134 FERC ¶ 61,045
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

North American Electric Reliability Corporation — RD10-6-000
RD09-7-002
(not consolidated)

ORDER ON VERSION 2 AND VERSION 3 VIOLATION RISK FACTORS AND VIOLATION SEVERITY LEVELS FOR CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

(Issue January 20, 2011)

1. On December 18, 2009, the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted proposed Violation Risk Factors (VRF) and Violation Severity Levels (VSL) to address the Version 2 Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-2 through CIP-009-2, which were approved by the Commission in September 2009.[1] The Commission's September 2009 Order required a compliance filing containing further modifications to the CIP Reliability Standards. On December 29, 2009, NERC responded with proposed Version 3 CIP Reliability Standards and conforming VRFs and VSLs to accommodate revisions made by the proposed Version 3 CIP Reliability Standards, approved separately by the Commission on March 31, 2010.[2] In this order, we approve the proposed Version 2 and Version 3 VRFs and VSLs, subject to modifications discussed in the body of this order.

I. Background

2. NERC and the Regional Entities use VRFs and VSLs to determine penalties for individual violations of Requirements of a Reliability Standard. A VRF is a pre-violation assessment of the potential risk to the reliability of the Bulk-Power System that violation

[1] *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291 (September 2009 Order), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009).

[2] *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010) (March 31 Order).

of a given Reliability Standard Requirement presents ("lower," "medium," or "high"). A VSL is a post-violation measurement of the degree to which a Reliability Standard Requirement was violated ("lower," "moderate," "high," or "severe"). To establish a Base Penalty range for a violation, NERC considers the Commission-approved VSL, together with the VRF approved for the Requirement that is violated.

3. In Order No. 706, the Commission approved the Version 1 CIP Reliability Standards, determining that the proposed Standards were just, reasonable, not unduly discriminatory or preferential, and in the public interest.[3] The Commission further approved 162 VRFs for the Version 1 CIP Reliability Standards. In addition, the Commission directed NERC to revise 43 of those VRFs and to submit proposals for nine CIP Reliability Standard Requirements, which were missing proposed VRFs in the original filing. The Commission also directed NERC to file VSLs for the Version 1 CIP Reliability Standards before the date by which entities were to be subject to compliance audits for them. According to the associated implementation plan, July 1, 2009 was the earliest date any entities were scheduled to reach that milestone.

4. On May 22, 2009, NERC filed the Version 2 CIP Reliability Standards in partial compliance with Order No. 706. NERC stated that the Version 2 filing represented the result of Phase 1 of its overall plan for revising the CIP Reliability Standards to comply with Order No. 706, and that subsequent phases will address the remainder of the Commission's directives in Order No. 706. NERC also stated that it would file revised VRFs and VSLs corresponding to these Version 2 CIP Reliability Standards on or before December 31, 2009.

5. The Commission completed its review and approval of the Version 1 VRFs, which covered a total of 171 Version 1 CIP Requirements, through three orders issued in 2009 on compliance filings.[4] Analyzing the proposed VRFs, the Commission applied its previously established VRF Guidelines: (1) consistency with the conclusions of the Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and

---

[3] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229, *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 126 FERC ¶ 61,065 (2009); Delegated Letter Order, Docket Nos. RM06-22-002, RM06-22-003 (Feb. 2, 2009); Delegated Letter Order, Docket No. RM06-22-009 (Aug. 20, 2009).

Recommendations;[5] (2) consistency within a Reliability Standard; (3) consistency among Reliability Standards; (4) consistency with NERC's definition of the VRF level; and (5) treatment of Requirements that co-mingle more than one obligation.[6]

6. On March 18, 2010, the Commission approved Version 1 VSLs for the Version 1 CIP Reliability Standards, as submitted by NERC and modified by the Commission.[7] The Commission relied on several previously established guidelines for determining appropriate VSLs: VSLs (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.[8] The Commission also set forth two new guidelines for use in the cyber security context :

> (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; and
>
> (2) Violation Severity Levels for cyber security Requirements containing interdependent tasks of documentation and implementation should account for their interdependence.[9]

7. These two additional guidelines (CIP Guidelines) were also considered in our determinations below.

---

[5] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004) (Final Blackout Report), *available at* http://www.ferc.gov/industries/electric/indus-act/blackout.asp.

[6] *North American Electric Reliability Corp.*, 119 FERC ¶ 61,145, at P 16, *order on reh'g*, 120 FERC ¶ 61,145 (2007).

[7] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 130 FERC ¶ 61,211 (CIP VSL Order), *reh'g denied*, 133 FERC ¶ 61,237 (2010). The Commission approved NERC's compliance filing by delegated letter order on September 8, 2010.

[8] *North American Electric Reliability Corp.*, 123 FERC ¶ 61,284 at P 17 (2008).

[9] CIP VSL Order, 130 FERC ¶ 61,211 at P 14.

II. NERC Filings

A. Version 2 CIP VRFs and VSLs, Docket No. RD10-6-000

8. On December 18, 2009, NERC submitted proposed VRFs and VSLs (Version 2 Filing) to address the eight Version 2 CIP Reliability Standards that were approved by the Commission's September 2009 Order (i.e., CIP-002-2 through CIP-009-2). In its filing, NERC proposed revisions to the VRFs for CIP-003-2 and CIP-006-2 associated with the requirements that were changed when converting the Version 1 CIP Reliability Standards into Version 2. The filing also included Version 2 VSLs for 36 Requirements in the Version 2 CIP Reliability Standards. NERC clarified that VRFs assess the impact on reliability of violating a single compliance requirement, while VSLs define the degree to which compliance with a Reliability Standard Requirement was not achieved. Consistent with the NERC Sanction Guidelines, NERC reiterated that VSLs are considered in conjunction with VRFs to determine the possible base penalty range for a violation of a Reliability Standard Requirement. NERC stated that Requirements that were not changed in the transition to the Version 2 CIP Reliability Standards carry forward the Version 1 VRFs and VSLs for those Requirements. NERC further requested that the Commission approve the proposed VRFs and VSLs to be effective upon issuance of this order.

B. Version 3 CIP VRFs and VSLs, Docket No. RD09-7-002

9. On December 29, 2009, in Docket No. RD09-7-002, NERC submitted a compliance filing that proposed changes to CIP-002-2 through CIP-009-2 pursuant to the Commission's directives in the September 2009 Order. NERC explained that, while the filing proposes modifications to two CIP Reliability Standards, NERC submitted a full set of CIP Reliability Standards, CIP-002-3 through CIP-009-3, as the Version 3 CIP Reliability Standards for ease of reference and to simplify the applicable entities' understanding of the appropriate implementation dates. The Version 3 CIP Reliability Standards proposed by this Version 3 filing were approved by the Commission in its March 31 Order.

10. Along with the Version 3 CIP Reliability Standards, NERC also filed conforming changes to the VRFs and VSLs to accommodate revisions made by the Version 3 CIP Reliability Standards. For those Requirements not modified by its Version 3 filing, NERC requested that the Commission carry forward the Version 2 VRFs and VSLs to apply to the Version 3 Requirements. NERC requested that the Commission approve the associated changes to VRFs and VSLs included in its Version 3 Filing, along with the proposed Version 3 Reliability Standards.

III. Notice and Responsive Pleadings

11. Notice of NERC's December 18, 2009 filing in Docket No. RD10-6-000 was published in the *Federal Register*, 75 Fed. Reg. 358 (Jan. 5, 2010). The City of Santa Clara, California, d/b/a Silicon Valley Power (City of Santa Clara) filed a timely motion to intervene and comments. Further, notice of NERC's December 29, 2009 filing in Docket No. RD09-7-002 was published in the *Federal Register*, 75 Fed. Reg. 1766 (Jan. 13, 2010). Edison Electric Institute and American Public Power Association filed timely motions to intervene.

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 (2010), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

B. Violation Risk Factors

1. Version 2

NERC Proposal

13. In its Version 2 filing, NERC proposed for review and approval 26 VRFs for Requirements selected across CIP-003-2 and CIP-006-2. Because many of the Version 2 CIP Requirements are revised from Version 1 in ways that are clerical in nature, such as correlating the VRFs to the revised numbering of Requirements, most do not require a further adjustment to the VRF value. However, one of NERC's proposed VRFs lowers the VRF in CIP-003-2 Requirement R2 from "medium" to "lower."

Commission Determination

14. The Commission approves NERC's proposed VRF designations for the Version 2 CIP Reliability Standards, subject to one modification discussed below. Contrary to NERC's request that we make these VRF designations effective upon issuance of this order, for ease of administration and enforcement, we are making them effective April 1, 2010, the date the Version 2 CIP Reliability Standards became effective. Further, we agree with NERC that the remaining Requirements carry forward their respective Version 1 VRFs. We find that the proposed VRFs are consistent with our guidelines as established in prior VRF orders.

15. However, we reject NERC's modification to the VRF for CIP-003-2 Requirement R2. CIP-003-2 specifically imposes the requirement that there be a single senior manager responsible for implementation of, and compliance with, the CIP Reliability Standards.

NERC changed the VRF associated with this Requirement R2 from "medium" to "lower" without an explanation or justification. As the change in the Reliability Standard CIP-003 Requirement 2 from Version 1 to Version 2 was only a clarification, it does not warrant a reduction of the approved VRF without justification.[10] Guideline 1 requires consistency with the conclusions of the Final Blackout Report, particularly recommendation number 43 to "[e]stablish clear authority for physical and cyber security." This recommendation highlights the need to have a single individual ultimately responsible for creation and implementation of policy. Therefore, the Commission directs the ERO to submit a compliance filing, within 60 days of this order, re-assigning a "medium" designation to this particular VRF, or provide a justification for the reassignment.[11]

2. Version 3

NERC Proposal

16. In its Version 3 Compliance Filing, NERC proposes eight VRFs for Requirements that were modified in the transition from Version 2 to Version 3 CIP Reliability Standards. Five of the VRFs address Requirements which were modified in ways that were either clerical in nature or otherwise did not necessitate an adjustment to the VRF value. The remaining three VRFs apply to CIP-006-3 Requirement R1.6, substantively modified from its Version 2 counterpart, and two newly created sub-parts, Requirements R1.6.1 and R1.6.2; each are assigned a "medium" VRF designation.

Commission Determination

17. The Commission finds that NERC's proposed VRFs for the Version 3 CIP Reliability Standards are consistent with the Commission's previously established guidelines for review of proposed VRFs. We therefore grant NERC's request and approve the proposed Version 3 VRFs. For ease of administration and enforcement, the proposed VRFs for the Version 3 CIP Reliability Standards shall become effective on

---

[10] Version 2 of CIP-003-002 Requirement 2 differs from Version 1 as follows: "Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2." (emphasis added).

[11] The Commission also notes that, in its exhibit proposing Version 2 VRFs for approval, NERC displays incorrect text for Reliability Standard CIP-003-2 Requirement R2. We therefore also direct the ERO to correct such inconsistencies in the compliance filing required by this order.

October 1, 2010, the date the Version 3 CIP Reliability Standards become effective. We also grant NERC's request to carry forward the Version 2 VRFs to the Version 3 Requirements for the remaining Requirements.

C. Violation Severity Levels

1. Version 2

NERC Proposal

18. In its filing, NERC submitted 36 sets of VSLs and explained that in proposing the Version 2 VSLs, it considered the Commission's guidelines for developing VSLs. NERC also states that, for consistency, it compared proposed VSL assignments for Version 2 to those offered for similar requirements in Version 1. NERC explains that it developed the Version 2 VSLs before it submitted its informational filing describing its revised method of assigning VSLs only to main requirements and not to sub-requirements. Therefore, NERC explained that it continued to assign a set of VSLs to each requirement and each sub-requirement that has an assigned VRF, with minor exceptions.

Comments

19. The City of Santa Clara proposes changes to the VSL assignments of two requirements: CIP-003-2 Requirement R2.1 and CIP-006-002 Requirement R3. For CIP-003-2 Requirement R2.1,[12] the City of Santa Clara argues that if the identification is missing for a single element (name, title, or date of designation), it should be assigned a "moderate" VSL rather than a "high" VSL. Additionally, if the identification is missing more than one element, but has a designation, it should be assigned a "high" VSL rather than a "severe" VSL. The City of Santa Clara states that, for example, if the identified person retires, a new person is installed with the same title and the registered entity failed to make the change, then one of the three elements is incorrect (name of the designee). However, there is a designated person and the date of designation is set forth. Therefore, the City of Santa Clara asserts, in such an instance, it would be inappropriate to find a "severe" VSL for that violation.

20. CIP-006-2 Requirement R3 addresses the protection of electronic access control systems and specifically states that "Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter." For CIP-006-2 Requirement R3, the City of Santa Clara states that there is a range of noncompliant performance that can be measured, and, therefore, gradated VSLs are appropriate. The City of Santa Clara asserts that the VSLs

[12] *See supra* P 15 for a description of CIP-003-2 Requirement R2.

for CIP-006-2 Requirement R3 should include lower steps for lesser offenses. It argues that gradation between lower, moderate, high, and severe should be incremented by the percentage of assets residing within a Physical Security Perimeter.

Commission Determination

21. The Commission approves the Version 2 VSLs subject to the modifications discussed below. Contrary to NERC's request that we make these VSL designations effective upon issuance of this order, for ease of administration and enforcement, we are making them effective April 1, 2010, the date the Version 2 CIP Reliability Standards became effective. Further, we agree with NERC that the remaining Requirements carry forward their respective Version 1 VSLs. Additionally, as discussed below, the Commission directs the ERO to file modifications to 27 of the VSLs in the Version 2 filing, within 60 days of the issuance of this order. For ease of reference, the modifications directed by the Commission are shown in Appendix 1 in track changes format.

22. The Commission applied its prior VSL Guidelines and the new CIP VSL Guidelines in making its determinations on NERC's proposed Version 2 CIP VSLs. As discussed above, in the CIP VSL Order, the Commission established two CIP Guidelines. CIP Guideline 1 addressed the "weakest link" characteristic, which states that a binary VSL should be applied to Requirements under which a single lapse in protection can compromise computer network security. CIP Guideline 2 addressed cyber security Requirements that contain interdependent tasks.[13] Six of the Requirements addressed by the Version 2 Filing contain identical language or materially similar provisions as the corresponding Version 1 Requirements for which the Commission directed changes to the Version 1 VSLs on the basis of the new CIP Guideline 1.[14] Additionally, nine of the Requirements addressed by the Version 2 Filing contain identical language or materially similar provisions as the corresponding Version 1 Requirements for which the Commission directed changes on the basis of the new CIP Guideline 2.[15] Therefore, we direct corresponding changes to the Version 2 VSLs to conform to the determinations made in the CIP VSL Order, based on CIP Guidelines 1 and 2, for parallel Requirement text. Specifically, we direct modifications as follows: (1) based on CIP Guideline 1, we direct modifications to CIP-004-2 Requirement R2.1, CIP-005-2 Requirement R1.5, and CIP-006-2 Requirements R1.2, R1.5, R2, and R8; and (2) based on CIP Guideline 2, we direct modifications to CIP-004-2 Requirements R1 and R2, CIP-005-2 Requirement

[13] CIP VSL Order, 130 FERC ¶ 61,211 at P 14.

[14] *Id*. P 15-19.

[15] *Id.* P 20-23.

R2.3, CIP-006-2 Requirements R1.1, R4, R5, and R6; and CIP-007-2 Requirements R2 and R3.

23. Next, in the CIP VSL Order, the Commission directed modifications to some Version 1 VSLs based on the Commission's VSL Guideline 2(b). For the 14 identical or parallel Version 2 Requirements addressed in the Version 2 Filing, we likewise direct changes to the corresponding VSL submissions to remove ambiguity and improve consistency.[16] Specifically, we direct modification to CIP-003-2 Requirements R2.1 and R3.2; CIP-004-2 Requirement R3; CIP-006-2 Requirements R1.7, R4, R6, and R7; CIP-007-2 Requirement R2, R2.3, R3, R3.2, R7, and R9; and CIP-008-2 Requirement R1. In addition, CIP-006-2 Requirement R3 contains an entirely new provision to which VSL Guideline 2(b) applies. NERC proposed a binary (therefore severe) VSL when a cyber asset that is used in access control or monitoring of an electronic security perimeter fails to reside in an identified physical security perimeter, as the new R3 requires. The Commission's VSL Guideline 2(b) provides that, to better ensure consistency and uniformity in the determination of penalties, Violation Severity levels assignments should not contain ambiguous language.[17] For clarity, under VSL Guideline 2(b), we direct a modification of the VSL to directly track the language of the new R3, as illustrated in Appendix 1.

24. Additionally, the CIP VSL Order addressed gradation of VSLs based on the timeliness of compliance for deadline-driven Requirements, and directed modifications to several Version 1 VSLs based on this VSL gradation discussion.[18] Here, Version 2 CIP-009-2 Requirement R3 proposes the same characteristic: gradation according to the length of time in which an entity is not compliant.[19] Again, our determination is that the magnitude of non-compliance allowed by NERC's proposed gradations for this requirement before reaching the "severe" level, in light of the lack of applicable historical compliance data that proves otherwise, leads us to conclude that the proposed Violation Severity Level assignments for CIP-009-2 Requirement R3 would condone a greater level of non-compliance than is appropriate.[20] Therefore, we direct modifications to CIP-009-2 Requirement R3 based on the same rationale, as illustrated in Appendix 1.

---

[16] *See Id*. P 28-33.

[17] *Id*. P 28.

[18] *Id*. P 24-27.

[19] *Id*. P 24.

[20] *Id*. P 27.

25. Further, the Commission identified five requirements in the Version 2 filing that should be revised to be consistent with new and prior Commission VSL guidelines but which were not revised by the CIP VSL Order. The Commission directs the modification illustrated in Appendix 1, on the basis of the guidelines noted. Specifically, addressing the topics of essential training programs and securing physical boundaries, the following requirements should be modified due to their multiple interdependent parts, in accordance with CIP VSL Guideline 1:[21] CIP-004-2 Requirements R1 and R2, and CIP-006-2 Requirement R1.1. CIP-006-2, Requirement R1.2 contains the "weakest link" characteristic because it addresses the need for all access points on the physical security perimeter to be protected.[22] CIP-007-2, Requirement R9, concerning annual review of system security management documentation, is directed for modification under VSL Guideline 2(b) to replace the term "nor" with "and," consistent with the discussion in the March 18 Order.[23]

26. The Version 2 Filing does not include proposed VSLs for CIP-007-2 Requirements R2.3 and R3.2. To comply with Order No. 706, NERC's Version 2 CIP Reliability Standards removed the "acceptance of risk" language from these two Requirements. However, the same language was not removed from the corresponding VSL language. The Commission directs the ERO to modify the VSLs for these Requirements, as illustrated in Appendix 1. While NERC may propose alternate VSL text in the future, the VSL language for Requirements R2.3 and R3.2 provided in Appendix 1 is approved to be effective on April 1, 2010, along with the other Version 2 VSLs modified and approved by this order, until the Commission approves an alternative proposal.

27. The Commission notes the "Complete Matrix of VSLs for Approved Reliability Standards" submitted by NERC contains only the CIP Reliability Standard Requirements proposed for modification and omits the unchanged Version 1 VSLs, which NERC requests be carried forward. The Commission directs NERC to provide, within 60 days, a complete list of all Version 2 CIP Reliability Standard Requirements, and their associated VSLs and VRFs, as determined or carried forward by this order.

28. The Commission, in response to the City of Santa Clara's comments, notes that the proposed minimum attributes for CIP-003-2 Requirement R2.1 include the name, title and date of designation of the senior manager. The Commission agrees with NERC's decision to require only a limited number of attributes to identify a senior manager and to

---

[21] *Id*. P 20-23.

[22] *Id*. P 15-19.

[23] *Id*. P 28.

then apply a binary VSL, which, as NERC explained, is always assigned as "severe." Partial compliance with the minimum set of attributes in the requirement does not provide any reliability benefit and, therefore, should not be gradated. It should be noted that the "Severe" Base Penalty range is very broad. In the penalty determination phase, the Regional Entity and NERC are accorded discretion in the determination of penalties, including the option to waive a penalty altogether. We believe such discretion is sufficient to address the City of Santa Clara's concern regarding varying levels of compliance.[24]

29. As for the City of Santa Clara's comments regarding CIP-006-2 Requirement R3, the Commission, in light of CIP Guideline 1, agrees with NERC's proposed VSL assignment. The lapse of computer protection can create an opening for malicious activity that has systemic critical infrastructure consequences. Allowing a single Cyber Asset used in the access control or monitoring of the Electronic Security Perimeter(s) to reside outside of an identified Physical Security Perimeter is a severe violation of the Requirement.

2. Version 3

NERC Proposal

30. The Version 3 CIP Reliability Standards contain substantive modifications to two standards. Specifically, NERC inserted provisions for a visitor control program into CIP-006-3 Requirement R1.6, adding new sub-requirements. NERC also removed the last sentence of CIP-008-3 Requirement R1.6. In order to accommodate these and other minor changes to the CIP Reliability Standards, NERC proposes seven sets of VSLs in the Version 3 Filing. However, NERC did not include proposed VSLs for CIP-006-3 Requirements R1.6.1 and R1.6.2, although it designates VRFs for these sub-requirements.

Commission Determination

31. The Commission approves the proposed VSL modifications to the Version 3 CIP Reliability Standards, subject to the modifications discussed in this section. For ease of administration and enforcement, the proposed VSLs for the Version 3 CIP Reliability Standards shall become effective on October 1, 2010, the date the Version 3 CIP Reliability Standards become effective. We also grant NERC's request to carry forward the Version 2 VSLs, as approved in this order, to the Version 3 Requirements for the remaining Requirements. Additionally, as in our Version 2 determination above, the

[24] *See Mandatory Reliability Standards for Critical Infrastructure Protection*, 133 FERC ¶ 61,237 at P 17 (describing the breadth of possible base penalty ranges).

Commission directs NERC to include in its compliance filing a complete list of all Version 3 CIP Reliability Standard Requirements, and their associated VSLs and VRFs, as determined or carried forward by this order. For ease of reference, the modifications directed by the Commission are shown in Appendix 2 in track changes format.

32. With regard to the omitted VSL sets noted above, for the newly created CIP-006-3 Requirements R1.6.1 and R1.6.2, NERC's filing appears to suggest that these new sub-requirements should be addressed by the VSLs proposed for the parent requirement, CIP-006-3 Requirement R1.6. We note that NERC originally assigned a binary VSL to the precursor parent requirement, CIP-006-1 Requirement R1.6, and we agree that this designation continues to be appropriate. The sub-requirements should follow suit because they are minimum components of the parent requirement. Each of the component sub-requirements is necessary to uphold compliance with the parent requirement. Therefore, treating the sub-requirements through the VSLs of the parent requirement is appropriate. The Commission therefore directs the ERO to revise its proposed VSL for CIP-006-3 Requirement R1.6 as shown in Appendix 2, and to add rows containing "N/A" for the new sub-requirements R1.6.1 and R1.6.2, consistent with how NERC has treated similar sub-requirements .

The Commission orders:

(A) NERC's December 18, 2009 filing is hereby approved with certain modifications, effective on April 1, 2010, as discussed in the body of this order. NERC's December 29, 2009 compliance filing is hereby approved with certain modifications, effective on October 1, 2010, as discussed in the body of this order.

(B) NERC is directed to file a compliance filing within 60 days of the date of this order, as discussed in the body of this order.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

APPENDIX 1: Commission Revisions to NERC's Proposed Version 2 CIP VSLs

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-003-2	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOW	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation. ~~The senior manager is not identified by name, title, and date of designation.~~	VSL Guideline 2(b)
CIP-003-2	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOW	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy ~~(pertaining to CIP 002 through CIP 009)~~in R1 but did not include either: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy ~~(pertaining to CIP 002 through CIP 009)~~in R1 but did not include both: 1) an explanation as to why the exception is necessary, and 2) any compensating measures.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-004-2	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	LOW	N/A~~The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices.~~	N/A~~The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~ The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, ~~nor~~or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.	CIP Guideline 2

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-004-2	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOW	N/A~~The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~	N/A~~The Responsibility Entity did not review the training program on an annual basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~ The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, nor~~or~~ document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	CIP Guideline 2
CIP-004-2	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MED	N/A~~At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	N/A~~At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	N/A~~At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	~~15% or more of~~Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were ~~not~~ trained prior to their being granted such access except in specified circumstances such as an emergency.	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-004-2	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 to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.	MED	N/A	The Responsible Entity has a personnel risk assessment program, ~~in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements,~~ 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 after such personnel were granted such access except in specified circumstances such as an emergency.	The Responsible Entity does not have a documented personnel risk assessment program, ~~in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements,~~ 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 except in specified circumstances such as an emergency.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-005-2	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2	MED	N/AA ~~Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but one (1) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3, Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.~~	N/AA ~~Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but two (2) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.~~	N/AA ~~Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but three (3) of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.~~	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) ~~is~~was not ~~afforded~~provided ~~without four (4)~~ one (1) or more of the protective measures as specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.	CIP Guideline 1
CIP-005-2	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MED	N/A	N/A	~~N/A The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.~~	The Responsible Entity did not implement ~~nor~~or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	CIP guideline 2

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R1.1	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MED	N/A	N/A~~Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	N/A~~Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.~~	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed ~~and~~or documented alternative measures to control physical access to ~~the~~such Cyber Assets within the Electronic Security Perimeter.	CIP guideline 2
CIP-006-2	R1.2	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MED	N/A	N/A~~The Responsible Entity's physical security plan includes measures to control entry at access points but does not identify all access points through each Physical Security Perimeter.~~	N/A~~The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.~~	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter ~~nor~~or does not identify measures to control entry at those access points.	CIP guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	MED	N/A	N/A	N/A~~The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with CIP-004-2 Requirement R4.~~	The Responsible Entity's physical security plan does not address the ~~process for~~ reviewing of access authorization requests ~~and~~ or the ~~process for~~ revocation of access authorization, in accordance with CIP-004-2 Requirement R4.	CIP guideline 1
CIP-006-2	R1.7	Update of the physical security plan within thirty calendar days of the completion 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 addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration but the plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.~~	The Responsible Entity's physical security plan does not address ~~a process for~~ updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MED	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but one (1) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.~~	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but two (2) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.~~	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with all but three (3) of the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.~~	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was ~~provided without~~ not afforded ~~four (4) or more of~~ the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.	CIP Guideline 1

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	MED	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) ~~did~~ does not reside within an identified Physical Security Perimeter.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R4.	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: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber	MED	N/A	N/A~~The Responsible Entity has implemented but not documented 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 one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber~~	N/A~~The Responsible Entity has documented but 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 one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.~~	The Responsible Entity has not documented ~~nor~~ 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 one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R5	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-008-2. One or more of the following monitoring methods shall be used: Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MED	N/A	N/A~~The Responsible Entity has implemented but not documented 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 using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	N/A~~The Responsible Entity has documented but not implemented 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 using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	The Responsible Entity has not documented ~~nor~~ or has not implemented 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 using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-2.	CIP guideline 2

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R6	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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	LOW	N/A~~The Responsible Entity has implemented but 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 following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.~~	N/A~~The Responsible Entity has implemented 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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, but has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.~~	N/A~~The Responsible Entity has documented but not implemented 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: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~	The Responsible Entity has not implemented or has notnor 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 following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~.~~ OR The Responsible Entity 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)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-006-2	R7.	R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.	LOW	N/A~~The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.~~	N/A~~The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.~~	N/A~~The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.~~	The responsible entity did not retain physical access logs for at least ninety calendar days.~~The Responsible Entity retained physical access logs for less than 45 calendar days.~~	VSL Guideline 2(b)
CIP-006-2	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MED	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include one of the Requirements R8.1, R8.2, and R8.3.~~	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include two of the Requirements R8.1, R8.2, and R8.3.~~	N/A~~The Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly but the program does not include any of the Requirements R8.1, R8.2, and R8.3.~~	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.	CIP Guideline 1
CIP-007-2	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MED	N/A	N/A~~The Responsible Entity established (implemented) but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	N/A~~The Responsible Entity documented but did not establish (implement) a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	The Responsible Entity did not establish (implement) or did not~~nor~~ 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)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-007-2	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	MED	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk ~~exposure or state an acceptance of risk.~~	VSL Guideline 2(b)
CIP-007-2	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement 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~~The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, a security patch management program but did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	N/A~~The Responsible Entity established (implemented) but did not document, either separately or as a component of the documented configuration management process specified in CIP-003-2 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).~~	N/A~~The Responsible Entity documented but did not establish (implement), either separately or as a component of the documented configuration management process specified in CIP-003-2 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).~~	The Responsible Entity did not establish (implement) or did not~~nor~~ document, either separately or as a component of the documented configuration management process specified in CIP-003-2 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 Perimeters(s).	CIP Guideline 2 VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-007-2	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	LOW	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk ~~exposure or an acceptance of risk.~~	VSL Guideline 2(b)

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

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-007-2	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOW	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-2 at least annually ~~nor~~ and~~were~~ changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.	VSL Guideline 2 (b)
CIP-008-2	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOW	N/A	N/A~~The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.~~	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 those components~~the plan does not address one or more of the subrequirements R1.1 through R1.6~~.	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.	VSL Guideline 2(b)

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL	Guideline
CIP-009-2	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 thirty calendar days of the change being completed.	LOW	N/A~~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 communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than30 but less than or equal to 120 calendar days of the change.~~	N/A~~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 communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.~~	N/A~~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 communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.~~	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 ~~more than 180~~ thirty calendar days of the change.	VSL Guideline 1

APPENDIX 2: Commission Revisions to NERC's Proposed Version 3 CIP VSLs

Standard	Reqt.	Requirement Language	VRF	Lower VSL	Moderate VSL	High VSL	Severe	Guideline
CIP–006-3	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM	~~N/A The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~	~~N/A The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~	~~N/A The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.~~	The Responsible Entity did not include or implement a visitor control program in its physical security plan or it does not meet the requirements of continuous escort.	CIP Guideline 2
CIP–006-3	R1.6.1	Visitor logs (manual or automated) to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of personnel with authorized, unescorted physical access performing the escort.	MEDIUM	N/A	N/A	N/A	N/A	
CIP–006-3	R1.6.2	Requirement for continuous escorted access within the Physical Security Perimeter of visitors.	MEDIUM	N/A	N/A	N/A	N/A	