133 FERC ¶ 61,237
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.

Mandatory Reliability Standards for Critical Infrastructure Protection — Docket No. RM06-22-012

ORDER ON REHEARING

(Issued December 16, 2010)

1. In this Order, the Commission denies a request for rehearing of the Commission's order addressing violation severity level assignments for critical infrastructure protection (CIP) reliability standards, issued March 18, 2010.[1]

I. Background

A. Violation Severity Levels

2. The North American Electric Reliability Corporation (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 Standard Requirement was violated (i.e., "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 June 2008, the

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 130 FERC ¶ 61,211 (2010) (March 18 Order).

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

Commission approved Violation Severity Levels corresponding to the Requirements and sub-Requirements of 83 Reliability Standards. It should be noted that the CIP Reliability Standards were not included among the approved standards.[3] In addition, the Commission directed NERC to submit a compliance filing and several reports. The Commission developed four guidelines to evaluate 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]

B. Order No. 706

4. 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; and 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.

5. In Order No. 706, issued on January 18, 2008, the Commission approved the eight Version 1 CIP Reliability Standards.[5] In addition, pursuant to section 215(d)(5) of the Federal Power Act (FPA),[6] the Commission directed NERC to develop modifications to address specific issues. NERC's submission of the eight CIP Reliability Standards did

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

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

[5] *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).

[6] 16 U.S.C. § 824o(d)(5) (2006).

not include Violation Severity Level assignments. Therefore, the Commission also directed NERC to file Violation Severity Levels before July 1, 2009.[7]

C. Compliance Filing

6. In response to Order No. 706, on June 30, 2009, NERC submitted a compliance filing. NERC's filing proposed 118 sets of Violation Severity Levels corresponding to 171 Requirements and sub-Requirements contained in the Version 1 CIP Reliability Standards. In its March 18 Order, the Commission noted that, in prior orders, it had retained the flexibility to consider the development of additional guidelines as appropriate, and determined that, in the context of the cyber security Requirements of the CIP Reliability Standards, additional guidelines are appropriate.[8] Exercising that flexibility, the Commission accepted NERC's proposed Violation Severity Level assignments, with modification, and established two additional guidelines for determining appropriate Violation Severity Levels specifically for cyber security Requirements:

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]

Applying the new and existing guidelines for analyzing Violation Severity Levels, the Commission directed NERC to submit a compliance filing modifying 57 sets of Violation Severity Level assignments.

---

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

[8] March 18 Order, 130 FERC ¶ 61,211 at P 14.

[9] *Id*. The Commission also explained that "gradation" means "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.' *Id.* n.11 (citations omitted).

II. Rehearing Request

7. On April 19, 2010, the American Public Power Association, Edison Electric Institute, and the National Rural Electric Cooperative Association (collectively, Joint Trade Associations) jointly filed a request for rehearing of the Commission's March 18 Order. They state that although they generally support the principles reflected in the CIP Violation Severity Level Guidelines, they are concerned that certain of the ordered modifications to the Violation Severity Level assignments are inappropriate. Joint Trade Associations request that the Commission grant rehearing and reinstate the gradation approach for certain Violation Severity Level assignments. Further, Joint Trade Associations ask the Commission to recognize and reflect that, contrary to CIP Violation Severity Level Guideline 2, the successful electronic implementation of electronic-access controls does not necessarily depend on the documentation of such controls. Joint Trade Associations also contend that rehearing of the Order is also appropriate so as to extend the 60-day compliance filing deadline so that NERC and other industry stakeholders can consider the new CIP Violation Severity Level Guidelines.

A. CIP Violation Severity Level Guidelines

8. The Joint Trade Associations take issue with the Commission's statement in the March 18 Order that the control systems that support reliability are only as secure as their weakest links. The Joint Trade Associations rebut the Commission's justification for CIP Violation Severity Level Guideline No. 1 by disputing the example Requirements discussed by the Commission. According to the Joint Trade Associations, the application of the new CIP Violation Severity Level Guideline No. 1 and the resulting modifications applicable to Reliability Standards CIP-005-1, Requirement 4 and CIP-005-1, Requirement 3.2 are inappropriate because they produce the anomalous result whereby an entity that monitors and assesses the vulnerability of 99 percent of its electronic access points will be treated the same as an entity that assesses the vulnerability of a significantly smaller percentage (or none) of such points. Additionally, the Joint Trade Associations state that this result conflicts with the Commission's Violation Severity Level Guideline No. 1,[10] arguing that it could cause an entity that knows it will not be able to perform vulnerability assessments for all of its electronic access points to simply not perform any additional vulnerability assessments. Joint Trade Associations believe this could occur because in either case the entity will be treated as having performed none. The Joint Trade Associations conclude that the Commission's determinations and directives in accordance with the CIP Violation Severity Level Guideline No. 1, in the March 18 Order, fail to consider or discuss anomalous results that a binary Violation

[10] The Commission's Violation Severity Level Guideline No. 1 states that a Violation Severity Level should not have the unintended consequence of lowering the current level of compliance.

Severity Level assignment potentially could produce for certain CIP Standard Requirements.

9. The Joint Trade Associations argue that the Commission's decision to assign binary Violation Severity Levels that contain "weakest link" characteristics does not give adequate recognition to numerous other administrative and technical controls that are associated with electronic access points, electronic security perimeters, and critical cyber assets. The Joint Trade Associations assert that a binary Violation Severity Level assignment in these instances ignores the "layered" nature of physical and cyber security boundaries by pre-determining that a single, unmonitored access point constitutes a guaranteed means of ingress for a would-be cyber-intruder. However, according to the Joint Trade Associations, there likely are multiple monitored and controlled access points beyond the unmonitored one that would need to be traversed in order to breach the security perimeter.

10. Additionally, the Joint Trade Associations contend that the Commission's determinations and directives in accordance with the CIP Violation Severity Level Guideline No. 1 are arbitrary and capricious because they fail to consider or discuss the anomalous results that a binary Violation Severity Level assignment potentially could produce for certain of the CIP Standards' requirements. Further, the Joint Trade Associations argue that the determinations in the March 18 Order are counter to the record evidence in this proceeding as set forth in the "Record Development of Proposed CIP Version 1 Reliability Standard Violation Severity Levels" that NERC submitted as Exhibit B in its June 30, 2009 CIP Violation Severity Level filing, which found a gradated approach to be the best way to accurately measure the severity of a CIP Standard violation. The Joint Trade Associations also argue that the CIP Violation Severity Level Guideline No. 1 constitutes an unexplained and irrational departure from the Commission's prior policy, in which the Commission indicated a preference for the assignment of Violation Severity Levels in multiple levels rather than under a binary approach.

11. The Joint Trade Associations argue that the underlying reason for CIP Violation Severity Level Guideline No. 2 is illogical because it ignores that implementation of the CIP Standards' Requirements can be achieved without documentation. Therefore, according to the Joint Trade Associations, the two interdependent tasks, implementation and documentation, often require different Violation Severity Level assignments. The Joint Trade Associations contend that CIP Violation Severity Level Guideline No. 2 is arbitrary and capricious because, as long as an entity can verify that a particular CIP Standard Requirement has been implemented, documentation is not vital to ensuring that the applicable Critical Cyber Assets have been protected. The Joint Trade Associations

cite CIP-007 Requirement R2.2[11] as an example to argue that failure to fully document detailed steps and results is not the equivalent of failing to actually perform the required actions. Additionally, the Joint Trade Associations state that CIP Violation Severity Level Guideline No. 2 ignores the fact that a lack of documentation is often the result of human error or omission, which can be difficult to prevent even with a strong compliance program.

B. Reliability Standards Development Procedures

12. The Joint Trade Associations state that the Violation Severity Level assignments submitted by NERC in the June 30, 2009 CIP Violation Severity Level filing were developed in accordance with the NERC Reliability Standards Development Procedures, are based on the cumulative cyber security and information technology expertise of the NERC Cyber Violation Severity Level drafting team, and reflect the consideration of NERC's Violation Severity Level development guidelines and criteria. On this premise, the Joint Trade Associations argue that NERC should be permitted to address the Commission's concerns regarding the 57 CIP Violation Severity Level assignments pursuant to these same procedures rather than being required to perform each of the ordered modifications without the opportunity to conduct a deliberative and open process conducted with the input of NERC's drafting team, and other industry stakeholders.

13. The Joint Trade Associations thus argue that certain of the ordered modifications to the CIP Violation Severity Level assignments do not reflect reasoned decision-making and, therefore, are arbitrary and capricious. Additionally, the Joint Trade Associations state that allowing NERC to revise the CIP Violation Severity Level assignments pursuant to its Reliability Standards Development Procedures would be consistent with section 215 of the FPA[12] because it requires that the Commission-certified Electric Reliability Organization (ERO) have procedures that provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing Reliability Standards and otherwise exercising its duties.

III. Discussion

14. In the March 18 Order, the Commission stated that our determinations were made in consideration of the Violation Severity Level Guidelines set forth in the Violation

[11] CIP-007 Requirement R2.2 addresses disabling ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeters.

[12] 16 U.S.C. § 824o (2006).

Severity Level Order.[13] The Commission further determined 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. Key among these characteristics are that new and increasing network interconnectivity in the electric industry introduces ever-changing opportunities for cyber attacks that can affect numerous entities across a wide area simultaneously – on a nearly instantaneous basis. In contrast to operations and planning tasks, where the bulk power system is designed to withstand loss of any single element, cyber security decreases when any one portal is left open. An analogy in the physical world would be to leave one hatch on a submarine open while closing the all other hatches and then submerging for a dive. As the Commission has previously explained,[14] unlike transmission planning, an N-minus-one criterion is not an appropriate risk-based assessment methodology for determining which assets need cyber protections because a cyber attack can strike multiple assets simultaneously and cause damage to those assets for such a time period that other asset outages may occur before the damaged asset can be returned to service. If an adversary can gain electronic access to a computer system, he may be able to gain control over that system and use it for his purposes, perhaps directing or even damaging physical assets. For that reason, there is little value in partial compliance for some types of cyber security requirements, and a binary VSL is appropriate. Therefore, the Commission developed two additional guidelines for analyzing the validity of Violation Severity Levels that specifically pertain to cyber security.

15. In the four years that have passed since the ERO filed the Version 1 CIP Reliability Standards, new cyber security threats and vulnerabilities have become apparent and public awareness has grown. Therefore, the CIP-specific guidance the Commission established in our March 18 Order is necessary and important at this juncture to ensure that any baseline strategies already employed across subject entities are not inadvertently relaxed by Violation Severity Levels that accept compliance at lower levels than precursor practices. Further, the fact that each cyber security standard, and many Requirements within them, must interact *together* with others to accomplish any baseline security, elevates the importance of the new guidelines in order to assure that each is reviewed in relation to its role in supporting the facility's cyber security posture.

A. CIP Violation Severity Level Guideline No. 1

16. The Commission reiterates that a single lapse of computer protection can create the opening for malicious activity that has systemic critical infrastructure consequences,[15]

[13] *Id.*

[14] Order No. 706, 122 FERC ¶ 61,040 at P 256.

[15] March 18 Order, 130 FERC ¶ 61,211 at P 15.

and rejects the Joint Trade Associations' arguments against CIP Violation Severity Level Guideline No. 1. CIP Violation Severity Level Guideline No. 1 reflects the Commission's finding that if just one access point to the electronic security perimeter does not have monitoring processes implemented, it presents an opportunity for undetected and unauthorized access to a critical cyber asset. Vulnerability assessments, along with mechanisms to detect and alert for attempted or actual unauthorized accesses, are some of the tools that must be in place and functioning.

17. The Commission disagrees with the Joint Trade Associations' assertion that CIP Violation Severity Level Guideline No. 1 will (a) produce the anomalous result of treating two entities the same for varying degrees of non-compliance, and (b) thereby lower the current level of compliance by encouraging non-performance of required actions. Compliance will not be deterred in this manner because the current compliance and enforcement structure allows ample discretion in application of penalties. The Sanction Guidelines provide for this discretion by outlining a series of factors that must be considered to tailor the penalty amount to the specific circumstances at issue – after the Violation Severity Levels are used to point to an initial value range of the base penalty amount.[16] Each of the twelve possible base penalty ranges are extremely broad. Each of the three "Severe" penalty ranges available to a binary Violation Severity Level, varying with the associated Violation Risk Factor, are so broad as to encourage an entity to comply. A "Medium" Violation Risk Factor is designated for each of the examples offered by the Joint Trade Associations, i.e., Requirements R3.2 and R4 of CIP-005-1.[17] Therefore, the application of the Severe base penalty amount, in accordance with the binary approach directed by this guideline, can range anywhere between $10,000 and

[16] *See* NERC Rules of Procedure, Appendix 4B, Sanction Guidelines of the North American Electric Reliability Corporation, section 4, Determination of Monetary Penalties, including the following steps: 4.1 Initial Value Range of the Base Penalty Amount (the range found at the intersection of the VRF and VSL on the Base Penalty Amount Table), 4.2 Setting of the Base Penalty Amount (at the lowest value in the range if two criteria apply), 4.3 Application of Adjustment Factors (mandatory application of eight factors to the circumstances at hand), 4.4 Setting of the Final Penalty Amount (subject to availability to pay, upon request).

[17] In summary, CIP-005 Requirement 3.2 requires the Responsible Entity to detect and communicate any attempted or actual unauthorized access in conjunction with appropriate notification or logging. CIP-005 R4 requires annual vulnerability assessments of electronic access points to the Electronic Security Perimeter(s).

$335,000 per violation of either Requirement. [18] In fact, all of the standards at issue in this proceeding have "Lower" and "Medium" Violation Risk Factors. The Severe base penalty amount for the Requirements with "Lower" Violation Risk Factors is $5,000 to $25,000. This broad penalty range, combined with the further discretion afforded by the Sanction Guidelines, is sufficient to avoid the "anomalous result" and "unintended consequences" discussed by the Joint Trade Associations.

18. In addition, the Violation Severity Levels are intended to be clear, preliminary "bright line" markers to establish, in rather mechanical fashion with the Violation Risk Factor, the appropriate parameters of the initial base penalty range for a given violation.[19] The design of a Violation Severity Level is not intended to measure the strength of a responsible entity's compliance program, with respect to the associated Requirement. Rather, the strength of an entity's compliance program may become a mitigating factor for enforcement authorities to consider when evaluating the specific circumstances surrounding the violation in order to determine a specific penalty within or below the initial base penalty range established by the Violation Severity Level and Violation Risk Factor, according to the discretion afforded by NERC's Sanction Guidelines.

19. The proposed use of percentage analysis to gradate eleven of these Requirements adds to our concern for their weakest link characteristics.[20] First, baseline individual protocols are at issue in these Requirements, which must map to or interact with other elements of a security program in a holistic manner if a security culture is to be achieved. Further, on a practical basis, the use of percentage analysis to assess the degree of compliance with these Requirements introduces new burdens of counting, calculating and auditing quantities – creating new opportunities for dispute while providing no recognizable benefit to improving reliability. In the examples used by the Joint Trade Association, it could take an inordinate effort to count and track numbers of access

[18] In total, for violations of the 171 CIP Version 1 Requirements, the penalty ranges top out as follows: 100 Requirements are capped at $25,000; 69 Requirements are capped at $335,000; and two Requirements are eligible for the full penalty amount of $1 million. The initial floor of the range for a given Requirement in any of these groupings varies with the gradation status of the respective VSL for each Requirement. The Sanction Guidelines provide direction for when the penalty should be reduced to the floor of the range or less, including the possibility of a zero penalty.

[19] *See* NERC Rules of Procedure, Appendix 4B, Sanction Guidelines of the North American Electric Reliability Corporation, section 4.

[20] The eleven Requirements subject to CIP VSL Guideline 1 that NERC proposed to gradate by percentage non-compliance are: CIP-004-1, R2.1; CIP-005-1, R3, R3.1, R4 and R5.2; and CIP-007-1, R2.1, R2.2, R4, R5.1.1, R6 and R8.

points, perhaps variable within a period, and generate documentation efforts that may otherwise be unnecessary. In the end, such efforts still would not indicate the comparability across entities that the Joint Trade Associations seek because the percentage of compliance with a given Requirement does not necessarily correlate proportionately to the quality of security achieved, or to the impact on reliability. The Commission maintains its position that 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. In the context of cyber security, severity of non-compliance is in many instances better addressed by a binary Violation Severity Level, as opposed to a gradated approach.[21]

20. In the context of their CIP-005-1 examples, the Joint Trade Associations discuss the layered nature of physical or cyber security boundaries. They argue that there are multiple monitored and controlled access points beyond an unmonitored access point, and numerous other administrative and technical controls may be associated with those layers that would need to be traversed to breach the security perimeter. The Commission agrees that such a layered approach would be more resilient to attacks than one that is only protected by a single boundary. We acknowledge that it is not necessary that all access controls be present on a single device or at each layer of security but that only through a combination of layered defense can all access points to the security perimeter be reliably protected. The approach described by the Joint Trade Associations is commonly known as defense in depth, and this is a best practice that has long been embraced by the Commission. For example, in Order No. 706, the Commission directed modifications to incorporate the defense in depth approach to the protection of physical and electronic security perimeters.[22]

21. Reliability Standard CIP-005-1 seeks to protect all Critical Cyber Assets within an identified Electronic Security Perimeter, as well as all access points on the perimeter. Regardless of whether a defense in depth strategy is implemented, Requirements R3.2 and R4, in particular, seek to protect against the penetration of the electronic security perimeter. To accomplish this protection, all access points must be known, unneeded ports and services disabled, and monitoring processes engaged to detect and alert for unauthorized access. In the cyber security realm, leaving one electronic access point unsecured while securing all others still leaves an entity open to attack. The vulnerability is independent of the number of unsecure access points. Further, the implementation of this standard establishes a baseline against which all later comparison and change to the Electronic Security Perimeter is measured. Without accurate assessment of the

[21] March 18 Order, 130 FERC ¶ 61,211 at P 15.

[22] Order No. 706, 122 FERC ¶ 61,040 at P 480, 496. NERC has not yet filed those modifications with the Commission.

Electronic Security Perimeter, including proactive discovery of all access points to the perimeter, it is not possible for an entity to conform to the Standard. Therefore, it is appropriate to address Electronic Security Perimeter issues with a binary Violation Severity Level designation for the purposes of establishing the initial base penalty range.

22. However, it is important to distinguish that the Joint Trade Associations are speaking to layers of defenses that are in addition to the security perimeter. In Order No. 706, the Commission emphasized that no single perfect defensive measure exists that will guarantee protection of the Bulk-Power System, and that many defensive measures are often dependent on the quality of active human maintenance. Therefore, the Commission found that it is in the public interest to require a responsible entity to implement two or more distinct security measures when constructing an electronic security perimeter.[23] Broadly speaking, the Commission directed the inclusion of defense in depth principles in requirements pertaining to both the electronic and physical security of critical assets. [24] However, NERC has not yet revised its standards to incorporate defense in depth for either electronic or physical security. And since defense in depth architecture is not required in the Commission-approved Version 1 CIP Reliability Standards cited by the Joint Trade Associations, it is not taken into account when determining the Violation Severity Level. Currently, the cyber security reliability standards require protocols in relation to singular physical and cyber security boundaries, and therefore, a binary Violation Severity Level designation is appropriate for purposes of establishing the base penalty range. Following that assessment, with the full scope of the entity's performance in view, the discretion afforded by the Sanction Guidelines can address the mitigating circumstances.[25]

23. We understand that the ERO's stakeholder process produced the proposal now subject to our consideration, and that it employed a gradated approach to measure the severity of a CIP Standard violation. However, the record evidence that the Joint Trade Associations refer to fails to explain why the gradated approach ensures reliability, in light of the vulnerabilities presented by the cyber security environment at issue here, and previously discussed in Order No. 706. Despite the recommendation of the ERO stakeholder process, the Commission finds that the Requirements to which the Joint Trade Associations now refer require unique consideration, and are more appropriately addressed with a binary approach. Our prior-stated preference for a gradated approach was outside of the cyber security context. When the Commission stated that it preferred the gradated approach, it acknowledged that circumstances could arise where we would

[23] *See* Order No. 706, 122 FERC ¶ 61,040 at P 496-497.

[24] *Id.* P 501, P 544 and P 573.

[25] *Id*. P 496.

see fit to develop additional guidelines.[26] The Commission's additional guidelines applicable to the cyber security context employ a binary approach, for reasons explained here and in the March 18 Order.

B. CIP Violation Severity Level Guideline No. 2

24. The Commission disagrees with the Joint Trade Associations' arguments that: (1) the CIP Violation Severity Level Guideline No. 2 is illogical or ignores that the CIP Standards' Requirements can be implemented without documentation; (2) documentation is not vital to ensuring that the applicable Critical Cyber Assets have been protected; and (3) CIP Violation Severity Level Guideline No. 2 ignores the fact that a lack of documentation is often the result of human error or omission.

25. For each of the requirements to which the CIP Violation Severity Level Guideline No. 2 was applied, the requirements called for the documentation and implementation of high level measures such as programs, policies, and procedures. For these particular requirements, these programs, policies, and procedures are necessary to ensure that an organization applies the technical and physical controls in a reliable and repeatable manner. Further, the Commission believes that sufficiency in the documentation of these programs, policies, and procedures serves to prevent some violations, reduce the incidence of others, and promote early detection of human error, all of which enhance cyber security protections and the reliability of the Bulk-Power System.

26. In addition to the documentation that establishes what tasks the programs, policies, and procedures discussed above entail, another category of documentation relates to the need for evidence that those tasks were appropriately completed in order to demonstrate compliance with the CIP standards. The Commission recognizes that, in the cyber security environment, electronic records are often created that are an integral part of performing a required task, such as date-stamped logging associated with various actions. These electronic records, when supplied upon request, may suffice for evidentiary documentation of compliance for regulatory purposes, if they contain sufficient and appropriate details to document that the required action was taken.

27. The Joint Trade Associations use CIP-007 Requirement R2.2 as an example to argue that implementation can and should be separately addressed by gradation when implementation can occur without documentation in the Violation Severity Level phase. Requirement R2.2 requires certain ports and services to be disabled prior to production usage, and it is impossible to demonstrate compliance with this aspect of the requirement without some sort of documentation. They assert that failure to fully document the detailed steps and actions taken to disable other ports and services, prior to production

[26] Violation Severity Level Order, 123 FERC ¶ 61,284 at P 17 n.12.

usage, is not the equivalent of failing to disable the ports and services. The Commission disagrees. In many of these requirements the directed actions require a particular sequence, and without the proper documentation it is difficult to assess if a particular action was taken at the proper time. Therefore, in this particular example, it is not sufficient to show that the appropriate ports and services are disabled at the time of audit or investigation. Rather, date-stamped electronic records or some other kind of evidentiary documentation is necessary to prove that the required action occurred at the proper time.

28. The Joint Trade Associations claim that documentation is not vital to ensuring protection of the applicable Critical Cyber Assets as long as the entity can verify that a particular CIP Standard Requirement has been implemented. To the contrary, the Commission finds that, for these particular standards, documentation is the only method by which to verify implementation.

29. As to the Joint Trade Associations' related argument that it is conceivable to separate implementation from documentation in some Requirements, we do not disagree. However, we do not believe it is appropriate for these particular Requirements in the CIP Reliability Standards. Moreover, we do not believe it is not necessarily appropriate to reflect this distinction through gradation of the Violation Severity Level. The decision to gradate should be made when partial compliance achieves a significant reliability-related value. As discussed previously, the value of partial compliance is reduced due to a number of factors: the complex combination of tasks contained therein, the integral nature of electronic evidentiary documentation often associated with completing such tasks, and the need for consistent repetition of the required programs, policies, and procedures. As explained above in relation to CIP Violation Severity Level Guideline No. 1, the base penalty range associated with binary treatment in NERC's Sanctions Table leaves a wide berth for discretion in determining the amount of a penalty based on the circumstances of a particular violation.

30. Additionally, considering the structure of modern networks, such as the multiple monitored and controlled access points along physical and electronic boundaries mentioned by the Joint Trade Associations, network intricacies clearly present difficulties to maintaining and securing a perimeter. Maintaining documentation of perimeter configurations including ports and services is vital to managing the security of a perimeter. Network configurations change for a variety of reasons, as do the staff supporting those networks. To maintain a clear organizational understanding of why rules are in place and what they accomplish, it is necessary to document the changes that occur. Implementing this line of logic is the essence of CIP-003, Requirement R6, which requires change control and configuration management.

31. We disagree with Joint Trade Associations that because the lack of documentation is often the result of human error or omission and difficult to prevent, these certain Violation Severity Levels should be gradated rather than binary. The Commission

expects responsible entities to employ due care to take appropriate and required actions. And, as noted above, NERC's Sanctions Table leaves a wide berth for discretion in determining the amount of a penalty based on the circumstances of a particular violation.

C. Reliability Standards Development Procedures

32. We disagree with the Joint Trade Associations' assertion that the Commission erred in ordering modifications to the Violation Severity Level assignments without first permitting NERC to modify those assignments through its Reliability Standards Development Procedures. As a result, we deny this portion of the Joint Trade Associations' rehearing request.

33. Reliability Standards set forth requirements with which responsible entities must comply. Violation Severity Levels, in contrast, do not set forth Requirements, but instead are post-violation measurements of the degree to which a requirement was violated.[27] The Violation Severity Levels, together with the Violation Risk Factors, are the initial factors that the ERO and Regional Entities will apply when determining an appropriate penalty range for a violation of a Commission-approved Reliability Standard.[28] Similar to Violation Risk Factors, the Commission has previously found that Violation Severity Levels are not part of the Reliability Standard itself.[29] Rather, they help ensure that any penalty is proportionate to the reliability risk incurred, as discussed above. Accordingly, the Commission finds that NERC's revisions of the assignment of Violation Severity Levels are not a modification to the Reliability Standards and, thus, are not required to comport with the Reliability Standards development provisions of section 215 of the FPA.

34. In a January 2007 order, the Commission discussed appropriate treatment of Violation Risk Factors, explaining that they should be treated like NERC's procedural rules:

> Because NERC proposes to employ Violation Risk Factors solely in determining penalties for violations of Reliability Standards, we believe that, like the Sanction Guidelines, Violation Risk Factors may be appropriately treated as an appendix to NERC's Rules of Procedure. As such, NERC approval of the Violation Risk Factors would be governed by section 1400 of

[27] Violation Severity Level Order, 123 FERC ¶ 61,284 at P 15.

[28] *Id.* P 13.

[29] *North American Electric Reliability Corp.*, 119 FERC ¶ 61,145 at P 17, *order on reh'g and compliance filing*, 120 FERC ¶ 61,145 (2007).

> NERC's Rules of Procedure, which addresses amendments to the Rules of Procedure. Thus, we believe that NERC should not use its Reliability Standards Development Procedure to develop the Violation Risk Factors for filing with the Commission.[30]

35. Thus, to the extent Joint Trade Associations' assert that the Commission *may not* direct NERC to modify its proposed Violation Severity Levels without going through the Reliability Standards Development Process, we reject that assertion. As discussed above, such arguments are inconsistent with Commission precedent. Moreover, the Commission has denied two rehearing requests that make the same argument regarding Violation Risk Factors.[31] And since the Violation Risk Factors and the Violation Severity Levels work in conjunction, the same precedent applies here.

36. To the extent Joint Trade Associations' contend that the Commission *should*, under these circumstances, allow NERC to revise the Violation Severity Levels, we decline to do so here. The Commission has previously clarified that it did not object to use of the Reliability Standards Development process to develop Violation Risk Factors so long as it produced timely results; the same applies to Violation Severity Levels.[32] However, in the situation presented here, we do not believe it is a prudent use of resources to require NERC and the industry to now rewrite the modified Violation Severity Levels applicable to the no-longer effective Version 1 CIP Reliability Standards. NERC has already made a compliance filing adopting the changes requested in the underlying order, and the Version 3 CIP Reliability Standards are now currently

---

[30] *North American Reliability Corp.*, 118 FERC ¶ 61,030, at P 91 (January 2007 Order), *order on clarification and reh'g*, 119 FERC ¶ 61,046 (2007); *see also* Violation Severity Level Order, 123 FERC ¶ 61,284 at P 15.

[31] In the April 2007 Order, protestors sought rehearing of the January 2007 Order, arguing that the Violation Risk Factors are performance elements of the Reliability Standards and, as such, must be developed with the same opportunity for public comment, due process, openness and a balance of interests as the Reliability Standards development process affords. The Commission denied the request for rehearing on this point, and again when the City of Santa Clara made the same request regarding a May 2007 Order. *North American Reliability Corp*., 118 FERC ¶ 61,030, *order on clarification and reh'g*, 119 FERC ¶ 61,046 at P 29. *North American Electric Reliability Corporation*, 120 FERC ¶ 61,145 at P 15.

[32] *North American Electric Reliability Corporation*, 120 FERC ¶ 61,145 at P 13 (citing North American Electric Reliability Corporation, 119 FERC ¶ 61,046 at P 15).

effective.[33] However, the Commission reminds the Joint Trade Associations that NERC and the industry can propose revised Violation Severity Levels at a future date that take into account the newly-established guidelines and that include different gradation based on historical experience, analogous to its recent filing in Docket No. RR08-4-000.

The Commission orders:

The request for rehearing is hereby denied, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

[33] *North American Electric Reliability Corp.*, Docket No. RM06-22-013 (Sept. 8, 2010) (delegated letter order).