6, R2	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.

VRF and VSL Justifications – CIP-007-6, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The Requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports. Depending on the port and the impact classification of the affected cyber asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the Requirement level, and the Requirement Parts are treated equally. Unprotected logical and physical ports are both access points into a BES Cyber System.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R1, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs.

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-007-6, R1</th></tr>
<tr><td></td><td colspan="3">Failure to disable or prevent access to a single logical or physical port on one BES Cyber System is unlikely to lead to Bulk Electric System instability, separation, or cascading failures. Therefore, this Requirement was assigned a Medium VRF.</td></tr>
<tr><td>FERC VRF G5 Discussion</td><td colspan="3">Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.
Unprotected logical and physical ports are both access points into a BES Cyber System.</td></tr>
<tr><th colspan="4">Proposed VSLs</th></tr>
<tr><th>Lower</th><th>Moderate</th><th>High</th><th>Severe</th></tr>
<tr><td>N/A</td><td>The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (1.2)</td><td>The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled. (1.1)</td><td>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R1. (R1)</td></tr>
</table>

VRF and VSL Justifications – CIP-007-6, R1	
NERC VSL Guidelines	Meets NERC’s VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-007-5 R1. The proposed VSLs removed the “identify, assess, and correct” concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement at the moderate or high VSL category would not necessarily compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The Requirement requires entities to manage security patches in a proactive way by monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner. Depending on the patch and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-007-5, R2, which has an approved VRF of Medium. Therefore the VRF is consistent with the FERC-approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage a security patch on one BES Cyber System is unlikely to lead to BES instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirement does not co-mingle more than one obligation. It defines required steps in a single process.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets. (2.1)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R2. (R2) OR

VRF and VSL Justifications – CIP-007-6, R2

evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (2.3)	evaluating cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan	OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (2.3)	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (2.4)

VRF and VSL Justifications – CIP-007-6, R2			
	within 50 calendar days but less than 65 calendar days of the evaluation completion. (2.3)		

VRF and VSL Justifications – CIP-007-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines— There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but failed to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement a security patch can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability. There may be instances where the security vulnerability is so severe that failure to patch alone can comprise computer network security, but these cases are the exception.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R3			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The requirement requires entities to have processes to limit and detect the introduction of malicious code onto the components of a BES Cyber System. Depending on the malware and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R3, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage malicious code on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR

VRF and VSL Justifications – CIP-007-6, R3			
		The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (3.3).	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (3.1)

VRF and VSL Justifications – CIP-007-6, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R3. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement malicious code protections can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R4	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The requirement requires entities to have processes to provide security event monitoring with the purpose of detecting unauthorized access, reconnaissance, and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. Depending on the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-5, R4, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage security events on one BES Cyber System is unlikely to lead to BES instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by	The Responsible Entity did not implement or document one or more process(es) that included the

VRF and VSL Justifications – CIP-007-6, R4			
Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (4.4)	Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (4.4)	the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (4.4)	applicable items in CIP-007-6 Table R4. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (4.1)

VRF and VSL Justifications – CIP-007-6, R4	
NERC VSL Guidelines	Meets NERC’s VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R4. The proposed VSLs removed the “identify, assess, and correct” concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the Requirement.

VRF and VSL Justifications – CIP-007-6, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement Parts for logging required types of events have a binary Severe VSL. Other Requirement Parts associated with security event monitoring do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-6, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities establish, implement, and document controls for electronic access to BES Cyber Systems. This includes enforcement of authentication for all user access and CIP Senior Manager, or delegate authorization for use of administrator, shared, default, and other generic account types. It prescribes procedural controls and conditions for changing default passwords and enforcing specific parameters for password based user authentication. Finally, it helps establish a process to limit (where technically feasible) unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for specific actions represented by multiple sub-requirements with a common set of objectives – to ensure the appropriate controls are in place for authorizing and establishing secure electronic access to BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007-5, R5, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement CIP Senior Manager oversight and establish controls to protect BES Cyber Systems from unauthorized electronic access could result in unauthorized access and could directly affect the ability to monitor or control the BES. Although the previous standards versions assigned a VRF of Severe, this is not consistent with the projected risk of BES Cyber System exploitation, which is why the VRF has been modified to Medium.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R5 have a common objective to provide controls to protect against unauthorized electronic access to BES Cyber Systems. The Requirements to authorize and review access, and the

VRF and VSL Justifications – CIP-007-6, R5			
	provided technical and procedural controls to prevent unauthorized access both specify the obligations to provide strong controls to monitor and control electronic access.		
Proposed VSLs			
Lower	Moderate	High	Severe
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce

VRF and VSL Justifications – CIP-007-6, R5			
		interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (5.6)	authentication of interactive user access. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not

VRF and VSL Justifications – CIP-007-6, R5			
			technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

VRF and VSL Justifications – CIP-007-6, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-007-5 R5. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-007-6, R5	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations. Gradations are based on the number of unidentified account types, or number of missed controls for authentication and access represent components of the overall requirement that are necessary to fully achieve the reliability of the main requirement.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement parts that can compromise computer network security have a Severe VSL. Other Requirement Parts associated with system access control do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-009-6, R2</th></tr>
<tr><td><b>Proposed VRF</b></td><td colspan="3"><b>LOWER</b></td></tr>
<tr><td>NERC VRF Discussion</td><td colspan="3">This Requirement’s VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.</td></tr>
<tr><td>FERC VRF G1 Discussion</td><td colspan="3">Guideline 1- Consistency with Blackout Report.
N/A</td></tr>
<tr><td>FERC VRF G2 Discussion</td><td colspan="3">Guideline 2- Consistency within a Reliability Standard.
Each Requirement row contributes to the common objective of implementing and maintaining the recovery plan.</td></tr>
<tr><td>FERC VRF G3 Discussion</td><td colspan="3">Guideline 3- Consistency among Reliability Standards.
This requirement maps from CIP-009-5, R2, which has an approved VRF of Lower.</td></tr>
<tr><td>FERC VRF G4 Discussion</td><td colspan="3">Guideline 4- Consistency with NERC Definitions of VRFs.
Failure to implement and maintain the recovery plan is an administrative Requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.</td></tr>
<tr><td>FERC VRF G5 Discussion</td><td colspan="3">Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.
The requirements in R2 have a common objective of implementing and maintaining recovery plans. Requirement Rows 2.1 and 2.3 specify the obligation to implement and test the plan. Requirement Row 2.2 specifies the obligation to maintain backup information used to recover the BES Cyber System.</td></tr>
<tr><th colspan="4">Proposed VSLs</th></tr>
<tr><th>Lower</th><th>Moderate</th><th>High</th><th>Severe</th></tr>
<tr><td>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months</td><td>The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar</td><td>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1)</td><td>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1)</td></tr>
</table>

VRF and VSL Justifications – CIP-009-6, R2			
between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (2.3)	months between tests of the plan. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3)

VRF and VSL Justifications – CIP-009-6, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to the previously-approved requirement CIP-009-5 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-009-6, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this requirement indicates the recovery plan was not properly tested and may have deficiencies, but a violation cannot immediately compromise computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This Requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-010-2, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration change management processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration change management processes can have a medium impact on the reliability and operability of the BES. Although the requirement is administrative in nature and is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration change management. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, R1 specifies the implementation of documented configuration change management processes in conjunction with CIP-010-2, R2, which specifies the implementation of documented configuration monitoring processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R1 requires the implementation of documented configuration change management processes. A failure to implement these documented processes has medium impact on the

VRF and VSL Justifications – CIP-010-2, R1

	reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-2, Requirement R1 addresses a single objective and has a single VRF.

Proposed VSLs

Lower	Moderate	High	Severe
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that

VRF and VSL Justifications – CIP-010-2, R1			
			deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did

VRF and VSL Justifications – CIP-010-2, R1			
			not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

VRF and VSL Justifications – CIP-010-2, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-010-1 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the ‘weakest link’ characteristic, should apply binary VSLs	A single lapse in protection is not expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R1 specifies that a Responsible Entity must implement and document the processes for configuration change management of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity “addressed” all the required elements of the configuration change management process. The drafting team’s intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-2, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration monitoring processes. A VRF assignment of Medium is consistent with the lower risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration monitoring processes has medium impact on the reliability and operability of the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration monitoring. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, R2 specifies the implementation of documented configuration monitoring processes in conjunction with CIP-010-2, R1, which specifies the implementation of documented configuration change management processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R2 requires the implementation of documented configuration monitoring processes. A failure to implement these documented processes has medium impact on the reliability and operability of the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-010-2, R2			
	CIP-010-2, Requirement R2 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	Moderate	High	Severe
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)

VRF and VSL Justifications – CIP-010-2, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines — Severe: the performance measured does not substantively meet the intent of the Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-010-1 R2. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The VSL is binary.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R2 specifies that a Responsible Entity must implement and document the processes for configuration monitoring of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration monitoring process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-2, R4	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement plan(s) that are intended to prevent

VRF and VSL Justifications – CIP-010-2, R4	
	Transient Cyber Assets and Removable Media from introducing malicious code to BES Cyber Systems. The impact of a failure to implement documented plans can have a medium impact on the reliability and operability of the BES. If violated, the requirement poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented plans that are intended to prevent Transient Cyber Assets and Removable Media from introducing malicious code to BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-2, Requirement R4 incorporates the concepts from other CIP requirements to define requirements for Transient Cyber Assets and Removable Media. Similar to other requirements, CIP-010-2, Requirement R4 has a medium risk impact of a violation to implement documented plan(s) and, therefore, has a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-2, Requirement R4 requires the implementation of documented plans for Transient Cyber Assets and Removable Media. A failure to implement these documented plans has medium impact on the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-010-2, R4			
	CIP-010-2, Requirement R4 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	Moderate	High	Severe
The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-2, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4)	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-2, Requirement R4. (R4)

VRF and VSL Justifications – CIP-010-2, R4			
Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Section 1.2. (R4)	OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-2, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

VRF and VSL Justifications – CIP-010-2, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security plans but fails to address one or more of the required sections of the cyber security plans. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	CIP-010-2, Requirement R4 is a new requirement and raises the level of compliance from the previous version where certain Protected Cyber Assets did not have any requirements applied.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-2, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection is not expected to compromise computer network security. Failure to implement the Transient Cyber Asset and Removable Media plan can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail to actuate the vulnerability. There may be instances where the security vulnerability is so severe that failure to implement transient device protections can comprise computer network security, but these cases are the exception.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-2, Requirement R4 specifies that a Responsible Entity must implement and document the plan(s) for Transient Cyber Assets and Removable Media. Documentation of these plan(s) is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan(s) in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required sections of the cyber security plan(s). The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-011-2, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities prevent unauthorized access to BES Cyber System Information. Failure to adequately identify, protect, and control access to such information could result in unauthorized access and lost, stolen, or misused Cyber System Information. Such failure represents a risk to the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for methods to identify, provide secure handling, and control access to Cyber System Information. The VRF is only applied at the requirement level and the requirement parts are treated equally. The identification, secure handling and control of access have the common objective to protect BES Cyber System Information.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-003, R4 and CIP-003-3, R4.1, which have an approved VRF of Medium. The Requirement also maps to CIP-003-3, R4.2 and CIP-003-3, R4.3 and to CIP-003-3, R5, CIP-003-3, R5.1, CIP-003-3, R5.2, and CIP-003-3, R5.3, which have an approved VRF of Lower. The requirement has the object of securing Cyber System Information. Version 5 combines requirements to ensure consistency. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately identify and protect BES Cyber System Information could result in disclosure of information to unauthorized persons, lost, stolen, or misused Cyber System Information. Such breaches of confidentiality represent a risk to the reliability of Bulk Electric System from misuse by unauthorized persons.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-011-2, R1			
	The sub requirements in R1 have a common objective to assure confidentiality of BES Cyber System Information. The obligations to identify, control access, and assure proper handling of BES Cyber System Information contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

VRF and VSL Justifications – CIP-011-2, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This requirement maps to the previously-approved requirement CIP-011-1 R1. The proposed VSLs removed the "identify, assess, and correct" concept but retained the same level of compliance for the requirements. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-011-2, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the ‘weakest link’ characteristic, should apply binary VSLs	The VSLs are binary for this requirement.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for document and implement.