

Violation Risk Factor and Violation Severity Level Justification

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

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 Number and Name or Standard Number]. 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 Justifications for CIP-008-6, Requirement R4	
Proposed VRF	Lower
NERC VRF Discussion	<p>A VRF of Lower is being proposed for this requirement.</p> <p>The VRF is being established for this requirement. A VRF of lower is appropriate due to the fact that the requirement is associated with reporting obligations, not response to Cyber Security Incident(s), Reportable Cyber Security Incident(s), or Reportable Attempted Cyber Security Incident(s). If violated, is administrative and would not be expected to adversely affect the electrical state or capability of the bulk electric system.</p>
<p>FERC VRF G1 Discussion</p> <p>Guideline 1- Consistency with Blackout Report</p>	N/A
<p>FERC VRF G2 Discussion</p> <p>Guideline 2- Consistency within a Reliability Standard</p>	N/A
<p>FERC VRF G3 Discussion</p> <p>Guideline 3- Consistency among Reliability Standards</p>	The proposed VRF is consistent among other FERC approved VRF’s within the standard.
FERC VRF G4 Discussion	The team relied on NERC’s definition of lower risk requirement.

VRF Justifications for CIP-008-6, Requirement R4

Proposed VRF	Lower
Guideline 4- Consistency with NERC Definitions of VRFs	
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	Failure to report would not, under 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.

VSLs for CIP-008-6, Requirement R4

Lower	Moderate	High	Severe
<p>The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4)</p> <p>OR</p> <p>The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable</p>	<p>The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes within the timeframes pursuant to Requirement R4, Part 4.4 after determination of the attribute(s) not reported pursuant to Requirement R4, Part 4.1. (4.4)</p> <p>OR</p>	<p>The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but failed to notify or update E-ISAC or ICS-CERT, or their successors, within the timeframes pursuant to Requirement R4, Part 4.3.</p>	<p>The Responsible Entity failed to notify E-ISAC or ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. (R4)</p>

VSLs for CIP-008-6, Requirement R4

Lower	Moderate	High	Severe
<p>Cyber Security Incident or Reportable Attempted Cyber Security Incident and the attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant to Requirement R4, Part 4.2.</p>	<p>The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed to report on one or more of the attributes after determination of the attribute pursuant to Requirement R4, Part 4.1.</p>		

VSL Justifications for CIP-008-6, Requirement R4

<p>FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance</p>	<p>The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.</p>
<p>FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties <u>Guideline 2a:</u> The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent <u>Guideline 2b:</u> Violation Severity Level Assignments that Contain Ambiguous Language</p>	<p>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.</p>
<p>FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement</p>	<p>The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.</p>

VSL Justifications for CIP-008-6, Requirement R4**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.