

# Violation Risk Factor and Violation Severity Level Justifications

## Project 2016-02 – Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of the violation risk factor (VRF) and violation severity levels (VSLs) for Requirement R2 in proposed NERC Reliability Standard CIP-003-TCA — Cyber Security — Security Management Controls. 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.

<b>VRF Justifications for CIP-003-TCA, Requirement R2</b>	
<b>Proposed VRF</b>	<b>Lower</b>
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard’s requirements for low impact BES Cyber Systems. The purpose of the plan is for entities to develop an approach involving multiple procedures to address a broad subject matter. Using a plan, Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems.
<b>FERC VRF G1 Discussion</b> Guideline 1 - Consistency with Blackout Report	N/A
<b>FERC VRF G2 Discussion</b> Guideline 2 - Consistency within a Reliability Standard	This requirement calls for the Responsible Entity to implement a documented cyber security plan that contains certain sections specified in Attachment 1. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of sections, not necessarily parts, that must be included in the cyber security plan, the VRF is reflective of the plan as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
<b>FERC VRF G3 Discussion</b> Guideline 3 - Consistency among Reliability Standards	This requirement maps from CIP-003-6, Requirement R2, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
<b>FERC VRF G4 Discussion</b>	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-003-TCA, Requirement R2	
Proposed VRF	Lower
Guideline 4 - Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
<b>FERC VRF G5 Discussion</b> Guideline 5 - Treatment of Requirements that Co-mingle More than One Obligation	The cyber security plan requirement encompasses a number of subject matter areas for low impact BES Cyber Systems. The VRF is identified at the risk level represented by all of the plan areas in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.

VSLs for CIP-003-TCA, Requirement R2			
Lower	Moderate	High	Severe
<p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (R2)</p> <p>OR</p> <p>The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for</p>	<p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing</p>	<p>The Responsible Entity documented the physical access controls for its assets containing low impact BES Cyber Systems, but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing</p>	<p>The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BES Cyber Systems according to Requirement R2, Attachment 1. (R2)</p>

<p>electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document one or more Cyber Security Incident response plans according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber</p>	<p>low impact BES Cyber Systems, but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BES Cyber System(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more incident response plans within its cyber security plan(s) for its</p>	<p>low impact BES Cyber Systems, but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)</p> <p>OR</p> <p>The Responsible Entity documented one or more Cyber Security Incident response plans within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)</p>	
---	---	--	--

<p>Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to Requirement R2, Attachment 1, Section 5.3. (R2)</p>	<p>assets containing low impact BES Cyber Systems, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible</p>	<p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation for threat of detected malicious code on</p>	
--	---	---	--



	<p>Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (R2)</p> <p>OR</p> <p>The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (R2)</p>	<p>the Removable Media prior to connecting Removable Media to a low impact BES Cyber System according to Requirement R2, Attachment 1, Section 5.3. (R2)</p>	
--	---	--	--

VSL Justifications for CIP-003-TCA, Requirement R2

<p><b>FERC VSL G1</b> Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance</p>	<p>The requirement maps to the previously-approved Requirement R2, CIP-003-6. Therefore, the proposed VSLs do not have the unintended consequence of lowering the level of compliance.</p>
<p><b>FERC VSL G2</b> 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><b>FERC VSL G3</b> Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement</p>	<p>The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.</p>

**VSL Justifications for CIP-003-TCA, Requirement R2**

<p><b>FERC VSL G4</b> Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations</p>	<p>The VSLs are based on a single violation, and not cumulative violations.</p>
<p><b>FERC VSL G5</b> Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs</p>	<p>There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security plan(s) but fails to address one or more of the required sections of Attachment 1. A single failure of this requirement does not compromise network computer security.</p>
<p><b>FERC VSL G6</b> VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence</p>	<p>The action of the requirement is to implement documented cyber security plan(s). Documentation of the plan(s) is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the plan in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity implemented all the required elements of the plan. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.</p>