NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2023-03 Internal Network Security Monitoring (INSM)

This document provides the standard drafting team's (DT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in Project 2023-03 INSM. 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 DT 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-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Medium VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM. Collection, detection, and analysis are key factors for the success of any INSM implementation.
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 one or more documented process(es) for ~~INSM~~ internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems ~~(BCS)~~ and medium impact BES Cyber Systems~~BCS~~ with External Routable Connectivity ~~(ERC) within the Responsible Entity's ESP~~ to provide methods for ~~increase the probability of~~ detecting and evaluating anomalous ~~or unauthorized~~ network activity. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. Also, the VRF is reflective of the implementation as a whole, even though~~While~~ the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security documented process(es)~~., the VRF is reflective of the implementation as a whole.~~ Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC	The VRF of Medium for Requirement R1 is consistent with the NERC VRF definition.

VRF Justifications for CIP-015-1, Requirement R1	
Proposed VRF	**[High, Medium, Lower]**
Definitions of VRFs	
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.

VSLs for CIP-15-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications (Part 1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from ~~collected at locations identified in~~ Part 1.1. (Part 1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine ~~appropriate~~ further action(s) (Part 1.3.).	The Responsible Entity did not include any of the applicable requirement ~~parts~~ Parts ~~to increase the probability of detecting an attack that has bypassed other security controls (1.1-1.3)~~for detecting and evaluating anomalous network activity. ~~OR~~ ~~The Responsible Entity did not identify network data collection locations and methods that provide value, based on the network security risk(s), to monitor network activity including connections, devices, and network communications (1.1).~~

VSL Justifications for CIP-015-1, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, ~~but~~ and only reflects the update to the requirement language.
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.
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-015-1, Requirement R2	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate for this requirement. Cyber security assessments enable effective implementation of the CIP standard's requirements for INSM.
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, except during CIP Exceptional Circumstances, one or more documented process(es) to protect ~~INSM~~ internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification~~, except during CIP Exceptional Circumstances~~. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R2 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R2 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.

VSLs for CIP-15-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect ~~INSM~~ internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification ~~(except during CIP Exceptional Circumstances)~~.

VSL Justifications for CIP-015-1, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, ~~but~~ and only reflects the update to the requirement language.
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	The proposed VSL~~s are~~ is ~~not b~~inary. ~~and do~~It does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-015-1, Requirement R2	
Consistent 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	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-015-1, Requirement R3	
Proposed VRF	**[High, Medium, Lower]**
NERC VRF Discussion	A Lower VRF is appropriate 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	This requirement calls for the Responsible Entity to implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring~~network communications~~ data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 except during CIP Exceptional Circumstances.~~ Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain high-impact and medium-impact BES Cyber Systems.
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The VRF of Lower for Requirement R3 is consistent with the NERC VRF definition.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	The VRF of Lower for Requirement R3 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.

VSLs for CIP-15-1, Requirement R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring ~~network communications~~ data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.~~and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3 (except during CIP Exceptional Circumstances).~~

VSL Justifications for CIP-015-1, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSL does not have the unintended consequence of lowering the level of compliance, ~~but~~ and only reflects the update to the requirement language.
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~~s are not~~is binary. ~~and do~~It does 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.
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.