NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-03 Cyber Security Supply Chain Risks

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the following Reliability Standards: CIP-005-7, CIP-010-4 and CIP-013-2. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

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.

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 Justification for CIP-005-7, Requirements R1 and R2

The VRFs did not change from the FERC-approved CIP-005-6 Reliability Standard.

VSL Justification for CIP-005-7, Requirements R1 and R2

The VSLs did not change from the FERC-approved CIP-005-6 Reliability Standard.

~~**VRF Justification for CIP-005-7, Requirement R2**~~

~~The VRF did not change from the FERC-approved CIP-005-6 Reliability Standard.~~

~~**VSL Justification for CIP-005-7, Requirement R2**~~

~~The VSL is explained in the following pages.~~

VRF Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VSL Justification for CIP-005-7, Requirement R3

The justification is provided on the following pages.

VRF Justification for CIP-010-4

The VRFs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VSL Justification for CIP-010-4

The VSLs for all requirements in CIP-010-4 did not change from the FERC-approved CIP-010-3 Reliability Standard.

VRF Justification for CIP-013-2~~, Requirement R1~~

The VRFs for all requirements in CIP-013-2 did not change from the FERC-approved CIP-013-1 Reliability Standard.

VSL Justification for CIP-013-2, Requirements R1 and R2

The VSLs did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirements.

~~**VRF Justification for CIP-013-2, Requirement R2**~~

~~The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.~~

~~**VSL Justification for CIP-013-2, Requirement R2**~~

~~The VSL did not substantively change from the FERC-approved CIP-013-1 Reliability Standard. In the Lower, Moderate, High and Severe VSL, the words "and their associated EACMS and PACS" were added to more closely reflect the language of the Requirement.~~

~~**VRF Justification for CIP-013-2, Requirement R3**~~

~~The VRF did not change from the FERC-approved CIP-013-1 Reliability Standard.~~

VSL Justification for CIP-013-2, Requirement R3

The VSL did not change from the FERC-approved CIP-013-1 Reliability Standard.

~~VSLs for CIP-005-7, Requirement 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.~~	~~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;~~

VSL Justifications for CIP-005-7, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs retain the VSLs from the FERC approved CIP-005-6 Reliability Standard, with the following exceptions. In the high and severe VSL, the second levels are removed because Requirement R2 Part 2.4 and Part 2.5 have been removed from the standard language. As a result, the proposed VSLs do not lower 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.

~~VSL Justifications for CIP-005-7, Requirement 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~~	~~Each VSL is based on a single violation and not cumulative violations.~~

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not document one or more processes for *CIP-005-7 Table R3 – Vendor Remote Access Management* for EACMS and PACS. (R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS but did not have a method ~~for detecting~~to authenticate vendor-initiated remote ~~access sessions~~connections for PACS ~~but had method(s) as required by Part 3.1 for other applicable systems types~~ (3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS but did not have a method for detecting vendor-initiated remote ~~access~~	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (R3).

VSLs for CIP-005-7, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
	The Responsible Entity had method(s) as required by Part 3.2 for EACMS but did not have a method to terminate established vendor-initiated remote ~~access sessions~~connections for PACS ~~but had method(s) as required by Part 3.2 for other applicable systems types~~ (3.2).	~~sessions~~connections for ~~other applicable system(s) types~~EACMS (3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS but did not have a method to terminate ~~established~~ authenticated vendor-initiated remote ~~access sessions~~connections for ~~other applicable system(s) types~~EACMS (3.2). ~~OR~~ ~~The Responsible Entity did not have method(s) as required by Part 3.1 or Part 3.2 for PACS and one or more other applicable systems type(s). (3.1 or 3.2)~~ ~~OR~~ ~~The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 for PACS but had method(s) as required by Parts 3.1 and 3.2 other applicable systems types.~~	~~OR~~ ~~The Responsible Entity had methods as required by 3.1 and 3.2 for PACS but did not have any methods as required by Parts 3.1 and 3.2 for other applicable system types (R3).~~

VSLs for CIP-005-7, Requirement R3			
Lower	Moderate	High	Severe
		~~OR~~ ~~The Responsible Entity did not have method(s) as required by Parts 3.1 and 3.2 for PACS and one or more other applicable system types. (3.1 and 3.2)~~	

VSL Justifications for CIP-005-7, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	~~The proposed VSLs are based on the newly formed CIP-005-7 Requirement R3 which are modified from CIP-005-6 Requirement R2 Part 2.4 and Part 2.5. The Requirement R3 were modelled after the original CIP-005-6 Requirement R2 VSL's with the addition of PACS as an applicable system at a lower level than the other applicable system types listed in Requirement R3 Part 3.1 and Part 3.2.~~The requirement is new. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-7, Requirement 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
NERC VRF Discussion	A VRF of Medium is being proposed for 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	The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirement R2~~ which Requirement R3 is modified from~~.

VRF Justifications for CIP-005-7, Requirement R3	
Proposed VRF	**Lower**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	A VRF of Medium for Requirement R3, which addresses Vendor Remote Access Management for EACMS and PACS, is consistent with Reliability Standard CIP-005-7 Requirement ~~R3~~R2, which addresses Remote Access Management and includes requirements for vendor access management for high and certain medium impact BES Cyber Systems and associated PCA.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Medium is consistent with the NERC VRF Definition.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	This requirement does not co-mingle a higher-risk reliability objective with a lesser-risk reliability objective.