Violation Risk Factor and Violation Severity Level Justifications

Project 2016-03 — Cyber Security — Supply Chain Risk Management

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **Project 2016-03 — Cyber Security — Supply Chain Risk Management.** Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines. The Cyber Security Supply Chain Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria for Violation Risk Factors

High Risk Requirement

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

Medium Risk Requirement

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

Lower Risk Requirement

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

FERC Guidelines for Violation Risk Factors

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

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

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

Guideline (3) – Consistency among Reliability Standards

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

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

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

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

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

NERC Criteria for Violation Severity Levels

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

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

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

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

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

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

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

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

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

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in an Operations Planning time ~~frame~~ horizon to develop one or more documented supply chain cyber security risk management plan(s). If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective, which is to address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle~~develop one or more documented supply chain cyber security risk management plan(s)~~. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-013-1, R1			
Lower	Moderate	High	Severe

The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the elements in Part 1.2.1 through Part 1.2.6.~~N/A~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the elements in Part 1.2.1 through Part 1.2.6.~~N/A~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.~~The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include one of the elements specified in Parts 1.1 or 1.2.~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop ~~The Responsible Entity did not implement~~one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.~~The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include either of the elements specified in Parts 1.1 or 1.2.;~~ ~~OR~~ ~~The Responsible Entity did not implement one or more~~

			~~documented supply chain risk management plan(s) as specified in the Requirement.~~

VRF Justifications for CIP-013-1, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of 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 Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF Justifications for CIP-013-1, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is 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	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to develop one or more documented supply chain cyber security risk management plan(s) that set forth the controls.
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	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in Operations Planning time ~~frame~~ horizon that requires entities to implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. If violated, failing to implement this plan could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R2

Lower	Moderate	High	Severe
~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.~~N/A	~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.~~N/A	~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.~~N/A	The Responsible Entity did not implement its supply chain cyber security risk management plan(s) as specified in the requirement.~~The Responsible Entity did not review and update, as necessary, its supply chain cyber security risk management plan(s) and obtain CIP Senior Manager or delegate approval within 18 calendar months of the previous review as specified in the Requirement.~~

VSL Justifications for CIP-013-1, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of 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 Ambiguous Language	Guideline 2a: The VSL assignment for R2 is SEVERE which is consistent with ~~not~~ binary criteria. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-013-1, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is 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	Proposed VSL~~s~~ ~~are~~ is based on a single violation and not a cumulative violation methodology.
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	~~An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.~~ A single VSL of Severe is assigned.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	R3 is a requirement in Operations Planning time ~~frame~~ horizon that requires the Responsible Entity to ~~perform~~ periodically review and obtain CIP Senior Manager or delegate approval of supply chain cyber security risk management plans. ~~implement one or more documented process(es) for software integrity and authenticity controls to address risks from compromised software and firmware on high and medium impact BES Cyber Systems.~~ The reliability objective is to ensure plans remain up to date and address current and emerging supply chain-related cyber security concerns and vulnerabilities. If the requirement is violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of ~~a the~~the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation**

VRF Justifications for CIP-013-1, R3	
Proposed VRF	Medium
	R3 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R3			
Lower	Moderate	High	Severe
The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.~~The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.~~

VSL Justifications for CIP-013-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of 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 Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. ~~The VSL assignment for R4 is Severe which is consistent with binary criteria.~~ Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-013-1, R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is 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	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
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	An entity's violation of the review requirement by some number of months less than 18 calendar months does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.~~Only a Severe VSL is assigned.~~
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-~~013~~005-~~01~~06, ~~R4~~R2

Proposed VRF	Medium
NERC VRF Discussion	~~R4~~ R2 is a requirement in an Operations Planning and Same Day Operations time ~~frame~~ horizon to implement one or more documented process~~(es)~~es for controlling vendor remote access to high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of ~~a~~ the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a ~~new~~ revised requirement with the addition of two parts addressing specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** ~~R4~~ R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-~~013~~005-~~1~~6, ~~R4~~R2			
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.~~N/A~~	The Responsible Entity did not implement~~ed one or more documented~~ process~~(es)~~es for one of the applicable items for Requirement Parts 2.1 through 2.3~~controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include one of the elements specified in Part 4.1 through Part 4.3~~.	The Responsible Entity did not implement~~ed one or more documented~~ process~~(es)~~es for two of the applicable items for Requirement Parts 2.1 through 2.3~~controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include two of the elements specified in Part 4.1 through Part 4.3~~.	The Responsible Entity did not implement~~ed one or more documented~~ process~~(es)~~es for three of the applicable items for Requirement Parts 2.1 through 2.3; ~~controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include any of the elements specified in Part 4.1 through Part 4.3;~~ OR The Responsible Entity did not have~~implement~~ one or more ~~documented process(es)~~methods for determining active ~~controlling~~ vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) ~~to high and medium impact BES Cyber Systems as specified in the Requirement~~and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

VSL Justifications for CIP-~~013~~005-~~1~~6, ~~R4~~R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of 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 Ambiguous Language	Guideline 2a: The VSL assignment for ~~R4~~ R2 is not binary. Guideline 2b: The proposed VSLs do not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-~~013~~005-~~1~~6, ~~R4~~R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
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	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-~~013~~010-1, ~~R5~~R1

Proposed VRF	~~Lower~~Medium
NERC VRF Discussion	~~R5~~ R1 is a requirement in Operations Planning time ~~frame~~ horizon that requires the Responsible Entity to implement one or more documented processes that include each of the applicable requirement parts for configuration change management. ~~with at least one asset identified in CIP-002 containing low impact BES Cyber Systems to have one or more documented cyber security policies to address software integrity and authenticity and vendor remote access for its low impact BES Cyber Systems. If violated, it would not, under the emergency, abnormal, or restorative conditions anticipated by the policies, 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.~~ If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a ~~new~~ revised requirement with an additional part to address~~ing~~ specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of ~~Lower~~ Medium is consistent with the NERC VRF definition as discussed above.

VRF Justifications for CIP-~~013~~010-1, ~~R5~~R1	
Proposed VRF	~~Lower~~Medium
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** ~~R5~~ R1 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation

VSLs for CIP-~~013~~010-~~1~~3, ~~R5~~R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity ~~had~~ 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) ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review~~.	The Responsible Entity ~~had~~ 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) ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 16 calendar months but less than or equal to 17 calendar months from the previous review~~.	The Responsible Entity ~~had~~ 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) ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include one of the elements in Parts 5.1 or 5.2~~; OR The Responsible Entity ~~had~~ has The Responsible Entity has a	The Responsible Entity ~~had~~ has not documented or implemented any configuration change management process(es) (R1); ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include either of the elements in Parts 5.1 or 5.2~~; OR The Responsible Entity ~~had~~ has documented and implemented a configuration change

		process to verify the identity of the software source (1.6.1) but does not have a process to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6.2).~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 17 calendar months but less than or equal to 18 calendar months from the previous review.~~	management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1); ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review~~. 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 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 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); OR The Responsible Entity does not have a process to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6).

VSL Justifications for CIP-~~013~~010-~~1~~3, ~~R5~~R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of 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 Ambiguous Language	Guideline 2a: The VSL assignment for ~~R5~~ R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-~~013~~010-~~1~~3, ~~R5~~R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is 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	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
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	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.