130 FERC ¶ 61,211
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Chairman;
Marc Spitzer, Philip D. Moeller,
and John R. Norris.

Mandatory Reliability Standards for Critical Infrastructure Protection	Docket No. RM06-22-008

ORDER ADDRESSING VIOLATION SEVERITY LEVEL ASSIGNMENTS FOR CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

(Issued March 18, 2010)

1. On June 30, 2009, the North American Electric Reliability Corporation (NERC) submitted a filing in compliance with Order No. 706, seeking the approval of Violation Severity Levels for eight Version 1 Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-1 through CIP-009-1 (Compliance Filing).[1] In this Order, the Commission approves the proposed Violation Severity Level assignments, as revised as discussed herein, effective as of the date of issuance of this order. Further, the Commission establishes additional guidance for determining appropriate Violation Severity Levels in the specific context of cyber security Requirements. Applying the new and existing guidelines for analyzing Violation Severity Levels, the Commission directs NERC to submit a compliance filing modifying 57 sets of Violation Severity Level assignments within 60 days of the issuance of this order, as discussed below.

I. Background

A. Violation Severity Levels

2. NERC and the Regional Entities use Violation Severity Levels to determine penalties for individual violations of Requirements of a Reliability Standard. A Violation Severity Level is a post-violation measurement of the degree to which a Reliability

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009).

Standard Requirement was violated ("Lower," "Moderate," "High," or "Severe"). To establish a Base Penalty range for a violation, NERC considers the Violation Severity Level, together with a Violation Risk Factor, which represents the potential risk to reliability.

3. In a June 2007 Order, the Commission directed NERC to develop Violation Severity Levels for each Requirement and sub-Requirement of each previously-approved Reliability Standard.[2] NERC submitted the required filing and, in a June 2008 Order, the Commission approved Violation Severity Levels corresponding to the Requirements and sub-Requirements of 83 Reliability Standards, not including the CIP Reliability Standards.[3] The Commission also directed NERC to submit a compliance filing and several reports. In addition, the Commission developed four guidelines for evaluating the validity of Violation Severity Level assignments. Specifically, Violation Severity Levels: (1) should not have the unintended consequence of lowering the current level of compliance; (2) should ensure uniformity and consistency among all approved Reliability Standards in the determination of penalties; (3) should be consistent with the corresponding Requirement; and (4) should be based on a single violation, not on a cumulative number of violations. The Commission also noted that it retains the flexibility to consider the development of additional guidelines as appropriate.[4]

4. On June 30, 2008, in a subsequent filing to revise certain Reliability Standards, NERC proposed to change the manner in which it assigns Violation Severity Levels, essentially eliminating assignments for certain sub-requirements. While the Commission found that it was "premature" to change its current policy of assigning Violation Severity Levels to each Requirement and sub-Requirement, it encouraged NERC to develop a comprehensive approach that would better facilitate the assignment of Violation Severity Levels.[5]

---

[2] *North American Electric Reliability Corp.*, 119 FERC ¶ 61,248, at P 80 (June 2007 Order), *order on clarification*, 120 FERC ¶ 61,239 (2007).

[3] *North American Electric Reliability Corp.*, 123 FERC ¶ 61,284 (VSL Order), *order on reh'g and clarification*, 125 FERC ¶ 61,212 (2008) (VSL Rehearing Order).

[4] VSL Order, 123 FERC ¶ 61,284 at P 17 n.12.

[5] *Version Two Facilities Design, Connections and Maintenance Reliability Standards*, Order No. 722, 126 FERC ¶ 61,255, at P 44-46 (2009). In August 2009, NERC submitted an informational filing describing more fully its plans for a new, comprehensive approach to assigning Violation Severity Levels. *See* NERC, Informational Filing Regarding the Assignment of Violation Risk Factors and Violation Severity Levels, Docket No. RM08-11-000 (Aug. 10, 2009). NERC has not submitted a

(continued)

B. Order No. 706

5. NERC submitted eight CIP Reliability Standards for Commission approval: CIP-002-1 - Critical Cyber Asset Identification; CIP-003-1 - Security Management Controls; CIP-004-1 - Personnel & Training; CIP-005-1 - Electronic Security Perimeter(s); CIP-006-1 - Physical Security of Critical Cyber Assets; CIP-007-1 - Systems Security Management; CIP-008-1 - Incident Reporting and Response Planning; CIP-009-1 - Recovery Plans for Critical Cyber Assets. The eight Version 1 CIP Reliability Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific Requirements to safeguard critical cyber assets.

6. In Order No. 706, issued on January 18, 2008, the Commission approved the eight Version 1 CIP Reliability Standards. In addition, pursuant to section 215(d)(5) of the Federal Power Act (FPA), the Commission directed NERC to develop modifications to address specific issues. NERC's submission of the eight CIP Reliability Standards did not include Violation Severity Level assignments. The Commission, therefore, also directed NERC to file Violation Severity Levels before July 1, 2009.[6]

II. NERC Compliance Filing

7. In the instant Compliance Filing, NERC proposes 118 sets of Violation Severity Levels corresponding to 171 Requirements and sub-Requirements contained in the Version 1 CIP Reliability Standards. NERC's filing does not individually assign any Violation Severity Levels to the remaining sub-Requirements; rather, NERC proposes that they would be governed by the Violation Severity Levels assigned to their respective main Requirements (14 of the 118 sets of Violation Severity Levels). NERC states that, in developing the Violation Severity Levels for the CIP Reliability Standards, the drafting team considered NERC's "VSL Development Guidelines and Criteria" (included in the filing as Exhibit E, for informational purposes only), a reference document that establishes seven categories to classify the various types of Requirements in NERC Reliability Standards.

8. NERC explains the development of the proposed Violation Severity Levels and its responses to issues that arose during the balloting process, namely: (1) distinguishing between risk and severity, as Violation Severity Levels measure the degree to which a provision is violated; (2) efforts to limit use of generic language to describe severity

---

formal filing on its proposed approach to setting Violation Severity Levels for Commission action as of the date of this order.

[6] *See* Order No. 706, 122 FERC ¶ 61,040 at P 758.

(such as "minor element") and make text as specific as possible; and (3) whether the Severe level should be assigned to "binary" Requirements.[7]

9. NERC also states that stakeholders raised concern regarding the potential for "double jeopardy" where Violation Severity Levels are assigned to every Requirement and sub-Requirement of a Reliability Standard. NERC decided the double jeopardy issue was beyond the scope of the drafting team because it is a compliance issue. NERC stated that, in accordance with current Commission policy, the standards drafting team assigned a Violation Severity Level to every Requirement and sub-Requirement that had a Violation Risk Factor previously assigned to it.

10. NERC states that the Violation Severity Levels received 84 percent weighted segment approval with 87 percent of the ballot pool participating. The NERC Board of Trustees approved the proposed Violation Severity Levels on June 29, 2009. NERC requests that the Commission approve the Violation Severity Levels for the Version 1 CIP Reliability Standards, effective on approval.

III. Notice of Filing

11. Notice of NERC's June 30, 2009 compliance filing was published in the *Federal Register*, 74 Fed. Reg. 39314 (2009), with interventions and comments due on or before August 20, 2009. The Southwest Transmission Dependent Utility Group (STDUG) filed a timely motion to intervene and comment.

IV. Discussion

A. Procedural Matters

12. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2009), the timely, unopposed motion to intervene serves to make the entity that filed it a party to this proceeding.[8]

---

[7] NERC explains that binary Requirements are those that can only be fully met or not met, and explains that violations of binary Requirements are designated as Severe because the Violation Severity Level is a measure of how well or completely the Requirement has been met (as distinguished from the Violation Risk Factor consideration of the expected impact to the Bulk-Power System resulting from a violation of a particular Requirement).

[8] STDUG submitted comments that are beyond the scope of the immediate proceeding because they pertain to a proposed relay loadability Reliability Standard, PRC-023-1, which is pending before the Commission in Docket No. RM08-13-000.

B. Commission Determination

13. NERC submitted 118 sets of Violation Severity Levels. The Commission approves the proposed Violation Severity Levels. Further, for the reasons discussed below, the Commission directs NERC to submit modifications to 57 sets of Violation Severity Level assignments within 60 days of the issuance of this order.[9]

14. In making these determinations, the Commission considered the Violation Severity Level Guidelines set forth in the VSL Order. Further, in the VSL Order, the Commission stated that it retains the flexibility to consider the development of additional guidelines as appropriate.[10] The Commission determines that, in the context of the cyber security Requirements of the CIP Reliability Standards, additional guidelines are appropriate to better reflect certain characteristics of the cyber environment. Specifically, we have developed the following two additional guidelines for analyzing the validity of Violation Severity Levels that pertain to cyber security:

(1) Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary rather than gradated Violation Severity Levels; [11] and

(2) Violation Severity Levels for cyber security Requirements containing interdependent tasks of documentation and implementation should account for their interdependence.

---

[9] The Appendix to this order lists the Version 1 CIP Reliability Standard Requirements for which the Commission is directing revisions to corresponding Violation Severity Levels. The revisions are shown in redline against the Violation Severity Levels proposed in NERC's Compliance Filing. In addition, the existing Version 1 Violation Risk Factors previously approved by the Commission are shown for reference. The Violation Severity Levels that are approved without change are not shown in the Appendix.

[10] VSL Order, 123 FERC ¶ 61,284 at P 17 n.12. As noted, the VSL Order did not address Violation Severity Levels assigned to CIP Reliability Standards.

[11] Violation Severity Level "gradation" refers to the ability to identify degrees of noncompliance that result in performance that partially meets the reliability objective of the Requirement such that the performance or product has some reliability-related value. Violation Severity Level sets with several levels are "gradated" and those with fewer levels than others are "less gradated." VSL Order, 123 FERC ¶ 61,284 at P 26-27; VSL Rehearing Order, 125 FERC ¶ 61,212 at P 65.

These guidelines are discussed below and applied in our analysis of whether to accept the proposed Violation Severity Levels corresponding to the provisions of the CIP Reliability Standards.

1. Additional Guidelines to Address Cyber Security Characteristics

a. CIP Guideline 1: Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary Violation Severity Levels

15. A single lapse of computer protection can create the opening for malicious activity that has systemic critical infrastructure consequences. In this sense, the control systems that support Bulk-Power System reliability are "only as secure as their weakest links." In such cases, the severity of non-compliance is not necessarily dependent on the number of similar lapses because a single vulnerability opens the computer network to potential malicious activity. Thus, in the context of cyber-security, severity of non-compliance is in many instances better assessed in a binary, as opposed to a gradated approach.

16. Although the Commission previously stated a preference for assigning Violation Severity Levels in multiple levels, i.e., the gradated approach, it also recognized that a binary approach can be appropriate, such as when a failure to comply is absolute.[12] The Commission concludes that a Requirement of the CIP Reliability Standards with the "weakest link" characteristic is such an instance, and directs NERC to revise specific Violation Severity Level assignments for such Requirements to employ a binary approach.[13]

17. A number of CIP Reliability Standards Requirements address a "weakest-link" vulnerability where the system is either in a "secure" or "not secure" state. In particular, the gradation of Violation Severity Levels across several severity levels is not appropriate for specific CIP Reliability Standards that require security actions to be taken for all Critical Cyber Assets or concern all access points to such assets. For example, CIP-005-1, Requirement R4 requires a vulnerability assessment of electronic access points to an Electronic Security Perimeter. If any one required preventative measure is neglected, the

[12] VSL Rehearing Order, 125 FERC ¶ 61,212 at P 65.

[13] The relevant provisions of the Version 1 CIP Reliability Standards, also identified in the Appendix, are as follows: CIP-004-1, Requirement R2.1; CIP-005-1, Requirements R1, R1.4, R1.5, R1.6, R2.2, R2.5, R3, R3.1, R3.2, R4 and R5.2; CIP-006-1 Requirements R1.5, R1.8 and R6; and CIP-007-1, Requirements R1, R2.1, R2.2, R4, R5.1.1, R5.2.3, R5.3, R6, and R8.

result is one or more insecure points of ingress – an unmitigated vulnerability that presents a severe risk to the Critical Cyber Asset.

18. There are also instances where monitoring controls present a "weakest link" condition. For example, CIP-005-1, Requirement R 3.2 requires responsible entities to detect attempts at unauthorized access to one or more components of a Critical Cyber Asset. If even one access point does not have monitoring processes implemented that include detection and alerting for attempts at or actual unauthorized accesses, there is an opportunity for undetected unauthorized access to the Critical Cyber Asset.

19. A variation on this theme is presented by CIP-007-1, Requirement R1, which is intended to address adverse consequences relating to adding or changing Cyber Assets within the Electronic Security Perimeter. The Requirement encompasses protection tasks enumerated in three sub-Requirements, and NERC proposes to gradate according to the number of sub-Requirements completed. However, when viewed independently, each sub-Requirement is binary; compliance with each is needed to complete the parent Requirement. Therefore, the Commission directs a binary approach, as shown in the Appendix.

b. CIP Guideline 2: Violation Severity Levels for Cyber Security Requirements Containing Interdependent Tasks of Documentation and Implementation Should Account for Their Interdependence

20. Certain provisions of the CIP Reliability Standards identify two or more tasks within one Requirement. For example, some provisions of the CIP Reliability Standards require performance of both implementation and documentation tasks. For a number of these Requirements, NERC proposes Violation Severity Level sets with gradations parsing out multiple actions contained in the Requirement. In fact, NERC's approach is consistent with the guidance provided in the VSL Order, in which the Commission stated its concern that the Violation Severity Levels need to consider the scenario where an entity has documented all the required elements in a plan, but failed to implement the plan.[14] However, upon further consideration, while this approach is generally appropriate for assigning Violation Severity Levels, a different approach is needed in the context of critical infrastructure protection, for the reasons discussed below.

21. In critical infrastructure protection, and especially in the cyber security environment, the implementation of security measures is largely dependent on complex plans, policies and procedures that must be repeatable and verifiable. This necessitates documentation of both (1) the procedures to be followed and (2) verification that the

[14] VSL Order, 123 FERC ¶ 61,284 at P 34.

procedures were followed as directed. These complex procedures require clear and consistent instructions (documentation) and consistent execution (implementation). Further, these procedures also require a method for reporting their completion. Each component is part of an iterative operation security framework. Planning, design and implementation of documentation enable the effective implementation of security measures and documentation of results. In fact, for certain Requirements of CIP Reliability Standards, it is difficult if not impossible to demonstrate that a network operator has implemented a specific plan or program without developing the documentation for the plan or program. Thus, the Commission believes that the interdependency between documentation and implementation in the context of critical infrastructure should be recognized in Violation Severity Level assignments.

22. For instance, CIP-005-1, Requirement R2 provides that a responsible entity must implement and document the processes and mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). NERC proposes gradated Violation Severity Levels based on implementation without documentation and vise versa. However, verifying the successful electronic implementation of many controls regarding electronic access depends on the documentation. Thus, separating implementation and documentation for Violation Severity Level assignments is not appropriate in this instance. If a responsible entity documents the processes and mechanisms, but does not follow through to implement them, then the entity is not secure. Also, if the entity attempts to implement the controls set forth in Requirement R2, but does not have documented organizational processes and mechanisms required to control electronic access to the Electronic Security Perimeter, the implementation may be faulty due to such factors as an imperfect memory of an employee or a recent change to cyber assets with which an employee is unfamiliar.

23. Other provisions of the CIP Reliability Standards include similar interdependent tasks, and present a similar concern with the appropriate assignment of Violation Severity Levels. Accordingly, we direct NERC to revise seventeen sets of Violation Severity Level assignments, specified in the Appendix, to address interdependency concerns discussed above.[15]

2. Timeliness of Compliance and Commission Guideline No. 1

24. For several Requirements in the CIP Reliability Standards, NERC proposes that the Violation Severity Level sets should be gradated according to the length of time in which an entity is not compliant. For certain of these Violation Severity Level sets, the

[15] Version 1 CIP Reliability Standards: CIP-003-1, Requirements R1, R1.3, R3.3, R4, R5, and R6; CIP-005-1, Requirements R2, R3, and R3.1; CIP-006-1, Requirements R2, R3, and R4; CIP-007-1, Requirements R2, R3, R4.2, R5, R6.1.

Commission believes that the proposed lengths of time are too permissive and violate the Commission's Guideline No. 1 as described in the VSL Order. Guideline No. 1 states that Violation Severity Level assignments should not have the unintended consequence of lowering the current level of compliance.[16] For example, in that Order, we expressed a concern that "assigning up to 25 percent non-compliance at the 'Lower' Violation Severity Level may have the unintended consequence of signaling that a greater level of non-compliance than historically evident is condoned.[17] The Commission further explained its intent to rely on historical compliance data to establish the current level of compliance in the VSL Rehearing Order.

25. However, the CIP Requirements at issue here are new and historical compliance data is extremely limited at best. While certain entities had to be auditably compliant with some of these CIP Requirements by June 30, 2009, the earliest auditably compliant date for other CIP Requirements is June 30, 2010.

26. The Violation Severity Level assignments proposed by NERC for these Requirements allow multiples of the time periods specified in the Requirement language before a violation is considered severe. For example, CIP-003-1, Requirement R3.1 requires an entity to document exceptions to its security policy within 30 days of being approved by the senior manager or delegate(s). The proposed Violation Severity Level assignments would allow an entity to take almost twice as long (59 days) to document exceptions and only trigger a "Lower" Violation Severity Level. They would allow an entity to take four-times as long (120 days) as the Requirement language specifies before triggering a "Severe" Violation Severity Level.

27. The magnitude of non-compliance allowed by NERC's proposed gradations for these CIP Requirements before reaching the "Severe" level of Violation Severity Level, in light of the lack of applicable historical compliance data that proves otherwise, leads the Commission to conclude that the proposed Violation Severity Level assignments for these CIP Requirements would condone a greater level of non-compliance than is appropriate. In making this determination, without applicable historical evidence, the Commission is placing significant weight on the terms of the Requirements in question. Once such historical evidence accumulates, NERC may return to us to demonstrate the basis for greater gradation. Until such a time, the Commission directs NERC to revise specific Violation Severity Level assignments, specified in the Appendix, to address the concern described above about levels of non-compliance.[18]

---

[16] VSL Order, 123 FERC ¶ 61,284 at P 17.

[17] *Id*. P 21.

[18] This reasoning applies to gradation modifications directed to CIP-003-1,

(continued)

3. Consistency and Clarity Concerns

28. In the VSL Order, the Commission's Guideline 2(b) provides that, to better ensure consistency and uniformity in the determination of penalties, Violation Severity Level assignments should not contain ambiguous language.[19] In numerous Violation Severity Levels corresponding to the CIP Reliability Standards, NERC uses the term "nor" to refer to two or more tasks where other language is more appropriate to clearly indicate that non-compliance of either one is captured by the Violation Severity Level category. The Commission directs revisions to clarify conjunction usage issues in various Violation Severity Level assignments, along with other changes, as identified in the Appendix.[20]

29. The Commission has identified other matters of consistency and clarity in these and other sets of Violation Severity Level assignments that require revision based on the application of Guideline 2(b) set forth in the VSL Order. Specifically, the Commission stated that "in general, relative and subjective language is subject to multiple interpretations that could result in inconsistent application of the Violation Severity Levels when determining penalties."[21]

30. For example, CIP-003-1, Requirement R3 specifies that a responsible entity must document as exceptions, authorized by the senior manager, instances where it cannot conform to its cyber security policy. The cyber security policy is required by CIP-003-1, Requirement R1, which specifies that the policy must address the Requirements in standards CIP-002-1 through CIP-009-1. NERC's proposed Violation Severity Levels for CIP-003-1, Requirements R3, R3.2 and R3.3 insert the parenthetical phrase, "pertaining to CIP-002 through CIP-009" even though this phrase does not appear in these specific Requirements. This phrase could be misunderstood to mean that an entity has the discretion to except itself from Requirements of the mandatory CIP Reliability Standards, which is not permitted.[22]

Requirements R2.2 and 3.1; CIP-007-1, Requirement R3.1; and CIP-009-1, Requirement R3.

[19] VSL Order, 123 FERC ¶ 61,284 at P 22-23, 28-31.

[20] Commission approved Reliability Standards: CIP-003-1, Requirements R1, R1.3, R2.1, R3.3, R4, R4.3, R5, R5.1.1, and R6; CIP-005-1, Requirements R1, R1.4, R2, R2.2, R3, and R3.1; CIP-006-1, Requirements R1.5, R2, R3, and R4; and CIP-007-1, Requirements R1, R2, R2.1, R2.2, R3, R4, R4.2, R5, R5.3, and R6.1.

[21] VSL Order, 123 FERC ¶ 61,284 at 31.

[22] Order No. 706, 122 FERC ¶ 61,040 at P 376.

31. CIP-004-1, Requirement R2.2 raises an issue of consistency of sub-parts with the parent Requirement. The sub-Requirements of CIP-004-1, Requirement R2 mandate minimum cyber security training tasks. NERC proposes gradation of Violation Severity Levels for these sub-Requirements based on how many of the minimum tasks are not performed. However, an effective and complete training program dealing with cyber assets requires all of these components. Therefore, the Commission directs a binary approach to reflect non-performance of one or more of the minimum required cyber security training tasks set forth in CIP-004-1, Requirement R2.2.

32. NERC's proposed Violation Severity Level sets include several that contain extraneous language that could cause confusion. For example, CIP-004-1, Requirement R2.3 requires that an entity "shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records." NERC's proposed Violation Severity Level text assumes that the training was "conducted annually," and distinguishes gradation based on failure to "include either the date the training was completed or attendance records." However, for the entity to plausibly "maintain documentation" that the training is conducted at least "annually," the entity must include at a minimum the date(s) the training was completed. Therefore, the either/or phrase cited above is not needed because the only remaining aspect of the Requirement to reference is the existence of "attendance records." The Commission directs NERC to remove the extraneous language concerning the date of training.

33. For the reasons set forth above, the Commission directs the ERO to revise certain Violation Severity Level assignments to remove ambiguity and improve consistency, as set forth in the Appendix.[23]

4. Violation Severity Levels that Address Main and Sub-Parts Together

34. As discussed earlier, the Commission previously directed NERC to develop Violation Severity Level sets for each Requirement and sub-Requirement of each Reliability Standard.[24] However, NERC's filing included 53 sub-Requirements for which

[23] Commission-approved Reliability Standards: CIP-003-1 Requirements R2.1, R3, R3.2 and R3.3, R4.3, R5.1.1, R6; CIP-004-1 Requirements R2.2, R2.3 and R3; CIP-005-1, Requirements R3 and R3.1; CIP-006-1, Requirement R1.7; CIP-007-1 Requirements R5.1.1, R6.4 and R7; CIP-008-1, Requirements R1 and R2; and CIP-009-1, Requirement R1.

[24] June 2007 Order, 119 FERC ¶ 61,248 at P 80. As noted earlier, NERC has filed an Informational Filing describing how it intends, at a future time, to propose a comprehensive reformulation of Violation Severity Levels, but has yet to submit a formal filing for Commission approval.

NERC proposes to apply the Violation Severity Levels assigned to the respective parent Requirements, 14 in all.[25]

35. Nonetheless, we will accept these Violations Severity Levels as an exception to our current policy. We are satisfied that none of the sub-parts without a Violation Severity Level assignment constitutes an independent compliance Requirement, separate from the primary Requirement. Accordingly, without ruling on the appropriateness of this approach for other standards or other versions of the CIP Reliability Standards, the Commission accepts the Violation Severity Levels assignments associated with these 14 provisions, and will not require NERC to submit additional assignments for them.

36. While approving this consolidated assignment of Violation Severity Level sets for these 14 Requirements, we are concerned about possible confusion as to which Violation Risk Factor applies in the event of one or more violations,[26] since the Commission has already approved Violation Risk Factor designations for each of the respective 53 sub-Requirements. To address this, we clarify that in such cases the Compliance Enforcement Authority[27] should determine the base penalty range for each sub-part of the Requirement that is violated by applying the Violation Risk Factor corresponding to that sub-part.[28]

---

[25] One of these 14 Requirements is CIP-002-1, Requirement R 2.1, for which the Commission approves the Violation Severity Level set NERC proposed to address it and its seven sub-Requirements. The remaining thirteen of these Requirements appear in Appendix A because their respective Violation Severity Level sets are subject to revisions directed by this order; these revisions also address the remaining 46 sub-Requirements for which NERC did not file individual Violation Severity Levels.

[26] *See* NERC's August 10, 2009 informational filing at 10-12.

[27] *See* NERC Rules of Procedure, Appendix 4C, NERC Compliance Monitoring and Enforcement Program, section 1.1.7 (stating the Compliance Enforcement Authority is NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards).

[28] *See also* NERC Sanctions Guidelines, section 3.10 (stating that "in instances of multiple violations related to a single act or common incidence of non-compliance," the resulting penalty should "generally be at least as large or expansive as what would be called for individually for the most serious of the violations.").

V. Conclusion

37. Applying the Commission's previously articulated guidelines for analyzing Violation Severity Level assignments, as well as additional guidelines that apply specifically in the cyber security context, we approve the proposed Violation Severity Level assignments. In addition, we direct NERC to revise 57 sets of Violation Severity Level assignments, as discussed in the body of this order and set forth in the Appendix. NERC must submit a compliance filing with the revised Violation Severity Level assignments within 60 days of date of issuance of this order.

The Commission orders:

(A) NERC's compliance filing is hereby approved, effective as of the date of this order, as discussed in the body of this order.

(B) NERC is hereby directed to submit a compliance filing that includes revised Violation Severity Level assignments as identified in the Appendix, within 60 days of the date of this order, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

Appendix

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-003-1	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	MED	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.	CIP Guideline 2 VSL Guideline 2(b)
CIP-003-1	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOW	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.	CIP Guideline 2 VSL Guideline 2(b)
CIP-003-1	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	LOW	N/A	N/A	The senior manager is identified by name, title, and date of designation but the designation is missing business phone or business address	Identification of the senior manager is missing one of the following: name, title, or date of designation.	VSL Guideline 2(b)
CIP-003-1	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOW	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.	VSL Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-003-1	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	LOW	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were documented, **but** were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were not documented.	VSL Guideline 2(b)
CIP-003-1	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	LOW	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).	VSL Guideline 1
CIP-003-1 .	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	LOW	N/A	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy in R1, but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.	VSL Guideline 2(b)
CIP-003-1	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	LOW	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved on an annual basis by the senior manager or delegate(s) to ensure the exceptions are still required and valid or the review and approval is not documented.	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-003-1	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MED	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	CIP Guideline 2 VSL Guideline 2(b)
CIP-003-1	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	LOW	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.	VSL Guideline 2(b)
CIP-003-1	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOW	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.	CIP Guideline 2 VSL Guideline 2(b)
CIP-003-1	R5.1.1.	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	LOW	N/A	N/A	The Responsible Entity did identify the personnel by name, title, and the information for which they are responsible for authorizing access, but the business phone is missing.	Personnel are not identified by name, title, or the information for which they are responsible for authorizing access.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-003-1	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	LOW	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.	CIP Guideline 2 VSL Guideline 2(b)
CIP-004-1	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	MED	N/A	N/A	N/A	Not all personnel having access to Critical Cyber Assets, including contractors and service vendors, were trained within ninety calendar days of such authorization.	CIP Guideline 1
CIP-004-1	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MED	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-004-1	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	LOW	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	VSL Guideline 2(b)
CIP-004-1	R3.	Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	MED	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R3, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in more than thirty (30) days of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, as stated in R3, for personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.	VSL Guideline 2(b)
CIP-005-1	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	MED	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter, OR the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-005-1	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	MED	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified ~~and~~ OR is not protected pursuant to the requirements of Standard CIP-005.	CIP Guideline 1 VSL Guideline 2(b)
CIP-005-1	R1.5.	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	MED	N/A	N/A	N/A	A Cyber Asset used in the access control and monitoring of the Electronic Security Perimeter(s) is not provided in one (1) or more of the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP- 006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP- 009.	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-005-1	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	LOW	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of one or more of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.	CIP Guideline 1
CIP-005-1	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	MED	N/A	N/A	N/A	The Responsible Entity did not implement or did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-005-1	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	MED	N/A	N/A	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and services.	CIP Guideline 1 VSL Guideline 2(b)
CIP-005-1	R2.5.	The required documentation shall, at least, identify and describe:	LOW	N/A	N/A	N/A	The required documentation for R2 did not include one or moreof the elements described in R2.5.1 through R2.5.4	CIP Guideline 1 CIP Guideline 2
CIP-005-1	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	MED	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.	CIP Guideline 1 CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-005-1	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	MED	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access point to dial-up devices.	CIP Guideline 1 CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-005-1	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	MED	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR the above alerts do not provide for appropriate notification to designated response personnel. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-005-1	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	MED	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for one or more of theaccess points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.	CIP Guideline 1
CIP-005-1	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	LOW	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.	CIP Guideline 1
CIP-006-1	R1.5.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	MED	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include procedures for reviewing access authorization requests or does not includerevocation of access authorization, in accordance with CIP-004 Requirement R4.	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-006-1	R1.7.	Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.	LOW	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration. OR The plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	VSL Guideline 2(b)
CIP-006-1	R1.8.	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	LOW	N/A	N/A	N/A	A Cyber Asset used in the access control and monitoring of the Physical Security Perimeter(s) is not afforded one (1) or more of the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP- 006 Requirements R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-006-1 .	R2.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	MED	N/A	N/A	N/A -	The Responsible Entity has not documented, or has not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using at least one of the access control methods identified in R2.1, R2.2, R2.3, or R2.4.	CIP Guideline 2 VSL Guideline 2(b)
CIP-006-1	R3.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	MED	N/A	N/A	N/A	The Responsible Entity **has not documented or has not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twentyfour hours a day, seven days a week using at least one of the monitoring methods identified in Requirements R3.1 or R3.2. OR One or more unauthorized access attempts have not been reviewed immediately and handled in accordance with the procedures specified in CIP-008.	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-006-1	R4.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	LOW	N/A	N/A	N/A	The Responsible Entity **has not implemented or has not documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the logging methods identified in Requirements R4.1, R4.2, or R4.3 or has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	CIP Guideline 2 VSL Guideline 2(b)
CIP-006-1	R6.	Maintenance and Testing — The Responsible Entity shall implement maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	MED	N/A -	N/A	N/A	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. OR The implemented program does not include one or more of the requirements; R6.1, R6.2, and R6.3.	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP- 007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	MED	N/A	N/A	N/A	The Responsible Entity did not ensure the prevention of adverse affects described in R1, by not including the required minimum significant changes, OR The Responsible Entity did not address one or more of the following: R1.1, R1.2, R1.3.	CIP Guideline 1 VSL Guideline 2(b)
CIP-007-1	R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MED	N/A	N/A	N/A	The Responsible Entity did not establish or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	CIP Guideline 2 VSL Guideline 2(b)
CIP-007-1	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	MED	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic SecurityPerimeter(s).	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	MED	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).	CIP Guideline 1 VSL Guideline 2(b)
CIP-007-1 .	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	LOW	N/A	N/A	N/A	The Responsible Entity **did not establish or did not** document, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s)	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	LOW	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.	VSL Guideline 1
CIP-007-1	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	MED	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, , on <u>one</u> or more Cyber Assets within the Electronic Security Perimeter(s).	CIP Guideline 1 VSL Guideline 2(b)
CIP-007-1	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	MED	N/A	N/A	N/A	The Responsible Entity **did not documentor did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R5	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.		N/A	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	CIP Guideline 2 VSL Guideline 2(b)
CIP-007-1	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	LOW	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.	CIP Guideline 1 VSL Guideline 2(b)
CIP-007-1	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	MED	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity has not implemented (one or more components of) a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOW	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2., R5.3.3 . **or** **does not use passwords** subject to R5.3.1, R5.3.2., R5.3.3.	CIP Guideline 1 VSL Guideline 2(b)
CIP-007-1	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	LOW	N/A	N/A	N/A	The Responsible Entity as technically feasible, did not implement automated tools or organizational process controls, , to monitor system events that are related to cyber security on one % or more of Cyber Assets inside the Electronic Security Perimeter(s).	CIP Guideline 1
CIP-007-1	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	MED	N/A	N/A	N/A	The Responsible Entity **did not implement or did not document** the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	CIP Guideline 2 VSL Guideline 2(b)
CIP-007-1	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOW	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.	CIP Guideline 1 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R7.	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	LOW	N/A	N/A	The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 **but** did not address redeployment as specified in R7.2.	The Responsible Entity did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005. OR The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005 but did not address disposal as specified in R7.1.. OR did not maintain records pertaining to disposal or redeployment as specified in R7.3 .	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-007-1	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOW	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment on one or more Cyber Assets within the Electronic Security Perimeter at least annually. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.	CIP Guideline 1
CIP-008-1	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	LOW	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with R1.4 or R1.5.	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all components of the sub-requirements R1.1 through R1.6.	VSL Guideline 2(b)
CIP-008-1	R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	LOW	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP-009-1	R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	MED	N/A	N/A	N/A	The Responsible Entity has not created or has not annually reviewed their recovery plan(s) for Critical Cyber Assets OR has created a plan but did not address one or more of the requirements CIP- 009-1 R1.1 **and** R1.2.	VSL Guideline 2(b)
CIP-009-1	R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	LOW	N/A	N/A	. N/A	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were not communicated to personnel responsible for the activation and implementation of the recovery plan(s) within 90 calendar days of the change.	VSL Guideline 1

Document Content(s)