NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2019-02 BES Cyber System Information Access Management

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 Project 2019-02 BES Cyber System Information Access Management CIP-004-X. 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-004-X, Requirement R1

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R1

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R2

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R2

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R3

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R3

The VSL did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R4

The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R4

The VSL has been revised to reflect the removal of Part 4.4 (moved to CIP-004-X, Requirement R6, Part 6.2) and a portion of Part 4.1 (moved to CIP-004-X, Requirement R6, Part 6.1). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justification for CIP-004-X, Requirement R5
The VRF did not change from the previously FERC approved CIP-004-6 Reliability Standard.

VSL Justification for CIP-004-X, Requirement R5
The VSL has been revised to reflect the removal of Part 5.3 (moved to CIP-004-X, Requirement R6, Part 6.3). The VSL did not otherwise change from the previously FERC approved CIP-004-6 Reliability Standard.

VRF Justifications for CIP-004-X R6	
Proposed VRF	**Medium**
NERC VRF Discussion	Requirement R6 is a Requirement in the Same Day Operations and Operations Planning time horizons to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-X Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. 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 with Blackout Report	**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	**Guideline 2- Consistency within a Reliability Standard** The proposed VRF is consistent among other FERC approved VRFs within the standard, specifically Requirements R4 and R5 from which Requirement R6 is modified.

VRF Justifications for CIP-004-X R6	
Proposed VRF	**Medium**
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals. The VRF assignment is consistent with similar Requirements in the CIP Reliability Standards.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	**Guideline 4- Consistency with NERC Definitions of VRFs** A 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	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** Requirement R6 contains only one objective, which is to implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable System" identified in *CIP-004-X Table R6 – Access Management for BCSI* that collectively include each of the applicable requirement parts in *CIP-004-X Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-004-X R6			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6)

provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

VSL Justifications for CIP-004-X R6	
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 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 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 cumulative violations.