Project 2008-06 - Cyber Security - Order 706 - V5

These tables provide a working draft of the analysis and justification for each VRF and VSL for each requirement in the Version 5 CIP Cyber Security Standards:

VRF and VSL Justifications – CIP-002-5, R1	
Proposed VRF	**HIGH**
NERC VRF Discussion	A VRF of High is assigned to this Requirement. The requirement specifies the “bright-line” criteria used to categorize Bulk Electric System (BES) Cyber Systems, and the identification of High and Medium impact BES Cyber Systems. A VRF assignment of High is consistent with the higher risk impact of a violation of the identification and categorization of High and Medium impact BES Cyber Systems, as well as the failure to identify and appropriately re-categorize the affected BES Cyber Systems after a BES reconfiguration. The compromise of these Systems due to a cyber security incident could lead to significant impact, up to and including cascading disturbances. Failure to protect High and Medium impact Cyber Assets and their potential compromise may 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.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. The impact categorization of BES Cyber Systems is based on their impact on the reliable operation of the BES. The criteria are based on BES functional tasks that map to the areas cited in the Blackout Report.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The Requirement specifies the “bright-line” criteria used to categorize Bulk Electric System (BES) Systems and the identification of High and Medium impact BES Cyber Systems. The VRF is only applied at the requirement level and the requirement part is treated equally. A VRF assignment of High is consistent with the higher risk impact of a violation of the identification and categorization of High and Medium

VRF and VSL Justifications – CIP-002-5, R1	
	impact BES Cyber Systems, as well as the failure to identify and appropriately re-categorize the affected BES Cyber Systems after a BES reconfiguration. The compromise of these Systems due to a cyber security incident could lead to significant impact, up to and including cascading disturbances.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-002-3/4, R2, which has an approved VRF of High and the proposed VRF for CIP-002-5, R1 remains consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to protect High and Medium impact Cyber Assets and their potential compromise may 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. Therefore, this requirement was assigned a High VRF.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-002-5-2, Requirement R1 contains one main objective: The identification and categorization of High and Medium impact BES Cyber Systems for the application of specific protective cyber security requirements and the application of programmatic controls to Low impact BES Cyber Systems. Since the requirement focuses on the specific identification and categorization of such High and Medium impact Systems, an assignment of a High VRF is justified.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to

VRF and VSL Justifications – CIP-002-5, R1			
according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems	assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR	been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or	Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been

VRF and VSL Justifications – CIP-002-5, R1			
have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but	medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

VRF and VSL Justifications – CIP-002-5, R1			
	less than or equal to 10 high or medium BES Cyber Systems have not been identified.		

VRF and VSL Justifications – CIP-002-5, R1	
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. Some measurable reliability benefit can be achieved if the Responsible Entity has correctly categorized their BES Cyber Systems but fails to identify or correctly categorize one or more of them. 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 paradigm in CIP-002-5 has evolved from a binary model to a multidimensional model that includes identification and categorization. The VSLs provided reflect this paradigm and is fundamentally different from the binary model in CIP Versions 1 to 4. With this fundamental difference, the VSLs are not intended to lower the current reliability objective sought by this standard.
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	The proposed VSLs 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-002-5, R1	
Ambiguous Language	

VRF and VSL Justifications – CIP-002-5, 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	This requirement is an identification and categorization requirement and 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	Not applicable since this requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-002-5, R1	
implementation should account for their interdependence	

VRF and VSL Justifications – CIP-002-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. The requirement specifies an annual review and approval of the identification and categorization of BES Cyber Systems. The impact of a failure to review and approve the identification and categorization within the prescribed period has minimal impact on the reliability and operability of the BES. The requirement is a requirement that, if violated, would not be expected to directly or adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. The requirement has no bearing on the areas cited in the Blackout Report.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement has no subpart, and its assignment of a Lower VRF is consistent with the impact of a violation of this requirement. The impact of a failure to review and approve the identification and categorization within the prescribed period has minimal impact on the reliability and operability of the BES. The requirement is administrative in nature and is 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. A VRF assignment of Lower is, therefore, justified.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps to CIP-002-4 R3, which has an assigned VRF of Lower and the proposed VRF for CIP-002-5, R2, remains consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-002-5, Requirement R2 requires an annual review and approval. The requirement is a requirement

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-002-5, R2</th></tr>
<tr><td></td><td colspan="3">that, if violated, would not be expected to directly adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. Therefore, this requirement was assigned a Lower 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.
CIP-002-5, Requirement R2 addresses a single objective and has a single VRF.</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 did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1)
OR
The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months</td><td>The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1)
OR
The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months</td><td>The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1)
OR
The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the</td><td>The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1)
OR
The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)</td></tr>
</table>

VRF and VSL Justifications – CIP-002-5, R2			
of the previous approval. (R2.2)	of the previous approval. (R2.2)	previous approval. (R2.2)	

VRF and VSL Justifications – CIP-002-5, R2	
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. Some measurable reliability benefit can be achieved if the Responsible Entity has appropriately reviewed and updated their identification of BES Cyber Systems but failed to complete the review and update within the specified timeframes. 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 proposed requirement is mapped to requirement R3 of CIP-002-3. The VSLs for the previous releases were based on lists of Critical Assets and Critical Cyber Assets, with separate requirements for review and approval. This version requires identification and categorization of BES Cyber Systems within a prescribed period. 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	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.

VRF and VSL Justifications – CIP-002-5, R2	
Ambiguous Language	

VRF and VSL Justifications – CIP-002-5, 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	This requirement is a periodic review and approval requirement and does not specify protective requirements.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and	Not applicable since this requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-002-5, R2	
implementation should account for their interdependence	

VRF and VSL Justifications – CIP-003-5, 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. This requirement maps from CIP-003-3, R1, which has an approved VRF of Medium; therefore, the proposed VRF remains consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security policy is unlikely, under Emergency, abnormal, or

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-003-5, R1</th></tr>
<tr><td></td><td colspan="3">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)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by</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)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by</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)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete</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)
OR
The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1)</td></tr>
</table>

VRF and VSL Justifications – CIP-003-5, R1			
R1 within 15 calendar months but did complete this review in less than or equal to 16 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 or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	R1 within 16 calendar months but did complete this review in less than or equal to 17 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 or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	this review in less than or equal to 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 or delegate according to Requirement R1 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 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 or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

VRF and VSL Justifications – CIP-003-5, 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-003-3 R1 and CIP-003-3 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.
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	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.

VRF and VSL Justifications – CIP-003-5, R1	
Ambiguous Language	
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	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	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,

VRF and VSL Justifications – CIP-003-5, R1	
documentation and implementation should account for their interdependence	therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower 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. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. However, given the scoping of the this requirement to only those BES assets that contain low impact BES Cyber Systems, a VRF of Lower 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 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-003-3, 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 policy 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.

VRF and VSL Justifications – CIP-003-5, R2			
FERC VRF G5 Discussion	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.		
Proposed VSLs			
Lower	Moderate	High	Severe
The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber

VRF and VSL Justifications – CIP-003-5, R2			
deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 18 calendar months of the previous approval. (R2)

VRF and VSL Justifications – CIP-003-5, R2			
months of the previous approval. (R2)	approval. (R2)		

VRF and VSL Justifications – CIP-003-5, 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 back to previously approved requirements CIP-003-3 R1 and CIP-003-3 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.
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	The Proposed VSLs are not binary and does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-003-5, R2	
Ambiguous Language	
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	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 or more 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	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,

VRF and VSL Justifications – CIP-003-5, R2	
documentation and implementation should account for their interdependence	accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-5, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The identification of a single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization. Cyber security is not simply a technical endeavor. Failure to provide clear governance and organizational leadership 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 specifies that a CIP Senior Manager be identified. The VRF is only applied at the requirement level and the requirement parts are treated equally. As there are no requirement parts, the VRF is, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-3, R2, 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. Because the purpose of the Requirement is for entities to properly identify and document the CIP Senior Manager in order to ensure there is clear authority and ownership of the CIP program within an organization, this Requirement is appropriately assigned a Medium VRF.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement does not co-mingle more than one obligation. The only obligation included in requirement CIP-003-5 R1 is the identification of the CIP Senior Manager. Therefore, the requirement has a single VRF.

VRF and VSL Justifications – CIP-003-5, R3			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

VRF and VSL Justifications – CIP-003-5, 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 identified its CIP Senior Manager but failed to document changes within the specified timeframes. 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 proposed Requirement, CIP-003-5 R3, maps to a previously approved requirement, CIP-003-3 R2. The proposed VSLs do not have the unintended consequence of lowering the current 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	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.

VRF and VSL Justifications – CIP-003-5, R3	
Ambiguous Language	
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	There is an incremental aspect to a violation of this Requirement in that some measurable reliability benefit can be achieved if the Responsible Entity identified its CIP Senior Manager but failed to document changes within the specified timeframes.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	Not applicable since the requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-003-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-003-5, 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-003-3, R 2.2 and R2.3, 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,

VRF and VSL Justifications – CIP-003-5, R4			
	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.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by title or name of the delegate) as required.

VRF and VSL Justifications – CIP-003-5, 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 back to a previously approved VSL in CIP-003-3 R2.2 and R2.3. The previously approved VSL was a binary Severe VSL. The SDT has determined that there are numerous delegations that take place, and there is a reliability benefit if the majority of those delegations are documented in compliance with the standard; and, as such, has assigned gradated VSLs to the requirement.
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,

VRF and VSL Justifications – CIP-003-5, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	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	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-004-5, R1	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have awareness of sound security practices. 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 ongoing security awareness reinforcement. The VRF is only applied at the Requirement level and the requirement parts are treated equally. The single Requirement Part constitutes the required security awareness program.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-3, R1, 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 convey security awareness practices within a calendar quarter 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 individuals with access to BES Cyber Systems have awareness of sound security practices and, therefore, does not co-mingle more than one obligation.

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-004-5, R1</th></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 did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)</td><td>The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)</td><td>The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)</td><td>The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1)
OR
The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)</td></tr>
</table>

VRF and VSL Justifications – CIP-004-5, 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. The SDT has determined that there is a reliability benefit to partial compliance with this requirement and has therefore assigned gradated VSLs.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R1, which did not graduate VSLs according to the time beyond meeting a compliance obligation and accumulated violations as a single violation. This version corrects the oversight by gradating the violation based on the number of days past the performance requirement. Failure to meet the requirement by a given number of days appropriately maps to the severity of the violation.
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,

VRF and VSL Justifications – CIP-004-5, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	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	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	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-004-5, 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-004-3, R2.2, which has an approved VRF of Medium. In this version, the training program requirements are distinct from the implementation, and the implementation in R3 has the previously approved VRF of Medium.
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.

VRF and VSL Justifications – CIP-004-5, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (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, and did not identify, assess and correct	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (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, and did not identify, assess and correct the deficiencies. (2.2) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (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, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with	The Responsible Entity did not implement a cyber security training program appropriate to 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, and did not identify, assess and correct the deficiencies. (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

VRF and VSL Justifications – CIP-004-5, R2			
the deficiencies. (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, and did not identify, assess and correct the deficiencies. (2.3)	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, and did not identify, assess and correct the deficiencies. (2.3)	authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

VRF and VSL Justifications – CIP-004-5, 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 CIP-004-3 R2.2, which did not graduate VSLs and treats all violations equally. This version corrects the oversight by gradating the violation based on the number of training elements missing in the program. Failure to meet the parts of the requirement appropriately maps to the severity of the violation.
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	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.

VRF and VSL Justifications – CIP-004-5, R2	
Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
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	A single failure of this requirement does not compromise network computer security.

VRF and VSL Justifications – CIP-004-5, R2	
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-004-5, 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.
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.

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-004-5, R3</th></tr>
<tr><td></td><td colspan="3">This requirement maps from CIP-004-3, R2, which has an approved VRF of Medium.</td></tr>
<tr><td>FERC VRF G4 Discussion</td><td colspan="3">Guideline 4- Consistency with NERC Definitions of VRFs.
Failure to implement a security training program could effect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.</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 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.</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 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 one individual, and did not identify, assess, and correct the deficiencies. (R3)
OR</td><td>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 two individuals, and did not identify, assess, and correct the deficiencies. (R3)
OR</td><td>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, and did not identify, assess, and correct the deficiencies. (R3)
OR
The Responsible Entity did conduct Personnel Risk Assessments (PRAs)</td><td>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 authorized cyber or authorized unescorted physical access. (R3)
OR
The Responsible Entity has a program for conducting Personnel</td></tr>
</table>

VRF and VSL Justifications – CIP-004-5, 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 confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and correct	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, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	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, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR

VRF and VSL Justifications – CIP-004-5, R3			
the deficiencies. (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 one individual, and did not identify, assess, and correct the deficiencies. (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	correct the deficiencies. (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 two individuals, and did not identify, assess, and correct the deficiencies. (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	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 three individuals, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and correct the deficiencies. (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, and did not

VRF and VSL Justifications – CIP-004-5, R3			
previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)		identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

VRF and VSL Justifications – CIP-004-5, 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 CIP-004-3 R2.2, which did not gradate VSLs and treats all violations equally. This version more appropriately gradates the violation based on the number of individuals with access to BES Cyber Systems who did not receive training. Failure for a given number of individuals to receive training appropriately maps to the severity of the violation.
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	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.

VRF and VSL Justifications – CIP-004-5, R3	
Ambiguous Language	
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. 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	This Requirement pertains to implementing the cyber security program and does not require procedural documentation.

VRF and VSL Justifications – CIP-004-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-004-5, 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	The Responsible Entity did not	The Responsible Entity did not	The Responsible Entity did not

VRF and VSL Justifications – CIP-004-5, R4			
verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (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 one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3)	verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (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 two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the	verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (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 three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR	implement any documented program(s) for access management. (R4) 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, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and correct the deficiencies. (4.2)

VRF and VSL Justifications – CIP-004-5, R4			
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 one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	deficiencies. (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 two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	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 three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	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 four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (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 four or more BES Cyber System Information

VRF and VSL Justifications – CIP-004-5, R4			
			storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)

VRF and VSL Justifications – CIP-004-5, 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 CIP-004-3 R3, which gradates the VSLs based on implementation of the Requirement. This does not lower the current level of compliance because new components of the program have been added.
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	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.

VRF and VSL Justifications – CIP-004-5, R4	
Ambiguous Language	
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	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	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-004-5, R4	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-004-5, 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-004-3 R4.2, which has an approved VRF of Lower, and CIP-007-3 R5.2.3., which has an approved VRF of Medium. The Requirement only addresses the securing of shared accounts for termination in CIP-007-3 R5.2.3, and not the audit trail. Because the securing of shared accounts upon termination is consistent with CIP-004-3 R4.2, then we can imply a VRF of lower for that component of the Requirement. 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

VRF and VSL Justifications – CIP-004-5, R5			
	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.		
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, and did not identify, assess, and correct the deficiencies. (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	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, and did not identify, assess, and correct the deficiencies. (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,	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, and did not identify, assess, and correct the deficiencies. (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	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, and did not identify, assess, and correct the deficiencies. (5.1)

VRF and VSL Justifications – CIP-004-5, R5			
do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR 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, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more	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 day following the predetermined date, and did not identify, assess, and correct the deficiencies. (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, and did not identify, assess, and correct the deficiencies. (5.3)	authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (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 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, and did not identify, assess, and correct the deficiencies. (5.3)	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 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, and did not identify, assess, and correct the deficiencies. (5.2)

VRF and VSL Justifications – CIP-004-5, R5			
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, and did not identify, assess, and correct the deficiencies. (5.5)			

VRF and VSL Justifications – CIP-004-5, 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 VSL gradates the severity based on whether the violation includes a scenario whether the individual no longer needed access, when an individual was terminated for cause, or when both occurred. The requirement no longer differentiates on scenarios of termination for cause.
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	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.

VRF and VSL Justifications – CIP-004-5, R5	
Ambiguous Language	
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 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	This requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-004-5, R5	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-005-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requirement ensures that all BES Cyber Systems are within an Electronic Security Perimeter and that all electronic routable communication and dialup communication across the perimeter is secured. Failure to properly secure the external communications to the BES Cyber Systems and the networks on which they reside could result in unauthorized access, which could directly affect the ability to 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. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Both Requirements in CIP-005 are of the same VRF as both insure the proper electronic security perimeter based controls are in place for preventing unauthorized access.
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 implement documented processes and adequate safeguards to prevent unauthorized access to an entity's networks could result in unauthorized access and potential disruption of monitoring and logical control of BES Cyber Assets. Consistent with the definition of a Medium VRF, unauthorized logical access could directly affect the electrical state or the capability of the Bulk Electric System and the ability to monitor and control the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common set of objectives to ensure access to BES Cyber Systems is authorized and protected. The obligations within the requirement collectively address the objective and only one VRF is assigned.

VRF and VSL Justifications – CIP-005-5, R1			
Proposed VSLs			
Lower	Moderate	High	Severe
N/A	N/A	The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for CIP-005-5 Table R1 – Electronic Security Perimeter. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

VRF and VSL Justifications – CIP-005-5, R1			
			OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)

VRF and VSL Justifications – CIP-005-5, 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 VSL's are in line with the currently approved VSL's in CIP-005-3a and therefore do not lower the current compliance level.
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	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.

VRF and VSL Justifications – CIP-005-5, R1	
Ambiguous Language	
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	With the exception of the portion of the VSLs dealing with the method aspect of the Requirement, the proposed VSL is binary and assigns a "Severe" category for the violation of the 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	A single violation of this requirement particularly at the Severe VSL category could result in an individual obtaining unauthorized access to BES Cyber Systems. Since the Electronic Security Perimeter is one of the first level of defenses around a network (or dialup modem) containing BES Cyber Systems, any lack of implemented requirements is a binary VSL. The gradation in the VSL is for lacking documentation only. The existence of a particular 'state' regarding documented and implemented processes does not alone constitute the likelihood of exploitation. Several factors centered on intent, motivation, and capabilities and lack of other mitigating controls would necessarily also determine System vulnerability as well as the impact rating of the BES Cyber System in question.
FERC VSL G6 VSLs for cyber security requirements containing	Due to the increased scope of Version 5 and the corresponding increase in the number of declared Electronic Security Perimeters and therefore the order of magnitude more ports and services that will be in scope among other things, the VSL for documentation purposes only has been gradated. Any lapse in the implementation of the actual security controls remains binary.

VRF and VSL Justifications – CIP-005-5, R1	
interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-005-5, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requirement ensures that interactive remote access to BES Cyber Systems includes documented processes and safeguards to prevent unauthorized access to an entity's networks. Failure to use intermediate devices and establish robust authentication and encryption techniques could result in unauthorized access, which could directly affect the ability to 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 specific intermediate devices to work in conjunction with authentication and encryption procedures for access to BES Cyber Systems. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Use of intermediate devices with proper authentication and encryption procedures for access share a common objective of preventing unauthorized access.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement documented processes and adequate safeguards to prevent unauthorized access to an entity's networks could result in unauthorized access and potential disruption of monitoring and logical control of BES Cyber Assets. Consistent with the definition of a Medium VRF, unauthorized logical access could directly affect the electrical state or the capability of the Bulk Electric System and the ability to monitor and control the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common set of objectives to ensure interactive remote access to BES Cyber Systems is authorized and protected. The obligations to place an inclusive subset of protective measures

VRF and VSL Justifications – CIP-005-5, R2			
	in place to authorize interactive remote access contribute collectively to the objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

VRF and VSL Justifications – CIP-005-5, 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	This is a new requirement, so this section is not applicable.
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	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.

VRF and VSL Justifications – CIP-005-5, R2	
Ambiguous Language	
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	A single violation of this requirement at the low, moderate, or high VSL category would not necessarily result in an individual obtaining unauthorized interactive remote access to BES Cyber Systems. The existence of a particular 'state' regarding documented and implemented processes does not alone constitute the likelihood of exploitation. Several factors centered on intent, motivation, and capabilities and lack of other mitigating controls would necessarily also determine system vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	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,

VRF and VSL Justifications – CIP-005-5, R2	
documentation and implementation should account for their interdependence	therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-006-5, 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-006-3, R1, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-5, R1 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-006-5, 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

VRF and VSL Justifications – CIP-006-5, R1			
	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, 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. 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.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not

VRF and VSL Justifications – CIP-006-5, R1			
The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for	assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (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) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or

VRF and VSL Justifications – CIP-006-5, R1			
		unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) 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 documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified

VRF and VSL Justifications – CIP-006-5, R1			
			deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (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 has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and

VRF and VSL Justifications – CIP-006-5, R1			
			identified deficiencies, but did not assess or correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (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-006-5, 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

VRF and VSL Justifications – CIP-006-5, R1			
			access logs for 90 calendar days. (1.9)

VRF and VSL Justifications – CIP-006-5, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are in line with the currently approved VSLs in previous versions and therefore do not lower the current compliance level.
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.

VRF and VSL Justifications – CIP-006-5, 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 Requirement Parts for restricting access have a binary Severe VSL. Other Requirement Parts associated with the physical security plan do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security	Failure to document processes carries a Severe VSL.

VRF and VSL Justifications – CIP-006-5, R1	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-006-5, 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-006-3, R1.6, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-5, R2 is consistent.
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.

VRF and VSL Justifications – CIP-006-5, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included 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 and but did not identify, assess, or correct the deficiencies. (2.2) OR	The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	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 The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

VRF and VSL Justifications – CIP-006-5, R2			
	The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		

VRF and VSL Justifications – CIP-006-5, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSL's are in line with the currently approved VSL's in CIP-006-3 and therefore do not lower the current compliance level.
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.

VRF and VSL Justifications – CIP-006-5, 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	A single violation of this Requirement at the low, moderate, or high VSL category would not necessarily compromise computer network security. The Requirement to further restrict access to only authorized individuals would compensate this control.
FERC VSL G6 VSLs for cyber security	Failure to document processes carries a Severe VSL and therefore recognizes the linkage between documentation and implementation.

VRF and VSL Justifications – CIP-006-5, R2	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-006-5, R3	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. This Requirement calls for one or more documented Physical Access Control System maintenance and testing programs. Failure to implement Physical Access Control System maintenance and testing would not be expected to directly or adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
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 Access Control System maintenance and testing 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's VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement Physical Access Control System maintenance and testing programs 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.

VRF and VSL Justifications – CIP-006-5, R3			
	The proposed Requirement has a single objective of ensuring that Responsible Entities implement one or more Physical Access Control System maintenance and testing programs and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

VRF and VSL Justifications – CIP-006-5, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are in line with the currently approved VSLs in CIP-006-3 and therefore do not lower the current compliance level.
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.

VRF and VSL Justifications – CIP-006-5, R3	
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	Performing the maintenance activity obligations provides additional assurance in the physical security controls in place, but failure to do so would not necessarily compromise computer network security given other protections. Other Requirement Parts associated with physical security controls do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security	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-006-5, R3	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, 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-007-3, 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 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.
FERC VRF G5 Discussion	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.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented and documented	The Responsible Entity has implemented and documented	The Responsible Entity did not implement or document one or

VRF and VSL Justifications – CIP-007-5, R1			
	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 and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR 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 but did not identify, assess, or correct the deficiencies. (1.2)	processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR 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 but did not identify, assess, or correct the deficiencies. (1.1)	more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

VRF and VSL Justifications – CIP-007-5, 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 CIP-004-3 R2.2, which did not gradate VSLs and treats all violations equally. This version provides more appropriate gradation of the VSLs while still providing a Severe VSL for all types of egregious failures.
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	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.

VRF and VSL Justifications – CIP-007-5, R1	
Ambiguous Language	
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	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	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-007-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, 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-007-3, R3, which has an approved VRF of Lower. This version more appropriately assigns a VRF as Medium given other changes in the Requirement. Failure for a given number of individuals to receive training appropriately maps to the severity of the violation.
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.

VRF and VSL Justifications – CIP-007-5, R2			
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 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 and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR 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 evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR 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 evaluating cyber security patches for applicable Cyber	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 and has identified deficiencies but did not assess or correct the deficiencies. (2.1) 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 but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR 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

VRF and VSL Justifications – CIP-007-5, 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 but did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the deficiencies. (2.3)	Assets but did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released	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 and has identified deficiencies but did not assess or correct the deficiencies. (2.2) 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 days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR 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 but did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the

VRF and VSL Justifications – CIP-007-5, R2			
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 but did not identify, assess, or correct the deficiencies. (2.3)	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 but did not identify, assess, or correct the deficiencies. (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 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did	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 and has identified deficiencies but did not assess or correct the deficiencies. (2.3) 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	deficiencies. (2.4) 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 but did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity

VRF and VSL Justifications – CIP-007-5, R2			
	not assess or correct the deficiencies. (2.3) 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 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	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 but did not identify, assess, or correct the deficiencies. (2.4)

VRF and VSL Justifications – CIP-007-5, 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	This Requirement maps to a previously approved VSL for CIP-007-3 R3. The proposed version more appropriately gradates the violation, which is scaled to the risk created by the severity of violation.
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	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.

VRF and VSL Justifications – CIP-007-5, R2	
Ambiguous Language	
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	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	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-007-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, 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-007-3, 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 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**
	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table*

VRF and VSL Justifications – CIP-007-5, R3			
	are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR 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 and did not identify, assess, or correct the deficiencies. (3.3)	not mitigate the threat of detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR 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 and did not identify, assess, or correct the deficiencies. (3.2) OR 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 and has identified deficiencies but did not assess or correct the deficiencies. (3.3)	*R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR 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 and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity has implemented one or more

VRF and VSL Justifications – CIP-007-5, R3			
		OR 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 and did not identify, assess, or correct the deficiencies. (3.3)	documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)

VRF and VSL Justifications – CIP-007-5, 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 a previously approved VSL for CIP-007-3 R4. The proposed version includes a time-based gradation for applying malicious code protection updates which violation intended to match to the degree of severity the violation would pose to the BES.
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	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.

VRF and VSL Justifications – CIP-007-5, R3	
Level Assignments that Contain Ambiguous Language	
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	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	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-007-5, R3	
interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, 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-007-3, R6, 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.

VRF and VSL Justifications – CIP-007-5, R4			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
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 an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined	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 an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined	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) 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 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR 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) for the Applicable Systems (per device or	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (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

VRF and VSL Justifications – CIP-007-5, R4			
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 but did not identify, assess, or correct the deficiencies. (4.4)	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 but did not identify, assess, or correct the deficiencies. (4.4)	system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1	the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) 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 and did not identify, assess, or correct the deficiencies. (4.1)

VRF and VSL Justifications – CIP-007-5, R4			
		(where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify	

VRF and VSL Justifications – CIP-007-5, R4			
		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 and did not identify, assess, or correct the deficiencies. (4.4)	

VRF and VSL Justifications – CIP-007-5, 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 a previously approved VSL for CIP-007-3 R5. The proposed version also includes the new requirement to manually review logs.
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	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.

VRF and VSL Justifications – CIP-007-5, R4	
Ambiguous Language	
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 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	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-007-5, R4	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, 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-007-4 R5, which has an approved VRFs of Lower and 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.

VRF and VSL Justifications – CIP-007-5, R5			
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 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 and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has	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 and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has	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) and has identified deficiencies but did not assess or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has

VRF and VSL Justifications – CIP-007-5, R5			
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 and did not identify, assess, or correct the deficiencies. (5.6)	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 and did not identify, assess, or correct the deficiencies. (5.6)	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) and did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did	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 and has identified deficiencies but did not assess or correct the deficiencies. (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 authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did

VRF and VSL Justifications – CIP-007-5, R5			
		not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3) 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 and has identified deficiencies but did not assess or correct the deficiencies. (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	not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4) 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 but did not identify, assess, or correct the deficiencies. (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 and

VRF and VSL Justifications – CIP-007-5, R5			
		one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (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 and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for	has identified deficiencies but did not assess or correct the deficiencies. (5.5) 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 and did not identify, assess, or correct the deficiencies. (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 18 calendar months of the last

VRF and VSL Justifications – CIP-007-5, R5			
		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 and did not identify, assess, or correct the deficiencies. (5.6)	password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) 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 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (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

VRF and VSL Justifications – CIP-007-5, R5			
			generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) 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 and did not identify, assess, or correct the deficiencies. (5.7)

VRF and VSL Justifications – CIP-007-5, 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 previous binary VSL for this Requirement has not proven accurate after several iterations of its application. Account access management and procedures for monitoring and controlling access are complex with an often intensive scope. Errors resulting in potential or single instances of unauthorized access do not have the same criticality as multiple instances and blatant lack of controls.
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	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.

VRF and VSL Justifications – CIP-007-5, R5	
Ambiguous Language	
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. 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	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-007-5, R5	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R1	
Proposed VRF	**LOWER**
NERC VRF Discussion	This requires each Responsible Entity to have a plan to respond to Cyber Security Incidents. Failure to have an incident response plan could delay recovery actions and hinder entities in understanding and reporting the incident. The planning component of the Requirement is administrative in nature and, if violated, would not be expected to affect 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 procedures to respond to Cyber Security Incidents. The VRF is only applied at the requirement level and the Requirement Parts are treated equally. Each requirement part is a necessary component of an incident response plan.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1, which has an approved VRF of Lower.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have an incident response plan could delay recovery actions and hinder entities in understanding and reporting the incident. The planning component of the Requirement is administrative in nature and, if violated, would not be expected to affect the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common objective of having a plan for responding to, handling, and reporting Cyber Security Incidents. These contribute to the overall objective to minimize the loss and destruction of Cyber Security Incidents and providing timely information about the incident.

VRF and VSL Justifications – CIP-008-5, R1			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-008-5, R1</th></tr>
<tr><td></td><td></td><td></td><td>Incident. (1.2)</td></tr>
</table>

VRF and VSL Justifications – CIP-008-5, 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 from CIP-008-3 R1 and has similar VSL assignments. The previously approved VSL differentiated between High and Severe on the basis of whether the entity had maintained the plan. The change made to this version differentiates based on specific components of the plan, which provides more objectivity.
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	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.

VRF and VSL Justifications – CIP-008-5, R1	
Ambiguous Language	
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	A single violation of this Requirement indicates an entity does not have a documented and consistent response to a Cyber Security Incident, but a single lapse in protection would not be expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	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-008-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	This Requirement ensures entities implement their incident response plan(s). Failure to implement the incident response plan 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. Each Requirement row contributes to the common objective of implementing the incident response plan. The Requirement to retain incident documentation ensures the entity can review actual incidents at a later date.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1.6 and R2, which has an approved VRF of Lower.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement the incident response plan 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 Requirements in R2 have a common objective of implementing incident response plans. Requirement Row 2.1 specifies the obligation to implement the plan during an incident, and Requirement Row 2.2 specifies the obligation to periodically exercise the plan. Requirement Row 2.3 specifies the obligation to retain incident documentation to ensure the entity can review actual incidents at a later date.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not	The Responsible Entity has not	The Responsible Entity has not	The Responsible Entity has not

VRF and VSL Justifications – CIP-008-5, R2			
tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

VRF and VSL Justifications – CIP-008-5, 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 proposed version more appropriately gradates the violation, which is scaled to the risk created by the severity of violation.
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	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.

VRF and VSL Justifications – CIP-008-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	This requirement maps from CIP-008-3 R1 and has similar VSL assignments. The previously approved VSL was binary. The change made to this version differentiates based on the number of days late in a time-based performance. This reflects the lesser degree of risk posed to BES reliability for exceeding timed requirements. New requirements have also been incorporated into the VSL.
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 of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	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-008-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R3	
Proposed VRF	**LOWER**
NERC VRF Discussion	This Requirement ensures incident response plans remain up-to-date and that individuals with responsibilities in the plans have the most current version.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of keeping response plans up-to-date and communicating changes to individuals with responsibilities in the plans. The obligations to keep the response plans up-to-date include changes in response to lessons learned in an incident or organizational and technology changes.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1.4 and R1.5, which has an approved VRF of Lower.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to update and communicate changes to the incident response plan(s) are administrative requirements and are 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 requirements in R2 have a common objective of keeping response plans up-to-date and communicating changes to individuals with responsibilities in the plans.

Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not notified each person or group with a defined role in the Cyber	The Responsible Entity has not updated the Cyber Security	The Responsible Entity has neither documented lessons learned nor	The Responsible Entity has neither documented lessons learned nor

VRF and VSL Justifications – CIP-008-5, R3			
Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60	documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the	documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

VRF and VSL Justifications – CIP-008-5, R3			
	and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

VRF and VSL Justifications – CIP-008-5, 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 proposed Requirement has more specificity about reviewing and updating the plan than prior versions of the standard, and the failure to update the plan in a timely manner has less of an impact than not performing the review at all.
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	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.

VRF and VSL Justifications – CIP-008-5, R3	
Ambiguous Language	
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	A single violation of this Requirement should not compromise the security of the BES Cyber System because this is in response to an incident which has already occurred,
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	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-008-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R1

Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requires each Responsible Entity have a plan to recover to BES Cyber Systems. Failure to have a recovery plan could increase the downtime and destruction in a hazardous situation, which could affect the ability to effectively monitor, control, or restore the Bulk Electric System in an Emergency situation.
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 recover BES Cyber Systems. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Each Requirement Part is a necessary component of a recovery plan.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-009-3 R1, which has an approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a recovery plan could increase the downtime and destruction in a hazardous situation, which could affect the ability to effectively monitor, control, or restore the Bulk Electric System in an Emergency situation.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common objective of having a plan for recovering BES Cyber Systems. These contribute to the overall objective to minimize downtime and destruction in a hazardous situation. T he requirement to preserve data during recovery provides information for post-event analysis, but this requirement best fits here because it involves the actions taken during recovery.

VRF and VSL Justifications – CIP-009-5, R1			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

VRF and VSL Justifications – CIP-009-5, 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 from CIP-009-3 R1, and has similar VSL assignments. The previously approved VSL did not have a differentiation between having a plan and missing some elements of the plan, but the severity of not having a plan is higher than missing a single element in a plan.
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	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.

VRF and VSL Justifications – CIP-009-5, R1	
Ambiguous Language	
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	A single violation of this Requirement indicates an entity has not created recovery plan(s) for BES Cyber Systems, but a single lapse in protection would not be expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This requirement only specifies documentation, and not implementation.

VRF and VSL Justifications – CIP-009-5, R1	
documentation and implementation should account for their interdependence	

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-009-5, R2</th></tr>
<tr><th>Proposed VRF</th><th colspan="3">LOWER</th></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-009-3 R2, R4, and R5, 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</td><td>The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not</td><td>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17</td><td>The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18</td></tr>
</table>

VRF and VSL Justifications – CIP-009-5, R2			
15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (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, and when tested, any deficiencies were identified, assessed, and corrected. (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	exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (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, and when tested, any deficiencies were identified, assessed, and corrected. (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, and when	calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (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 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (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, and when tested, any deficiencies were identified, assessed, and	calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (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 18 calendar months between tests. (2.2) OR

VRF and VSL Justifications – CIP-009-5, R2			
between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	tested, any deficiencies were identified, assessed, and corrected. (2.3)	corrected. (2.3)	The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (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) OR

VRF and VSL Justifications – CIP-009-5, R2			
			The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)

VRF and VSL Justifications – CIP-009-5, 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 CIP-009-3 R2 and R3 and adds the obligation to perform a full operational exercise. The portions of the Requirement from CIP-009-3 carry forward similar VSLs, and the failure to perform a full operational exercise is proposed as a High VSL because it does not carry the same potential consequence of not having exercised the recovery plan. In addition, the proposed VSLs gradate failure to perform a test of the recovery plan based on the amount of time lapse between tests. This more appropriately reflects the severity of the corresponding type of violation.
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	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.

VRF and VSL Justifications – CIP-009-5, R2	
Ambiguous Language	
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	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	This Requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-009-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R3			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement ensures BES Cyber System plans remain up-to-date and effective and that individuals with responsibilities in the plans have the most current version.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of keeping recovery plans up-to-date and effective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. The assignment of a Lower VRF is consistent of the impact of a violation of this Requirement and is therefore consistent among Reliability Standards.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to review, update or communicate changes to the recovery plan is administrative in nature 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 Requirements in R2 have a common objective of keeping response plans up-to-date and effective.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or

VRF and VSL Justifications – CIP-009-5, R3			
	actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or Technology changes.	actual recovery. (3.1.1)

VRF and VSL Justifications – CIP-009-5, 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 proposed Requirement has more specificity about reviewing and updating the plan than prior versions of the standard, and the failure to update the plan in a timely manner has less of an impact than not performing the review at all.
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	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-009-5, R3	
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 are 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 should not compromise the security of the BES Cyber System because this is in response to an incident which has already occurred.
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-010-1, 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-010-1, R1 specifies the implementation of documented configuration change management processes in conjunction with CIP-010-1, 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-010-1, 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-010-1, 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-010-1, 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) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR	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) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (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) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (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

VRF and VSL Justifications – CIP-010-1, R1			
The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification	OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) 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 and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a	OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did	The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)

VRF and VSL Justifications – CIP-010-1, R1			
documentation. (1.4.3)	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 not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that	OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that 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

VRF and VSL Justifications – CIP-010-1, R1			
		required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a	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 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

VRF and VSL Justifications – CIP-010-1, R1			
		change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the deficiencies. (1.5.2) OR	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-010-1, R1			
		The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	

VRF and VSL Justifications – CIP-010-1, 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 proposed Requirement is new and has no mapping to a Requirement in a previous NERC CIP Standards Version. It does not have the unintended consequence of lowering the current 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	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-010-1, R1	
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-010-1, 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-010-1, 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-010-1, R2 specifies the implementation of documented configuration monitoring processes in conjunction with CIP-010-1, 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-010-1, 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-010-1, R2			
	CIP-010-1, 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) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to

VRF and VSL Justifications – CIP-010-1, R2			
			the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)

VRF and VSL Justifications – CIP-010-1, 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	The proposed Requirement is new and has no mapping to a Requirement in a previous NERC CIP Standards Version. It does not have the unintended consequence of lowering the current 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-010-1, 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-010-1, 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-010-1, R3	
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 vulnerability assessment processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls of BES Cyber Assets and BES Cyber Systems. Failure to implement vulnerability assessment processes may impact the reliability and operability of the BES. The requirement is a requirement that, 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 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 vulnerability assessment processes. 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 act as a component in an overall program to periodically ensure the proper implementation of security controls of BES Cyber Assets and BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. Requirement Part 3.1 maps from CIP-005-4, R4 (which has an assigned VRF of Medium) and CIP-007-4, R8 (which has an assigned VRF of Lower), Requirement Part 3.2 is a new requirement, while Requirement Part 3.3 maps from CIP-005-4, R4.5 (which has an assigned VRF of Medium) and CIP-007-4, R8.4 (which has an assigned VRF of Medium). Most of the aforementioned requirements had an approved VRF of Medium and, therefore, the proposed VRF for CIP-010-1, R3 is consistent. While the drafting team recognizes that CIP-007-4, R8 was assigned a VRF of Lower, to maintain consistency among reliability

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-010-1, R3</th></tr>
<tr><td></td><td colspan="3">standards, an assigned VRF of Medium is appropriate.</td></tr>
<tr><td>FERC VRF G4 Discussion</td><td colspan="3">Guideline 4- Consistency with NERC Definitions of VRFs.
CIP-010-1, Requirement R3 requires the implementation of documented vulnerability assessment processes. A failure to implement these documented processes may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, 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.
CIP-010-1, Requirement R3 addresses a single objective and has a single VRF.</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 implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1)
OR
The Responsible Entity has implemented one or more documented active vulnerability assessment processes for</td><td>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1)
OR
The Responsible Entity has implemented one or more</td><td>The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1)
OR
The Responsible Entity has implemented one or more documented active vulnerability</td><td>The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3)
OR
The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber</td></tr>
</table>

VRF and VSL Justifications – CIP-010-1, R3

Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has

VRF and VSL Justifications – CIP-010-1, R3			
			implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

VRF and VSL Justifications – CIP-010-1, 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.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed requirement is mapped to Requirement R4 and R4.5 of CIP-005-4 and Requirement R8 and R8.4 of CIP-007-4. Additionally, Requirement Part 3.2 is a new requirement and has no mapping to a Requirement in a previous NERC CIP Standards Version. The binary VSL for the previous releases were based on performing vulnerability assessments annually, or not including one or more of the various elements identified in the related sub-requirements in a vulnerability assessment. This version's VSLs have evolved from this binary component model to a multidimensional component model. The proposed requirement does not have the unintended consequence of lowering the current 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 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-010-1, R3	
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	This Requirement seeks to implement vulnerability assessment processes that if not done may impact the reliability and operability of the BES, but 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-010-1, Requirement R3 specifies that a Responsible Entity must implement and document the processes for vulnerability assessments 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 vulnerability assessment 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-011-5, 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. 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

VRF and VSL Justifications – CIP-011-5, R1			
	Information contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	Moderate	High	Severe
N/A	N/A	The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

VRF and VSL Justifications – CIP-011-5, R1			
		procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	

VRF and VSL Justifications – CIP-011-5, 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 previously approved VSLs included a combination of binary and gradated VSLs. The Proposed VSLs are consistent with the approved VSLs for the CIP 011-5 R1 requirement, which maps to CIP 004-3, R4 and CIP 004-3, R5.
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	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-011-5, R1	
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 and implement a BES Cyber System information protection program has a binary Severe VSL. Other Requirement Parts associated with the information protection program 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	Interdependent tasks of documentation, identification, and implementation are treated in a uniform manner and have not been separated for each topical area addressed in the requirement.

VRF and VSL Justifications – CIP-011-1, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. This requirement ensures that Responsible Entities take action to prevent unauthorized retrieval of BES Cyber System information prior to disposal or reuse of asset storage media. A violation would not be expected to affect the electrical state or capability of the Bulk-Power System or the ability to effectively monitor and control the Bulk-Power System. Several other factors, including capabilities and intention of the individual and lack of other mitigating controls, would be required to make the BES Cyber System vulnerable. Therefore, the VRF of lower is consistent with the NERC definition of VRFs.
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 ensures that Responsible Entities take action to prevent unauthorized retrieval of BES Cyber System Information prior to disposal or reuse of asset storage media. The VRF is only applied at the requirement level and the requirement parts are treated equally. R2.1. calls for the Responsible Entity to take action to prevent unauthorized retrieval of BES Cyber System Information at the time of reuse. R2.2. mandates that Responsible Entities take action to prevent unauthorized retrieval of such information at the time of disposal. The VRF of lower is consistent with the risk of a violation across the requirement parts.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007 R7, which has a VRF of Lower. The Requirement has the object of preventing unauthorized retrieval of BES Cyber System Information from asset media prior to reuse or disposal. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately protect information contained in asset storage media during reuse or disposal would not be expected to affect the electrical state or capability of the Bulk Power System or the ability to effectively monitor or control the Bulk-Power System. Several other factors, including capabilities and

<table>
<tr><th colspan="4">VRF and VSL Justifications – CIP-011-1, R2</th></tr>
<tr><td></td><td colspan="3">intention of the individual and lack of other mitigating controls, would be required to make the BES Cyber System vulnerable. Therefore, the VRF of lower is consistent with the NERC definition of VRFs.</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 requirement/sub-requirements in R2 have a common objective to assure confidentiality of BES Cyber System Information. The obligations to protect such information, which may be contained on asset media, during both reuse and destruction, contribute to this objective and only one VRF is assigned.</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 implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)</td><td>The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)</td><td>The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)</td></tr>
</table>

VRF and VSL Justifications – CIP-011-1, 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 previously approved VSLs included a combination of binary and gradated VSLs. The proposed VSLs are consistent with the approved VSLs for the CIP-007 R7 requirement, which maps to this requirement. There is no unintended consequence of lowering the current 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	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement. The VSL does not expand the requirement.

VRF and VSL Justifications – CIP-011-1, R2	
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 processes 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	Interdependent tasks of documentation, identification, and implementation are treated in a uniform manner and have not been separated for each topical area addressed in the requirement.