UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Version 5 Critical Infrastructure Protection Reliability Standards	**)** **)**	**Docket No. RM13-5-000**

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON THE NOTICE OF PROPOSED RULEMAKING FOR VERSION 5 CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

The North American Electric Reliability Corporation ("NERC") hereby provides comments on the Notice of Proposed Rulemaking ("NOPR") regarding NERC's proposed Version 5 Critical Infrastructure Protection ("CIP Version 5") Reliability Standards[1] issued by the Federal Energy Regulatory Commission ("FERC" or "Commission") in this proceeding on April 18, 2013.[2] NERC provides these comments as the Commission-certified[3] electric reliability organization ("ERO") responsible for the development and enforcement of mandatory Reliability Standards, including the proposed CIP Version 5 Reliability Standards.[4]

In the NOPR, the Commission proposes to approve CIP Version 5 (CIP-002-5 through CIP-009-5, CIP-010-1 and CIP-011-1) submitted by NERC for approval. The Commission states that the proposed CIP Version 5 Reliability Standards, which pertain to the cyber security of the Bulk Electric System ("BES"), represent an improvement over the current Commission-approved CIP Reliability Standards as they adopt new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards. The Commission

---

[1] *See* NERC Feb. 1, 2013 Petition for Approval of Critical Infrastructure Protection Reliability Standards ("Petition").

[2] *Version 5 Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 143 FERC ¶ 61,055 (2013).

[3] *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[4] Capitalized terms not otherwise defined herein, shall have the meaning set forth in the NERC *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), available at http://www.nerc.com/files/Glossary_of_Terms.pdf.

proposes, however, to direct that NERC develop modifications to the proposed CIP Version 5 Reliability Standards to address certain matters identified by the Commission. The Commission has requested comments on its proposal.

I. Introduction

NERC supports the Commission's proposal to approve the proposed CIP Version 5 Reliability Standards and commends the Commission's effort to expeditiously issue the NOPR. NERC respectfully requests that the Commission issue its final rule in this proceeding as soon as reasonably possible to assist NERC in providing clear transition guidance to the industry on a timely basis and provide the industry additional clarity on the obligations imposed by the proposed CIP Version 5 Reliability Standards.

NERC requests that the Commission approve the proposed CIP Version 5 Reliability Standards as filed. As discussed below, the Commission should approve the "identify, assess, and correct" language[5] that is included in certain requirements in proposed CIP Version 5 because the language will improve reliability by strengthening internal security processes. The self-correcting language is intended to prescribe the manner in which entities must implement their policies and procedures for specific areas of security protection, requiring entities to demonstrate that they are implementing processes in a manner that identifies, assesses, and corrects deficiencies.

The self-correcting language is auditable and enforceable as an implementation obligation that can be verified by a trained auditor and does not affect the enforceability of the underlying obligations in the applicable requirements. Responsible entities must implement the technical controls ("Technical Parts") contained in the tables in each affected CIP Reliability

[5] The "identify, assess, and correct" language is also referred to herein as "self-correcting language."

Standard or risk potential noncompliance for failure to do so. The self-correcting language, where used, mandates the specific approach entities must use in the implementation of their documented processes. Whether the entity used the mandated implementation method to identify, assess, and correct a deficiency would be verified by an auditor. As discussed below, the standard drafting team intended the self-correcting language to work in concert with a compliance approach for frequently occurring obligations that present a lesser risk to reliability. Should the Commission approve the self-correcting language, NERC commits to submit a compliance filing to explain the compliance approach associated with the self-correcting language that is currently in development.

These comments provide additional technical support for the proposed requirements and definitions, as well as the proposed Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs"). Many of the issues the Commission raises in the NOPR require further evaluation and are more appropriately the subject of a technical conference than a directive to modify the proposed CIP Version 5 Reliability Standards in the final rule. Considering these issues through a technical conference will allow for timely implementation of the improvements in proposed CIP Version 5 and allow for additional discussion on the issues. The CIP Reliability Standards have been in a constant state of revision, with multiple versions of the Reliability Standards, and time is needed for entities to focus on implementation of proposed CIP Version 5 prior to the addition of any further changes. Additionally, NERC continues to support the proposed implementation plan and discusses the need for the proposed implementation periods.

II. The Commission Should Approve the "Identify, Assess, and Correct" Language Without Modification

As the Commission notes in the NOPR, 17 requirements in the proposed CIP Version 5 Reliability Standards include language that requires the responsible entity to implement the

requirement *in a manner to "identify, assess, and correct" deficiencies*.[6] As noted in NERC's Petition, the self-correcting language, where used, is presented in the following format:

> Each Responsible Entity shall implement, *in a manner that identifies, assesses, and corrects deficiencies*, one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table].

In the NOPR, the Commission expresses concern that the "identify, assess, and correct" language is unclear with respect to the implementation and compliance obligations it places on regulated entities and that it is "too vague" to audit and enforce compliance.[7] Generally, the Commission seeks comment on the meaning of this language and how it will be implemented and enforced.[8] Depending on the comments and explanations received, the Commission states that it may direct NERC to develop modifications, which could require NERC to: (1) clarify both the implementation and compliance obligations created by this language and the criteria by which auditors will be able to determine compliance; or (2) remove this language if the Commission determines that its inclusion results in requirements that "degrade the protections afforded by the CIP Version 5 Standards and are difficult to implement and enforce."[9]

NERC requests that the Commission approve the "identify, assess, and correct" language without modification. As discussed further below, this self-correcting language has tangible reliability benefits as it will strengthen internal security processes and allow responsible entities to focus their resources on detecting and correcting deficiencies in their cyber security programs. By focusing on the identification, assessment, and correction of deficiencies, these proposed CIP Version 5 requirements impose an obligation on responsible entities to take a proactive approach

---

6 NOPR at P 4 (emphasis added).

7 *Id*.

8 *Id*. at P 46.

9 *Id*.

to protecting their BES Cyber Systems. Each technical requirement in CIP Version 5 identifies the controls or Technical Parts that the responsible entity's documented processes must cover and requires implementation of those processes to achieve the Technical Parts. In the requirements that include the self-correcting language, *how* the entity must execute its implementation obligation is prescribed by the inclusion of the phrase "in a manner that identifies, assesses, and corrects deficiencies" in the standard language itself.

Whether the entity uses the mandated implementation method of identifying, assessing, and correcting deficiencies would be reviewed by an auditor. This review will require a heightened level of discretion and use of professional judgment by auditors when determining whether the entity implemented the requirement in the prescribed manner. NERC and the Regional Entities will train auditors and develop guidance to provide for consistent and effective auditing practices across the ERO. NERC is currently developing compliance tools, such as Reliability Standard Audit Worksheets ("RSAWs"), to provide the necessary clarity.[10] Additionally, the self-correcting language was intended to work in concert with a compliance approach for frequently occurring security obligations ("High Frequency Security Obligations") that present a lesser risk to reliability that reduces the administrative burden of the compliance process. NERC requests that the Commission approve the self-correcting language and permit NERC to submit a compliance filing, by the later of June 1, 2014 or six months from the date of the final rule on the proposed CIP Version 5 Reliability Standards, describing the compliance approach associated with the "identify, assess and correct" language.

If the Commission directs any changes to the "identify, assess, and correct" language, NERC respectfully asks that the Commission provide a reasonable time frame for meeting a

[10] As explained in section V below, NERC will conduct a pilot program during the transition from CIP Version 3 to CIP Version 5. This pilot program will provide valuable feedback to NERC compliance staff on the RSAWs and on the transition process.

directive through the Reliability Standards development process. Resolving how to approach the requirements with High Frequency Security Obligations is a complex task and was a major focus in the development of proposed CIP Version 5. The standard drafting team addressed this issue with the inclusion of the "identify, assess, and correct" language. If the Commission directs removal or material modification to that language, the drafting team may need to consider alternative options. As a result, modifying or removing this language through the Reliability Standards development process could delay implementation of the proposed CIP Version 5 Reliability Standards. NERC urges the Commission to approve the language and accept NERC's commitment to submit a compliance filing to support the compliance obligations for the language.

Below, NERC provides: (1) background on the development of the "identify, assess, and correct" language; (2) an explanation of the meaning of and the performance expectations created by the "identify, assess, correct" language; (3) a discussion of the reliability benefits of the self-correcting language; and (4) a discussion of the proposed compliance approach associated with the self-correcting language and a commitment to submit a compliance filing further detailing that compliance approach. NERC also explains that the self-correcting process is consistent with the principles of the National Institute of Standards and Technology's ("NIST") Risk Management Framework ("NIST Framework").

a. Background

The inclusion of self-correcting language in certain requirements is consistent with the standard drafting team's original intent for the development of the proposed CIP Version 5 standards. As early as October of 2010, the standard drafting team identified that a zero defect approach to compliance for certain requirements in the CIP Reliability Standards needed to be

addressed in the proposed CIP Version 5 Reliability Standards.[11] Experience with prior versions of the CIP Reliability Standards demonstrated that because several CIP requirements require entities to perform certain security operations on a frequent or continual basis for a significant number of assets, it is difficult to perform with 100% accuracy. For these High Frequency Security Obligations, a zero-defect approach to compliance does not encourage entities to proactively search for deficiencies in these environments due to the resulting compliance process burden. That is, by increasing diligence in areas where it is difficult to perform an obligation with 100% accuracy, an entity may frequently trigger an extensive administrative compliance process, regardless of the level of risk that the potential noncompliance poses to the reliability of the Bulk-Power System.

In order to focus entities on creating and maintaining a high performing security program that demonstrates continuous security awareness, the standard drafting team set a goal early in the CIP Version 5 development process to minimize the compliance burdens associated with High Frequency Security Obligations.[12] In other words, the standard drafting team drafted requirements that acknowledge the nature of these High Frequency Security Obligations and focus entities' efforts on identifying and correcting deficiencies. The purpose was to support the development of requirements in proposed CIP Version 5 that foster a "culture of security."[13] To that end, the standard drafting team inserted the "identify, assess, and correct" language in

---

[11] *See* 27th Meeting Summary, Cyber Security Order 706 SDT — Project 2008-6, *available at* http://www.nerc.com/pa/Stand/Project%2020086%20Cyber%20Security%20Order%20706%20RF/CSO706-SDT-Oct-12-14_Toronto_FINAL_Meeting-Summary_(2).pdf.

[12] *Id.*

[13] *See* 30th Meeting Summary, Cyber Security Order 706 SDT — Project 2008-06, available at http://www.nerc.com/pa/Stand/Project%2020086%20Cyber%20Security%20Order%20706%20RF/CSO706_SDTJan_18-20_2011_Meeting_Summary.pdf.

requirements that contained High Frequency Security Obligations to require entities to detect and correct deficiencies as part of the required performance.

The intention was not to eliminate accountability for the registered entities or the ability for Regional Entities, NERC, and the Commission to engage in oversight. The placement of the "identify, assess, and correct" language in the requirements prescribing the implementation method was not intended to dictate how compliance would ultimately be measured. In fact, during the development of draft 3 of the proposed CIP Version 5 Reliability Standards, NERC standards development staff worked with NERC compliance staff to make certain that the language used in the proposed CIP Reliability Standards would be compatible with the compliance program, *regardless* of how compliance is measured, now or in the future.

b. Meaning of and Performance Expectations Created by the "Identify, Assess, and Correct" Language

The self-correcting language is intended to prescribe the manner in which entities must implement their policies and procedures for specific areas of security protection. While Reliability Standards generally do not delineate how a Responsible Entity must implement a requirement, this self-correcting approach is essential given the High Frequency Security Obligations in some of the proposed CIP Version 5 requirements. As indicated above, for the proposed requirements that include High Frequency Security Obligations, the optimal approach from a reliability standpoint is to focus entities on correcting identified deficiencies in its implementation of the Technical Parts of the proposed requirements to promote continuous awareness in an entity's cyber security program.

In drafting all of the requirements for proposed CIP Version 5, the standard drafting team intended to write straightforward requirements that state the desired behavior that will maximize the reliability of the Bulk Electric System. As a result, the proposed CIP Version 5 requirements

are written to require documented processes that must address and be implemented to achieve the specific Technical Parts in the requirements. The Technical Parts, therefore, set the "bright-line" parameters for the processes and the expectations for implementation. In other words, the requirements mandate the minimum protection that must be provided to BES Cyber Systems by the users, owners, and operators of the Bulk-Power System necessary to maintain reliability.

Some of these requirements in proposed CIP Version 5 contain the self-correcting language that prescribes how the entity will implement the processes, while others do not. For the proposed CIP Version 5 requirements that do not contain the self-correcting language, entities are obligated to: (1) have the documented processes stated in the requirement; and (2) implement the documented processes to achieve the Technical Parts. How the entity chooses to implement the process would be documented for the Compliance Enforcement Authority, as required by the associated Measure. For these requirements, the entity either has the process in place and the process achieves the Technical Parts or the entity does not have a process in place and/or its process does not achieve the Technical Parts.

In requirements where the self-correcting language is used, the self-correcting language does not affect the underlying obligation in the requirement to achieve the Technical Parts. Rather, the addition of the "identify, assess, and correct" language in the requirements mandates that the entity use a self-correcting process in its implementation of its documented policies to achieve the Technical Parts.

In summary, in accordance with requirements in the proposed CIP Version 5 Reliability Standards that require a documented process, regardless of whether such requirement includes the identify, assess and correct language, the requirement contains *two* obligations. The first is to have the process and the second is to implement the process. The difference is that those

requirements containing self-correcting language set additional parameters for the manner in which an entity should implement the process.

During the Reliability Standards development process, the standard drafting team did not create a specific definition for the terms "identify," "assess," "correct," or "deficiency." NERC agrees with creating defined terms for "identify," "assess," and "correct" because responsible entities are in the best position to define their own internal compliance processes based on the particular characteristics and make-up of their systems, including whether they will use internal controls or a different type of compliance management process to meet their specific system design. Specifying a uniform definition of "identify," "assess," and "correct" is impracticable given the wide range of systems and the number of assets that make up an entities' systems.

The following example, addressing requirements for logging electronic and physical events, illustrates how the "identify, assess, and correct" language would work in practice.[14] In Version 4 of the CIP Reliability Standards, the requirements covering logging electronic and physical events, (CIP-005-4, Requirement R3[15] and CIP-006-4, Requirement R5[16]) require that logs be collected "twenty-four hours per day, seven days a week," essentially mandating a 100% up-time for the central logging server that is collecting and managing the logs. This 100% availability target, however, is difficult to attain for several reasons: hardware can fail, disks can fill up, power can be interrupted, or software clean-up routines can stop working.[17] These are all

[14] This example is provided for illustrative purposes only and not for use in complying with the proposed CIP Version 5 requirements.

[15] Measure M3 for CIP-005-4 requires the responsible entity to make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in CIP-005-4, Requirement R3.

[16] Measure M5 for CIP-006-4 requires the responsible entity to make available documentation identifying the methods for monitoring physical access as specified in CIP-006-4, Requirement R5.

[17] Additionally, the systems that collect these logs qualify as "physical access control systems" or "electronic access control and monitoring systems," which must be protected in accordance with CIP-005-4, Requirement R1.5 and CIP-006-4, Requirement R2.2, which in turn, reference CIP-007-4, Reference R3 (Security Patch Management).

real world situations that likely pose little or no risk to the Bulk-Power System so long as they are corrected in a timely manner.

The proposed CIP Version 5 requirements approach this issue differently. Rather than focusing on the device or method used to collect and store the logs, proposed CIP-005-5, Requirement R1, Part 1.8 and CIP-007-5, Requirement R4 Part 4.1 focus on the act of *collecting* the logs. For example, proposed CIP-007-5, Requirement R4 Part 4.1 requires entities to "[l]og events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents …" The associated Measure in Part 4.1 states that examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events that are listed in the Part 4.1.

These logging requirements in proposed CIP Version 5 must be "implemented, in a manner that identifies, assesses, and corrects deficiencies" through the use of "one or more documented processes." As such, an entity must: (1) have a documented process that describes how events will be logged and maintained such that the after-the-fact investigation can be performed, *i.e.* the documented process meets the Technical Part (Part 4.1); and (2) implement that process to fulfill the obligations in the Technical Part. As part of such implementation, an entity will also demonstrate that its implementation includes the identification, assessment, and correction of deficiencies in its process as part of its implementation obligation on how it implements the documented process.

Patch management typically requires that systems be rebooted following a patch installation in order for the patch to be fully installed, but the reboot requirement causes the logging system to be unavailable. Although it is possible to implement redundant log collecting systems, even these systems cannot guarantee 100% up-time as required by the standard.

An entity's documented process is expected to accommodate anticipated failure modes, such as hardware and software failures at the central log server, as well as communication pathway failures between the log generators and the logging system.[18] An entity's processes would be expected to account for failures in the processes used to generate logs as well as failures to successfully transmit those log entries to the central server. If experience shows that the entity's procedures were found to be insufficient, or actual performance of the program did not meet expectations, the "identify, assess, and correct" language mandates that the entity's processes and implementation be modified to correct any deficiencies. Depending on the facts and circumstances of the deficiency, there may be a potential violation if actual performance does not meet the Technical Parts.

c. Reliability Benefits Associated with the "Identify, Assess, and Correct" Language

The self-correcting language improves the protections of the CIP Reliability Standards. Implementing a self-correcting process is a best practice used by many entities in their compliance with all Reliability Standards. The inclusion of this process is appropriate for use in the CIP Reliability Standards because it promotes robust internal security programs in a constantly changing cyber security environment by requiring entities to examine their systems for issues and correct them. Such a process would provide incentives for responsible entities to be more aware of security issues, thereby increasing the reliability and resiliency of the Bulk Electric System. Importantly, as explained below, the "identify, assess, and correct" language does not eliminate accountability for the registered entities or the ability for Regional Entities, NERC, and the Commission to engage in oversight.

[18] For example, because it is well known that hardware fails for any of a number of reasons, the documented process should include provisions for (1) detecting when the hardware fails, (2) notifying appropriate support personnel of the failure, and (3) instructions for how to fix or replace the failed hardware and restore the logging system to full functionality. It is expected that there be time targets associated with each of these steps.

While this type of self-correcting process is currently used today on a voluntary basis by many entities complying with Reliability Standards generally, the practice is not mandatory and enforceable. Mandating the use of a self-correcting process in these requirements in the CIP context will provide auditors a view into the range of processes and programs entities use to resolve deficiencies in their compliance processes – a view not necessarily available to auditors measuring compliance under the current CIP Reliability Standards. Requiring entities to demonstrate how each step in the self-correcting process was met will place auditors in a position to fully understand an entity's program and how it protects its security environment.

d. Compliance Approach Associated with the "Identify, Assess, and Correct" Obligation

The standard drafting team intended the self-correcting language to work in concert with a modified compliance approach for High Frequency Security Obligations that result in lesser risk deficiencies. It was anticipated during the Reliability Standards development process that NERC would design a compliance approach through RSAWs to reduce the compliance process burden for High Frequency Security Obligations that result in lesser risk deficiencies and move away from a zero defect approach to compliance for the requirements containing the self-correcting language. A zero defect approach to compliance for such obligations would result in an administratively burdensome compliance process that does not (1) distinguish between lesser and higher risk deficiencies, (2) focus an entity's resources through a mandatory requirement to "correct" a deficiency in the overall security program, or (3) result in greater reliability. The standard drafting team acknowledged during development that this associated compliance element is a developing concept and would require industry to continue to work with NERC on this approach.[19]

[19] NERC Petition, Ex. D, Oct. 26, 2012 Consideration of Comments at 9.

NERC remains committed to developing the RSAWs and other guidance to support the self-correcting language.[20] To that end, if the Commission approves the "identify, assess and correct" language, NERC commits to submit a compliance filing with the Commission by the later of June 1, 2014 or six months from the date of the final rule on the proposed CIP Version 5 standards that further outlines the compliance and enforcement aspects of this language, including when entities are expected to self-report or maintain documentation of its self-correcting process for audit, what constitutes potential noncompliance, and the necessary guidance for auditors. NERC is currently developing tools, such as the RSAWs, to reduce the compliance process burden on entities while making certain entities remain responsible for the underlying Technical Parts of the requirements.

During the Reliability Standards development process, NERC provided a sample RSAW to help the standard drafting team understand how NERC might match the compliance guidance to the specific self-correcting approach incorporated into certain requirements in proposed CIP Version 5. It was provided for illustrative purposes only and the explanation that follows is also provided as an example of what was intended for the compliance approach to maximize the reliability benefit and reduce the compliance process burden where appropriate.

In the sample RSAW, NERC delineated how an entity would demonstrate compliance with the Technical Parts of the proposed standard. In a following section, NERC provided additional compliance monitoring instruction for the implementation aspect of the requirement to verify that the entity has implemented the necessary Technical Parts in a manner that identifies, assesses, and corrects deficiencies. While the RSAW provides a non-exclusive list of examples of how a deficiency may be corrected by an entity, the guidance focused on first requiring the

[20] As noted herein, the NERC compliance staff will also have the opportunity to work closely with certain entities utilizing the RSAWs during early implementation of CIP Version 5 through a pilot program. This will allow NERC staff to make any necessary adjustments to the RSAWs during the transition.

Compliance Enforcement Authority to obtain an understanding of the entity's implementation of the applicable technical controls and review a representative sample of the entity's documentation to review whether the entity is implementing the technical controls in a self-correcting manner.

Entities have the ability to demonstrate to an auditor the process they used to identify a deficiency, how they assessed the deficiency, and whether the process corrected the deficiency. The focus of the Compliance Enforcement Authority will be on the effectiveness of the process, determined by the correction of the deficiency and, based on the professional judgment of the auditor, whether the correction of the deficiency was sufficient to prevent future occurrences of the deficiency. The method itself for identifying, assessing, and correcting deficiencies will need to be understood by and documented for the auditor to determine the facts and circumstances of the specific deficiency and the level of information required to demonstrate proper implementation through assessing and correcting an identified deficiency.

In the sample RSAW, "deficiencies" referred to potential noncompliance with the proposed CIP Version 5 requirement; however, not all deficiencies would be treated as possible violations depending on the specific facts and circumstances surrounding the deficiency. An entity would be expected to document the identification, assessment, and correction of deficiencies. However, while the correction of lesser risk deficiencies would be documented for review by the Compliance Enforcement Authority, entities would be expected to continue to self-report higher risk deficiencies. Not requiring the individual reporting and processing of corrected lesser risk deficiencies will result in resource savings and, more importantly, allow entities to focus efforts on the security issues rather than the administrative aspects of the compliance processes. The Regional Entities, NERC, and the Commission would maintain

visibility and oversight of the correction of lesser risk deficiencies through documentation of the correction provided during an audit. NERC will address what constitutes a higher and lesser risk deficiency in the compliance filing.

In response to the Commission's concern regarding the timing of the self-correcting process, an entity's own internal processes would dictate the timing aspect. However, to the extent an entity delays the identification, assessment, or correction of a deficiency until shortly before an audit, that entity would not be identifying, assessing, and correcting deficiencies as intended by the language and the entity would likely be found to be noncompliant with its implementation obligation. As part of an audit, the entity would explain the timing of its process to the auditor and the timing would be one factor considered by the auditor in understanding the process that led to the correction.

The compliance processes and audit criteria associated with compliance monitoring for the self-correcting language are in development and will be discussed in NERC's compliance filing. However, it is important to emphasize that the purpose of the self-correcting language was not to shield the entity from responsibility if an event occurs as a result of a deficiency, but to allow Regional Entities and NERC to monitor and oversee how registered entities correct deficiencies such that the compliance process burden could be reduced without sacrificing reliability.

e. Consistency with the NIST Framework

The inclusion of self-correcting language as the prescribed manner of implementation in certain requirements is also consistent with the NIST Framework. The NIST Framework[21]

[21] The NIST Framework is available on NIST's website at http://csrc.nist.gov/groups/SMA/fisma/framework.html.

includes steps to implement, assess, and monitor security controls.[22] Under the NIST Framework, organizations are expected to implement the security controls and document how the controls are deployed within the information system and environment of operation.[23] This is similar to the approach in the proposed CIP Version 5 Reliability Standards to have a documented process that accounts for the Technical Parts of the requirements and to implement these processes to achieve those Technical Parts.

Organizations using the NIST Framework are also asked to assess their security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[24] This is similar to the proposed CIP Version 5 Reliability Standard requirements to identify, assess, and correct deficiencies. This self-correcting implementation obligation requires entities to: (1) determine the extent to which their controls are implemented correctly by looking for and finding deficiencies; (2) correct any identified deficiency and adjust their processes in an effort to prevent a reoccurrence of the deficiency; and (3) achieve the desired outcome, which is greater awareness for the specific security protection in a specific technical area.

In sum, requiring entities to continuously demonstrate that they are implementing processes in a manner that identifies, assesses, and corrects, is similar to the monitoring steps of the NIST Framework,[25] which require organizations to, on an ongoing basis, assess security

---

22 *See e.g.*, NIST's Frequently Asked Questions document on continuous monitoring at http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf and NIST Special Publications 800-53, 800-37, and 800-137.

23 *See* NIST Special Publication 800-137.

24 *Id.*

25 *Id.*

control effectiveness and document changes to the system or environment of operation (*i.e.*, modifying documented processes in the CIP Reliability Standard context).

III. BES Cyber Asset Categorization and Protection

a. Facility Rating Categorization

In response to the Commission's directive in Order No. 706 to review NIST's standards to determine whether they contain provisions that will be useful for adoption in the CIP Reliability Standards, NERC proposed to incorporate the concept of categorizing assets as having a "Low," "Medium," or "High" Impact.[26] Proposed Reliability Standard CIP-002-5 requires responsible entities to categorize BES Cyber Systems as "Low," "Medium," or "High" Impact based on the adverse impact that loss, compromise, or misuse could have on the reliable operation of the Bulk Electric System.

The Commission notes in the NOPR that NERC's reliability-based proposed approach to categorization differs from the NIST Framework, which utilizes a categorization process based on the loss of confidentiality, integrity, and availability of systems.[27] The Commission proposes to accept NERC's proposal, although the Commission notes it may revisit the categorization at a later time.[28]

NERC notes that the standard drafting team evaluated the CIP Reliability Standards to determine whether aspects of the NIST Framework are appropriate for inclusion into the mandatory CIP Reliability Standards. The standard drafting team concluded that a "Low," "Medium," or "High" Impact categorization based on facility rating was appropriate because it (1) reflects a well understood and commonly used method for categorizing assets within the

---

[26] This asset categorization is based on the NIST Framework.

[27] NOPR at PP 61-64.

[28] *Id*. at P 64.

electricity sector; (2) provides a clear and measurable method for identifying assets; and (3) directly relates to a facility's impact on the Bulk Electric System, which is consistent with the NIST Framework approach to categorizing assets based on risk levels.

The NIST Framework requires entities to assign "security categories [that are] are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."[29] In a NERC Reliability Standard, the analog to "assigned mission" is the continued reliable operation of the Bulk-Power System, thus the impact level categorization method is appropriate. Further, the NIST standards are "information protection" standards, while the NERC standards are "reliability standards" necessitating a slightly different categorization approach that is aimed more broadly at the reliability of the Bulk-Power System across all entities rather than categorization by a single organization.

For these reasons, NERC requests that the Commission adopt the NOPR proposal to accept NERC's categorization approach. A change from a facility-based approach would require significant overhaul of the CIP Reliability Standards. To the extent this topic is revisited in the future, NERC requests that the topic first be discussed in a technical forum led by NERC or the Commission to obtain input from industry subject matter experts.

[29] *See* Federal Information Processing Standard 199, Standards for Security Categorization of Federal Information and Information Systems at 3, *available at*, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

b. Protection of Low Impact BES Cyber Assets

The Commission states that "NERC's new approach to categorizing BES Cyber Systems is a step closer to comprehensively protecting assets that could cause cyber security risks to the bulk electric system."[30] The Commission asserts, however, that NERC should consider modifying the protections to identify specific controls for Low Impact assets. The Commission notes that Requirement R2 of Reliability Standard CIP-003-5 sets forth the single compliance obligation for BES Cyber Systems categorized as Low Impact. In short, CIP-003-5, Requirement R2 requires entities to implement "documented cyber security policies" for Low Impact BES Cyber Systems.[31] The Commission is concerned that without enumerating specific, technically-supported cyber security controls, this requirement may be insufficient to protect Low Impact BES Cyber Assets.[32]

To that end, the Commission proposes to direct NERC to develop a modification to CIP-003-5, Requirement R2 to require responsible entities to adopt specific, technically-supported cyber security controls for Low Impact assets.[33] The Commission has requested comments on the value of adopting specific controls for Low Impact assets that reflect their cyber security risk level, similar to the NIST Framework.[34] Additionally, the Commission is seeking comment on the lack of a requirement to have an inventory, list, or discrete identification of Low Impact BES Cyber Systems.[35]

---

30 NOPR at P 59.

31 *Id*. at P 66. Requirement R2 requires that a responsible entity have documented policies for (1) cyber security awareness; (2) physical security controls; (3) electronic access controls for external routable protocol connections and Dial-up Connectivity; and (4) incident response to a Cyber Security Incident.

32 *Id*. at PP 66-70.

33 *Id*. at P 70.

34 *Id*.

35 *Id*. at P 71.

NERC respectfully requests that the Commission not direct NERC to prescribe specific controls for Low Impact assets. Proposed CIP Version 5 represents a significant improvement over prior versions of the CIP Reliability Standards, in part because a significant number of assets that were previously not subject to the CIP Reliability Standards will now be identified as Low Impact assets under CIP-002-5. In accordance with CIP-003-5, Requirement R2, responsible entities will now be obligated to develop and *implement* cyber security policies for Low Impact assets that address (1) cyber security awareness; (2) physical security controls; (3) electronic access controls for external routable protocol connections and Dial-up Connectivity; and (4) incident response to a Cyber Security Incident. This obligation is a significant step in more comprehensively protecting assets that could cause cyber security risks to the bulk electric system.

In deciding on the appropriate level of protection for Low Impact assets, the standard drafting team considered: (i) the risk level associated with Low Impact assets; (ii) the great diversity of asset types that would fit this category; (iii) the diversity in entity types that have Low Impact assets; and (iv) that many of these assets and entities had never before been subject to the CIP Reliability Standards. Given the above-mentioned factors, the standard drafting team determined that it was not appropriate at this time to draft specific controls for these Low Impact assets with universal applicability. An overriding concern was that by mandating specific controls, the Reliability Standards would ultimately stunt the development of the range of controls necessary to protect the diversity of Low Impact assets now subject to the CIP Reliability Standards. The standard drafting team sought to take advantage of the industry's experience with and knowledge of these diverse assets by providing industry the room to develop the necessary controls in a manner that best fits their particular assets and operations.

Implementation experience with the existing proposed CIP-003-5 will allow NERC to understand how entities are approaching the protection of Low Impact systems and will inform the future development of specific controls if they are deemed necessary. NERC expects that entities will adopt the controls necessary to protect Low Impact systems (from a coordinated attack or otherwise). Auditors will have an opportunity to review the adequacy of those cyber security policies and implementation thereof. Recognizing that some entities may be designing and implementing cyber security policies for these assets for the first-time, NERC commits to conduct outreach to industry through webinars and other educational tools to assist industry in identifying effective controls for specific types of Low Impact systems. NERC will be reviewing asset categorization, especially in early period of CIP Version 5, to make sure responsible entities are appropriately determining impact levels.

With respect to the lack of a requirement to have an inventory, list or discrete identification of Low Impact BES Cyber Systems, NERC stresses that entities will need to be able to demonstrate compliance with CIP-002-5, which requires such entities to identify the assets that are associated with its Low Impact BES Cyber Systems. In complying with CIP-002-5, entities may choose to keep an inventory or list of its Low Impact assets to help ensure that it has properly identified and categorized its assets. However, the act of keeping such a list or inventory does not need to be included as a separate requirement. There is no added reliability benefit to creating a separate requirement obligating an entity to create and continually update a list of Low Impact assets.[36] NERC also notes that proposed CIP-002-5 Part 1.3 requires that responsible entities "[i]dentify each [BES] asset that contains a low impact BES Cyber System." This identification obligation results in a list of BES locations containing Low Impact BES

[36] In contrast, because the number of assets for Medium and High Impact BES Cyber Systems is more limited and such assets have a greater impact on reliability, it is appropriate to mandate that entities keep a list of such assets.

Cyber Systems, not a list of the Low Impact BES Cyber Systems themselves. The resulting list of locations provides for an audit approach consistent with existing sampling methods.

IV. Proposed Definitions

The Commission proposes to approve the fifteen new definitions and four revised definitions proposed by NERC.[37] The Commission also seeks comment on certain aspects of the proposed definitions, as discussed below.

a. BES Cyber Asset

NERC proposes to define "BES Cyber Asset" as:

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

The Commission seeks comment on the following two aspects of the definition of BES Cyber Asset:

- the purpose and effect of the 15-minute parameter for the identification of a BES Cyber Asset; and
- the purpose and anticipated effect of the provision stating that a "Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."

As discussed below, the Commission should approve the definition of BES Cyber Asset as proposed. The 15-minute parameter and the 30-day or less exclusion provisions are necessary

[37] NOPR at P 72.

for ensuring that the appropriate assets are defined as BES Cyber Assets. These qualifiers would also not leave any gaps in reliability, as explained below.

i. 15-Minute Parameter

The Commission notes in the NOPR that CIP Version 4 included a 15-minute parameter for the identification of Critical Cyber Assets associated with certain generation units.[38] As the Commission states, this 15 minute parameter was adopted to address the concern that "there may be facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes." The Commission is seeking comments on the purpose and effect of the proposed extension of this 15-minute parameter to the identification of all BES Cyber Assets.[39]

Specifically, the Commission seeks comments on (i) the type of Cyber Assets that would meet the 15-minute parameter; (ii) the types of assets or devices that the 15-minute parameter would exclude; (iii) whether the caveat "within 15 minutes" exempts devices that have an impact on the reliable operation of the bulk electric system; and (iv) whether the use of a specified time period as a basis for identifying assets for protection is consistent with the procedures adopted under other cyber security standards, such as the NIST Framework, that apply to industrial control and Supervisory Control and Data Acquisition ("SCADA") systems, as well as traditional information technology systems.[40]

The standard drafting team adopted the 15-minute parameter for the identification of a BES Cyber Asset to capture only those Cyber Assets that would have a real-time impact on the

---

[38] *Id*. at P 76. Specifically, CIP-002-4a includes a 15 minute parameter for the identification of Critical Cyber Assets associated with generation units at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

[39] *Id*. at PP 76-77.

[40] *Id*. at P 77.

reliable operation of the Bulk Electric System. As stated in the background section of proposed CIP-002-5, "[t]he time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of [the CIP Version 5 Reliability Standards] is defined as that which is material to real-time operations for the reliable operation of the BES." The 15-minute parameter is essentially used as a measurable proxy for real-time operations in the CIP context.[41]

The standard drafting team decided that a 15-minute parameter (as opposed to a longer or shorter time frame) was appropriate because: (1) it is grounded in other Reliability Standards related to real-time operations (*e.g.*, BAL-002, Requirement R4; PRC-023, Requirement R1.11; IRO-006-East, Requirement R4); (2) any effect on the Bulk Electric System that takes longer than 15 minutes to manifest after the Cyber Asset is called upon can be manually remediated through established procedures that have been developed over many years, and have a proven track record of being effective; and (3) 15 minutes was a long enough window to ensure that the definition would also include those assets that present information that operators use to trigger real-time operations. The standard drafting team considered longer time periods but concluded that any time window greater than 15 minutes would not capture any additional assets that would have a real-time operational impact.

The fundamental assumption underlying the use of the 15-minute parameter is the need to protect assets that, if they become unavailable in 15 minutes or less (*i.e.*, in real-time), could result in adverse reliability impacts to the Bulk Electric System. A number of non-CIP Reliability Standards also recognize that any effect on the Bulk Electric System that takes longer than 15 minutes to manifest after a Cyber Asset is called upon and rendered unavailable can be

[41] The NERC Glossary defines the term "Real-Time" as "[p]resent time as opposed to future time." The drafting team did not use this definition in the definition of BES Cyber Asset because the drafting team sought to provide a more measurable time frame in this context and avoid confusion during implementation. This approach is consistent with the shift in CIP Version 5 to provide for a more measurable basis on which to identify those assets/systems that are subject to CIP Reliability Standards.

remediated by operators before any reliability impact would occur.[42] If an event occurs in less than 15 minutes, however, it could result in adverse impacts.[43] The definition of BES Cyber Asset is thus only necessary for those assets that could have reliability impacts within the first 15 minutes of being compromised. To be clear, the 15-minute parameter is not about detecting and responding to a Cybersecurity Incident within 15 minutes; rather the 15-minute parameter is about identifying those assets that, when called upon in real-time or rendered unavailable in real-time, could impact reliable operations. This assumption was the basis for use of the 15-minute parameter in CIP Version 4, which was approved by the Commission.[44] In developing proposed CIP Version 5, the standard drafting team concluded, for the same reasons, that the 15-minute parameter was appropriate for the identification of all BES Cyber Assets.

Examples of the assets/systems that would typically be included in the 15-minute parameter are SCADA, Energy Management Systems, transmission protection systems, and generation control systems. Typical systems that might be excluded by the 15-minute parameter are systems that collect data for engineering analysis and support, and maintenance rather than

---

[42] *See*, *e.g.*, BAL-002, Requirement R4; PRC-023, Requirement R1.11; IRO-006-East, Requirement R4.

[43] Accordingly, there are a number of Reliability Standards that require recovery within 15 minutes. For example, BAL-002, R4 sets the default Disturbance Recovery Period as 15 minutes after the start of a Reportable Disturbance. That is, if a generator is compromised such that its output will be reduced (or brought to zero), the system operator, in conjunction with both manual and automated systems, can call on reserve generation to make up for the loss in output, ramping up the replacement power to match the decline in output from the failing generator within 15 minutes. Additionally, PRC-023, Requirement R1.11 recognizes that if an operator determines that the transmission system could not recover from an overload within 15 minutes remedial action needs to be taken. If the system can recover within 15 minutes, an operator need not take any action. Similarly, IRO-006-East, Requirement R4, requires reliability coordinators to implement certain transmission congestion management actions within 15 minutes of a notification that a transmission line's capacity limit may be exceeded.

[44] The Commission concluded that NERC adequately explained and justified the 15-minute parameter in its final rule approving CIP Version 4. *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 Fed. Reg. 24594 (Apr. 25, 2012), 139 FERC ¶ 61,058 at P 33 (2012), *order denying reh'g*, 140 FERC ¶ 61,109 (2012). In its petition supporting CIP Version 4, NERC explained that if certain Cyber Assets are compromised "there may be a significant amount of time before this affects real-time operation—time during which detection and remediation may be able to be effected." NERC Petition, Docket No. RM11-11-000, at 12 (Feb. 10, 2011). The drafting team adopted a 15-minute parameter finding that "there may be facilities which, while essential to the reliability and operability of the generation facility, may not have real-time operational impact within the specified real-time operations impact window of 15 minutes." *Id.*

providing input to the operator for real-time operations or triggering automated real-time operations. Such excluded systems would include those used to collect data for the purpose of determining maintenance schedules for assets such as transformers or for engineering analysis.[45]

It is important to understand, however, that there are significant differences in the way that certain assets or systems are used across the Bulk Electric System. Therefore, whether a particular asset is included or excluded from the definition of BES Cyber Asset is necessarily dependent upon the individual facts and circumstances of how an entity uses that asset. An illustrative example is a phasor measurement unit. In some cases a phasor measurement unit would be excluded from the definition if its use is limited to providing historical data for engineering analysis. In such a scenario, it would not have a real-time reliability impact. Other entities, however, may use a phasor measurement unit to provide data for real-time operations. In the latter case, the phasor measurement unit would be considered a BES Cyber Asset because the asset has a real-time reliability impact. Responsible entities must thus evaluate how their various assets are used to determine whether a particular asset should be categorized as a BES Cyber Asset.[46]

Lastly, the use of a specified time period as a basis for identifying BES Cyber Assets is more measurable and defined than the procedures adopted under other cyber security standards, such as the NIST Framework, because it was specifically tailored for the physical characteristics of the electricity sector and the need to capture those assets with a real-time impact. Additionally, as noted above, the use of time parameters of this nature are consistent with other Commission-approved NERC Reliability Standards.

---

[45] The 15-minute parameter is irrespective of the activation of redundant BES Cyber Assets or BES Cyber Systems because, from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

[46] Any such determination will be subject to audit.

ii. 30-Day or Less Exclusion

The Commission also seeks comment on the purpose and anticipated effect of the 30-day or less exclusion language. Specifically, the Commission seeks comment on (1) whether the clause could result in the introduction of malicious code or new attack vectors to an otherwise trusted and protected system; and (2) the types of Cyber Assets used for "data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."[47]

In adopting the 30-day or less exclusion, the standard drafting team focused the definition of BES Cyber Asset on those assets directly associated with the Bulk Electric System, which the CIP Reliability Standards are designed to protect. The proposed definition clarifies that devices that are connected on a transient or temporary basis and used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes are not considered BES Cyber Assets. An example of such a transient device is a laptop connected on a temporary basis to run vulnerability assessment software or to perform computer network traffic analysis. If such devices were included in the definition of BES Cyber Asset, responsible entities would be required to apply the complete set of CIP Reliability Standards to any such device, no matter how long that device were connected to the network or who owned and managed the device. Such a requirement would be impractical and difficult to enforce and detract from a clear definition of assets that are included within the term "BES Cyber Asset."

The exclusion of such temporary devices from the definition of BES Cyber Asset, however, will not create a reliability gap. That is because the proposed CIP Version 5 Reliability Standards are designed to protect the applicable BES Cyber Systems from risks, including those risks associated with the connection of any non-BES Cyber Assets, such as transient and

[47] NOPR at P 78.

temporary devices, *regardless* of the duration of that connection or whether that device is included within the definition of BES Cyber Asset. For example, responsible entities have an affirmative obligation pursuant to CIP-007-5 to prevent malicious code from being introduced on the applicable BES Cyber System, no matter where it might originate. The absence of temporary devices in the definition of BES Cyber Asset does not relieve or otherwise lessen an entity's obligation to take the necessary steps to protect its BES Cyber Systems. As such, the 30-day or less exclusion does not provide an avenue for the introduction of malicious code or new attack vectors to an otherwise trusted and protected system. Because proposed CIP Version 5 requires entities to take the appropriate measures to ensure that its BES Cyber Systems are protected from any harm that could result from the temporary connection of non-BES Cyber Assets, it is not necessary to include such temporary devices in the definition of BES Cyber Asset to protect against the risks associated with such devices.

The standard drafting team determined that it was best to provide a 30-day time window so as to provide a bright-line, measurable proxy for what constitutes a temporary device that would not be classified as a BES Cyber Asset. The standard drafting team determined that 30 days was the appropriate cut-off, concluding that when a device is connected for longer than 30-days it reaches the point where it should be subject to the requirements applicable to BES Cyber Assets.[48]

b. Control Center

[48] Because the proposed CIP Version 5 Reliability Standards address the risks associated with the connection of temporary devices, concerns regarding circumvention of the CIP 5 Reliability Standards by briefly disconnecting assets regularly used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes in order to restart the 30-day qualification period is unfounded. Even if an entity did take such action, the proposed CIP Reliability Standards still require entities to protect their BES Cyber Assets from any risks associated with the connection of removable media. The definition intentionally does not prescribe how to document that an asset has been connected to the Bulk Electric System for less than 30 days. The facts and circumstances of how the entity maintains its documentation will need to be examined to determine whether the definition has been properly applied.

NERC proposes to define "Control Center" as:

> One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

The Commission seeks comments "on the meaning of the phrase 'generation Facilities at two or more locations' and, specifically, whether the phrase includes two or more units at one generation plant and/or two or more geographically dispersed units."[49]

The phrase "generation Facilities at two or more locations" refers to two or more geographically dispersed generation plants, not two or more units at one generation plant.[50]

c. Cyber Assets

NERC proposes to define "Cyber Assets" as '[p]rogrammable electronic devices, including the hardware, software, and data in those devices." The Commission notes that NERC's proposed definition of Cyber Assets differs from the current definition of that term in the NERC Glossary because the proposed definition does not specifically include "communication networks" as a Cyber Asset.[51] The Commission further notes that the Federal Power Act ("FPA") defines "cybersecurity incident" to include events that disrupt the operation of communication networks.[52] The Commission seeks (i) an explanation of the purpose and intended effect of removing "communication networks" from the proposed definition; and (ii)

---

49 NOPR at P 80.

50 *See* NERC Petition, Ex. D, Consideration of Comments on Draft 4 of CIP Version 5 at 22.

51 NOPR at P 81. NERC's currently-effective Glossary defines Cyber Asset as "[p]rogrammable electronic devices and communication networks including hardware, software, and data."

52 *Id*. (citing 16 U.S.C. 824o(a)(8)).

whether the removal of "communication networks" could create a gap in cyber security and the proposed CIP Reliability Standards.[53]

Additionally, the Commission seeks comment on the purpose and intended effect of the phrase "data in those devices;" in particular, whether the phrase excludes data being transferred between devices.[54]

The standard drafting team removed the term "communication network" from the definition of Cyber Asset to provide clarification as to the appropriate target of the requirements applicable to BES Cyber Assets (*i.e.*, what assets the requirements intended to protect). The standard drafting team sought to clarify that the BES Cyber Assets are those electronic devices that are capable of executing a set of instructions (*i.e.*, programmable devices).[55] That is because programmable electronic devices are the key assets susceptible to a cyber attack, such as the introduction of malicious code. The standard drafting team did not intend to exclude all components of a communication network from the definition of Cyber Asset, only non-programmable components. So long as a component of a communication network is programmable (*e.g.*, routers and switches), that component would be a Cyber Asset under the revised definition.

While the drafting team recognizes that it is important to protect non-programmable devices, the standard drafting team concluded that it was not appropriate for non-programmable devices to be included in the definition of BES Cyber Asset, particularly in light of the obligations imposed on responsible entities for protecting BES Cyber Assets under the proposed

---

53 *Id.* at P 82.

54 *Id.*

55 Note that at the time the definition was developed, the Commission had not yet issued an order in Docket No. RD12-3 remanding NERC's interpretation of "communication network." *N. Am. Elec. Reliability Corp.*, 142 FERC ¶ 61,203 (2013).

CIP Reliability Standards. Many of these obligations are tailored to programmable electronic devices and are not appropriate if applied to non-programmable devices, such as a network cable. For instance, CIP-007, Requirement R3 obligates responsible entities to deploy methods, such as the installation of antivirus software, to deter, detect, or prevent malicious code. This requirement has no application in relation to a cable. To avoid confusion in the implementation of such requirements, the standard drafting team determined that the broad term "communication network" should be removed from the definition of Cyber Asset.

NERC notes that the definition of "cybersecurity incident" in the FPA and the definition of Cyber Asset in NERC's glossary have different purposes. Removing communication networks from the definition of BES Cyber Asset does not mean that a "cybersecurity incident" could not be caused by a disruption of a communication medium connected to a programmable electronic device. Interference with non-programmable devices in a communication network could impact the reliability of a BES Cyber System and be considered a "cybersecurity incident," as defined in the FPA and in the NERC Glossary.[56] NERC notes that CIP-008-5 requires responsible entities to mitigate the risk to the reliable operation of the Bulk Electric System from cyber security incidents by implementing incident response requirements. NERC expects that any incident response plan adopted pursuant to CIP-008-5 would include a plan for responding to interference with communication devices that could result in a cyber security incident.

With respect to the phrase "data in those devices," the drafting team distinguished between data at rest (*e.g.*, data stored on a hard drive) and data in motion (*e.g.*, data being transferred between programmable electronic devices, wirelessly or through a network cable).

[56] The NERC Glossary defines a Cyber Security Incident as a malicious act or suspicious event that (i) compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or (ii) disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. A Reportable Cyber Security Incident is defined as a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

The drafting team concluded that the definition of BES Cyber Asset should include data stored in programmable electronic devices to clarify that the protections afforded to BES Cyber Assets extends to the data stored in those devices.

d. Reliability Tasks

In the NOPR, the Commission notes that the term "reliability tasks" is an undefined term in NERC's proposed definitions of BES Cyber System, Control Center, and Reportable Cyber Security Incident. Due to its concern that the use of the undefined term could lead to confusion during implementation and result in interpretation requests, the Commission is seeking comment on the meaning and scope of the phrase "reliability tasks" and whether there is a common understanding of this phrase to assure accurate and consistent implementation of the definitions and the proposed CIP Version 5 Reliability Standards.[57]

The drafting team determined that it was not necessary to separately define the phrase "reliability tasks" in the NERC Glossary because it is a commonly understood phrase from NERC's Reliability Functional Model,[58] which provides the framework for the development and applicability of NERC's Reliability Standards. The Reliability Functional Model reviews the tasks required for maintaining electric system reliability and organizes these tasks into basic groups, called "Functions."[59] Each Function thus consists of a set of related "reliability tasks." The Reliability Functional Model then assigns each Function to a functional entity, that is, the entity that performs the Function. The Reliability Functional Model describes in general terms each Function, the reliability Tasks related to that Function and the relationships between the

---

[57] NOPR at P 84.

[58] The NERC Reliability Functional Model is available at http://www.nerc.com/pa/Stand/Pages/FunctionalModel.aspx.

[59] The Reliability Functional Model defines the term "Function" as "[a] set of related reliability Tasks." "Task" is defined as [o]ne of the elements that make up a Function in the Functional Model."

functional entities that are responsible for performing the Tasks within the Function. Drafting teams use the Reliability Functional Model to help them determine which functional entity should be required to comply with each requirement in a Reliability Standard.[60]

Because the phrase "reliability tasks" is commonly understood to refer to the set of tasks applicable to a particular reliability Function in the Reliability Functional Model, the use of such phrase in the definitions of BES Cyber System, Control Center, and Reportable Cyber Security Incident should not cause confusion in implementation or result in interpretation requests. Because each reference to the term "reliability task" in the NERC Glossary is connected to the role of a functional entity, it is clear that the meaning of the term "reliability task" in the NERC Glossary is the same commonly understood meaning of that term in the NERC Reliability Functional Model.

e. Intermediate Devices

NERC's proposed definitions for Electronic Access Control or Monitoring Systems ("EACMS") and Interactive Remote Access include the undefined term "intermediate devices." The Commission notes that in previous draft versions of the proposed CIP Version 5 Reliability Standards, the proposed defined term "Intermediate Systems" was originally referred to as "Intermediate Device."[61] The Commission is seeking comment on whether the proposed defined term "Intermediate Systems" is the appropriate reference in the proposed definitions of EACMS and Interactive Remote Access.[62]

---

60 Drafting teams assign each reliability requirement within a Reliability Standard to a functional entity. These assignments work because a given Reliability Standard requirement will correspond to a reliability Task within a Function. While a Reliability Standard requirement will be very specific, a reliability Task in the Reliability Functional Model is more general in nature.

61 NOPR at P 85.

62 *Id*. at P 86.

NERC clarifies that "Intermediate Systems," not "Intermediate Devices," is the appropriate reference in the proposed definitions of EACMS and Interactive Remote Access. As the Commission notes, during the course of drafting CIP Version 5, the defined term "Intermediate Systems" was originally referred to as "Intermediate Device." Although the standard drafting team intended to make this a universal change, due to an oversight the term "Intermediate Device" was not changed to "Intermediate Systems" in the proposed definitions of EACMS and Interactive Remote Access. Going forward, those definitions should be revised to use the term "Intermediate Systems." NERC will make the necessary errata change for Commission approval.

V. Implementation Plan

NERC proposes an implementation plan for the proposed CIP Version 5 Reliability Standards that addresses two issues. First, NERC proposes to transition from CIP Version 3 to the proposed CIP Version 5, bypassing implementation of CIP Version 4, so as to alleviate uncertainty as to whether entities would have to move to CIP Version 4 on April 1, 2014, the effective date for CIP Version 4, before the effective date for proposed CIP Version 5. Second, NERC proposes to provide for a 24-month implementation period for High Impact and Medium Impact BES Cyber Systems, and a 36-month implementation period for Low Impact BES Cyber Systems.

The Commission proposes to approve NERC's proposal to allow responsible entities to transition from compliance with the currently-effective CIP Version 3 Standards to compliance with the proposed CIP Version 5 Reliability Standards.[63] However, the Commission seeks comment on whether the implementation periods proposed by NERC for the proposed CIP

[63] *Id*. at P 89.

Version 5 Reliability Standards are necessary.[64] Specifically, the Commission seeks comment on: (i) the activities that responsible entities will have to undertake to achieve timely compliance with the proposed CIP Version 5 Reliability Standards; (ii) whether responsible entities can achieve compliance with the proposed CIP Version 5 Reliability Standards in a shorter period for those Cyber Assets that responsible entities have identified to comply with the currently-effective CIP Reliability Standards; and (iii) the feasibility of a shorter implementation period and the reasonable time frame for a shorter implementation period.

NERC continues to support the proposed implementation plan developed by the standard drafting team and supported by both the industry and the NERC Board of Trustees. Bypassing CIP Version 4 allows entities to devote the necessary resources and attention to implement the improved set of cyber security controls in proposed CIP Version 5. It also allows the ERO to devote resources to the CIP Version 3 to CIP Version 5 transition without an additional step with CIP Version 4.

Additionally, the implementation periods properly balance the urgency to implement the improved standards with the time needed for entities to develop the necessary procedures, software, facilities, staffing or other relevant capabilities. As stated in NERC's Petition, "[w]hile the general framework of the proposed standards follow the organization of the previous CIP versions…NERC and its stakeholders have proposed the most comprehensive set of mandatory cybersecurity standards ever utilized on a widespread basis in the electric industry."[65]

a. Implementation Periods

The implementation periods were designed to reflect the time it will take responsible entities to implement the changes proposed in CIP Version 5. The implementation periods were

64 *Id.*

65 Petition at 5.

developed by experts in the field with firsthand knowledge of what would be required for their organizations and other organizations to comply with the proposed CIP Version 5 Reliability Standards. The implementation plan was also vetted with industry through the Reliability Standards development process.

The 24-month and 36-month periods provide sufficient time for entities to take the necessary steps to become compliant with the proposed CIP Version 5 Reliability Standards. While there are similarities between the prior versions of the CIP Reliability Standards, proposed CIP Version 5 will require entities to change their processes and procedures to match the revised requirements and the technical controls in proposed CIP Version 5. Entities will also need time to retrain employees during the implementation period after their new processes and procedures are developed. Additionally, with the addition of non-routable assets, the assets covered by proposed CIP Version 5 would be significantly more than those assets covered by all previous versions. While some entities may be closer to compliance with proposed CIP Version 5 than others, the implementation periods need to cover all responsible entities.

The 24-month implementation period for "High Impact" and "Medium Impact" BES Cyber Systems appropriately balances the desire to implement the improvements in proposed CIP Version 5 as expeditiously as possible for those assets with the greatest impact on reliability while also providing entities sufficient time to establish and modify their various procedures to become fully compliant by the end of the 24-month implementation period. Further, as noted above, because non-routable assets are now included, there would be significantly more assets that we be categorized as High or Medium Impact.[66] Entities will need time develop and implement policies for these assets.

[66] The drafting team estimates that approximately twice as many assets will be categorized as High or Medium Impact.

The 36-month implementation period for "Low Impact" BES Cyber Systems is necessary because this category will cover many assets that were previously not covered by prior versions of the CIP Reliability Standards. Also, with the inclusion of Low Impact assets, many entities that had never been subject to the CIP Reliability Standards now have assets subject to these Reliability Standards. Three years of implementation for "Low Impact" BES Cyber Systems is thus necessary to provide entities sufficient time to formulate and implement effective security solutions for physical and electronic perimeter protection for these newly covered assets, while simultaneously implementing the proposed CIP Version 5 standards for "High Impact" and "Medium Impact" BES Cyber Systems during the first 24 months. This implementation period appropriately focuses entities on the protection of the "High Impact" and "Medium Impact" BES Cyber Systems during the initial months of the implementation period.

NERC also notes that budget cycles and budget approval timelines could present challenges to entities in addition to technical challenges presented by the implementation of the proposed CIP Reliability Standards. For some entities, the budget process may include review and approval by a state public utility commission or another third-party entity. For Regional Transmission Organizations and Independent System Operators, the budget process might include review by their members requiring additional time to obtain necessary budget approvals. The standard drafting team sought to ensure that the implementation periods accounted for such challenges.

NERC further notes that the end of the implementation periods represent the time that entities must be in *full* compliance with the proposed CIP Version 5 Reliability Standards. Thus, many entities will need to begin transitioning to proposed CIP Version 5 before the end of the implementation periods. The implementation plan contemplates that entities will begin

transitioning to proposed CIP Version 5 prior to the effective date. For instance, the implementation plan provides certain initial performance expectations[67] that on or before the effective date of proposed CIP Version 5, the responsible entities must comply initially with certain periodic requirements including CIP-002-5, Requirement R2 and CIP-003-5, Requirement R1. For proposed CIP-002-5, Requirement R2, the proposed implementation plan requires entities to have reviewed their identification and categorization of BES Cyber Systems and their associated BES Cyber Assets prior to the effective date and have their CIP Senior Manager (or his/her designee) approve the identifications. For CIP-003-5, Requirement R1, the proposed implementation plan requires entities to demonstrate that the CIP Senior Manager has reviewed and approved the entities' documented cyber security policies for its High Impact and Medium Impact BES Cyber Systems. Further, by the effective date of proposed CIP-003-5, entities must implement one or more documented cyber security policies for Low Impact BES Cyber Systems that has been reviewed and approved by a CIP Senior Manager.

b. NERC Transition Guidance and Pilot Program

NERC supports the Commission's goal of encouraging early transition to the improvements in proposed CIP Version 5. To that end, NERC is working with the Regional Entities and industry to develop ways to encourage entities that are able to comply with proposed CIP Version 5 in a shorter timeframe than contemplated by the implementation plan to do so, while preserving the full implementation period for those entities that may need more substantial changes to their programs to meet the proposed CIP Version 5 requirements. In addition to transition guidance that NERC will issue on how entities should transition from CIP Version 3 to CIP Version 5, NERC and the Regional Entities are working to develop a pilot program that will

[67] *See* NERC Petition, Ex. B at 2.

analyze how a select number of entities implement proposed CIP Version 5 prior to the proposed effective date with support and review by NERC and the applicable Regional Entities. As to the participants in the pilot program, NERC will seek to include entities that have both a strong compliance program and the ability to transition to CIP Version 5 in a short timeframe.

The pilot program will be designed to help identify best practices and lessons learned for transitioning from CIP Version 3 to CIP Version 5. This pilot program will provide valuable feedback during the implementation periods that would then be shared broadly with industry to help facilitate a transition for all entities in a cost-effective, efficient, and timely manner. The proposed implementation periods are thus necessary to allow NERC to develop and execute the pilot program, learn from the pilot participants' implementation of CIP Version 5, and disseminate the best practices and lessons learned to assist all entities in making an effective transition from CIP Version 3 to CIP Version 5.

In addition, the pilot program will allow the Regional Entities and NERC to make adjustments in their systems and approach to compliance with proposed CIP Version 5 while obtaining experience with entities in transition. In particular, this information will inform whether and how NERC may adjust its RSAWs.

NERC intends to submit an informational filing to the Commission in this docket detailing the pilot program after the issuance of a final rule in this proceeding. Regardless of the ultimate program design, this approach would be consistent with the proposed CIP Version 5 implementation plan. NERC will also engage Commission staff informally during the transition period to inform the Commission of progress and elicit feedback from Commission staff.

VI. Violation Risk Factor and Violation Severity Level Assignments

The Commission proposes to accept 30 of the 32 proposed VRFs and direct NERC to develop modifications to two VRFs.[68] Specifically, the Commission proposes to direct NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, and to modify the VRF assigned to CIP-004-5, Requirement R4 from Lower to Medium.[69] In addition, the Commission proposes to direct NERC to modify certain Violation Severity Levels ("VSL") in proposed CIP Version 5.

a. VRF for CIP-006-5, Requirement R3

NERC proposed a Lower VRF for CIP-006-5, Requirement R3, which addresses the maintenance and testing of Physical Access Control Systems. The Commission notes that the NERC mapping document comparing CIP Version 4 and proposed CIP Version 5 identifies CIP-006-4, Requirement R8, which addresses the maintenance and testing of all physical security mechanisms, as the comparable requirement to CIP-006-5, Requirement R3. CIP-006-4, Requirement R8 is assigned a Medium VRF. The Commission proposes to direct NERC to modify the VRF for CIP-006-5 to Medium.

The Commission should approve the Lower VRF for CIP-006-5, Requirement R3 because it appropriately reflects the reduced reliability risk in CIP-006-5, Requirement R3 as compared to CIP-006-4, Requirement R8. Specifically, CIP-006-4, Requirement R8 required "[t]esting and maintenance period of all physical security mechanisms on a cycle no longer than three years." CIP-006-5 now requires maintenance and testing "at least once every 24 calendar months." Because maintenance and testing of Physical Access Control Systems will occur more

[68] NOPR at P 91.

[69] *Id*. at PP 92-99.

frequently pursuant to proposed CIP Version 5, the reliability risk is reduced and a Lower VRF is appropriate.

b. VRF for CIP-004-5, Requirement R4

NERC proposed a Lower VRF for CIP-004-5, Requirement R4, which relates to access management programs addressing electronic access, unescorted physical access, and access to BES Cyber System Information.[70] In the NOPR, the Commission states that Recommendations 40[71] and 44[72] of the *U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* ("Blackout Report")[73] support assigning access management programs – such as those required under CIP-004-5, Requirement R4 – a Medium VRF.

Additionally, the Commission notes that NERC's proposal to assign a Medium VRF to CIP-004-5, Requirement R5, which addresses access revocation, results in a potential inconsistency between VRFs within CIP-004-5. The Commission states that access authorization, addressed in CIP-004-5, Requirement R4, is the companion to access revocation, addressed in CIP-004-5, Requirement R5, and proposes to direct NERC to modify the VRF for CIP-004-5, Requirement R4, to be consistent with CIP-004-5, Requirement R5.

The Commission should not direct NERC to modify the VRF for CIP-004-5, Requirement R4. In developing the VRF for CIP-004-5, Requirement R4, the drafting team

---

[70] Requirement R4 obligates a responsible entity to have a process for authorizing access to BES Cyber System Information, including periodic verification that users and accounts are authorized and necessary.

[71] Recommendation 40 of the Blackout Report states that access to operationally sensitive computer equipment should be "strictly limited to employees or contractors who utilize said equipment as part of their job responsibilities."

[72] Recommendation 44 of the Blackout Report states that entities should "develop procedures to prevent or mitigate inappropriate disclosure of information."

[73] The Blackout Report is available at http://www.ferc.gov/industries/electric/indus-act/reliability/blackout.asp.

adopted the Lower VRF used in CIP-003-4, Requirement R5, which is the comparable requirement from CIP Version 4, to provide for consistency. The standard drafting team concluded that because Requirement R4 is largely administrative and violations of the requirements do not pose a significant risk to the Bulk Electric System, a Lower VRF was still appropriate. In contrast, the drafting team concluded that a Medium VRF was appropriate to reflect the greater risk to the Bulk Electric System in the event of a failure to revoke access. The standard drafting team determined that failure to revoke access following termination of an employee, for instance, presents a greater risk to reliability and concluded, in turn, that a Medium VRF was appropriate for access revocation.

c. Violation Severity Level Assignments

As noted above, the Commission proposes to direct NERC to modify certain VSLs in proposed CIP Version 5. The Commission states that the VSL gradations for the following requirements are inconsistent with the Commission's VSL guidelines because the assignments are based on a cumulative number of violations rather than a single violation:[74] CIP-003-5, Requirement R3; CIP-003-5, Requirement R4; CIP-004-5, Requirement R1; CIP-007-5, Requirement R4.4; CIP-007-5, Requirement R5; and CIP-009-5, Requirement R3.

The Commission also notes that certain VSLs are unclear or contain typographical errors.[75] Lastly, the Commission stated that it may direct modifications to the VSLs that include the terms "identify," "assess," "correct," and "deficiencies" based on the comments it receives on that language.[76]

---

[74] NOPR at P 101.

[75] The Commission stated that the requirements that raise concerns in this respect are: CIP-004-5, Requirement R4.2 CIP-003-5, Requirements R1, R2, R3; CIP-007-5, Requirement R5; CIP-008-5, Requirements R2, R3; CIP-009-5, Requirements R2, R3.

[76] *Id*. at P 103.

With respect to the cumulative violations issue, a review of each VSL assignment that the Commission cites as an instance where the VSL assignment is based on cumulative violations reveals that the drafting team did in fact base the assignment on a single violation, consistent with Commission precedent.[77] Specifically, in each such instance, the requirement obligates the responsible entity to take certain action within a specific time period. In developing the proposed VSLs for these requirements, the drafting team based its VSL assignment on how much time had passed before the responsible entity complied with the requirement, if ever, not the number of violations.[78]

The following is a discussion of each instance in which the Commission raises a concern that the VSL assignment is based on cumulative violations:

CIP-003-5, Requirement R3. CIP-003-5, Requirement R3 requires that responsible entities "identify a CIP Senior Manager by name and document any change within 30 calendar days of the change." A Lower VSL is assigned where an entity violates the requirement by failing to document the change within the 30-day window but does so within 40 days. A Medium VSL is assigned where the entity fails to document the change within the 30-day window but does so within 50 days. A High VSL is assigned where the entity fails to document the change within the 30-day window but does so within 60 days and a Severe VSL is assigned where the responsible entity has not identified a CIP Senior Manager or where the entity fails to document a change within 60 days. Failing to document the change within 40, 50 or 60 days

---

77 *N. Am. Elec. Reliability Corp.*, 123 FERC ¶ 61,284 ("Violation Severity Level Order"), *order on reh'g*, 125 FERC ¶ 61,212 (2008).

78 These VSL assignments are thus distinct from the case the Commission discusses in the Violation Severity Level Order. That case involved the VSL assignment for Reliability Standard IRO-004-1, Requirement R6, which requires a Reliability Coordinator to direct entities to address potential system operating limit violations. NERC's proposed VSL assignments for that requirement were based on the number of occasions during a calendar month that a Reliability Coordinator did not direct its required entities to address those potential violations. As discussed below, none of the VSL assignments for CIP Version 5 are based on the number of violations.

does not create two separate violations. Rather, the failure to document the change within 30 days remains a single violation no matter how long it takes for an entity to comply. The proposed VSL simply acknowledges that the severity level should increase the longer it takes for an entity to document the change. Additionally, failure to identify a CIP Senior Manager in the first instance is also a single violation. Thus, the VSL assignment for CIP-003-5, Requirement R3 is not based on cumulative violations.

CIP-003-5, Requirement R4. The VSL assignment for CIP-003, Requirement R4 works in a similar fashion to the VSL assignment for CIP-003-5, Requirement R3. Requirement R4 requires responsible entities to implement – in a manner that identifies, assesses, and corrects deficiencies – a documented process to delegate authority. Further, any delegations must be documented and such documentation must be updated within 30 days of any change to the delegation. A Lower VSL is assigned to a single instance where the responsible entity has properly identified a delegation but fails to document a change to a delegation within the 30-day window but does so within 40 days. The severity increases to a Medium VSL where the change is not documented until sometime between 41 and 50 days. A High VSL is assigned where the responsible entity either: (1) fails to correct identified deficiencies in its delegation process; (2) fails to identify, assess or correct deficiencies, or (3) fails to document a change within 50 calendar days. The VSL increases to Severe where the responsible entity does not have a process for delegation or fails to document a change within 60 calendar days.

The Commission states that the proposed VSL for this requirement is based upon the number of incorrect delegations. This appears to be a misunderstanding of the proposed VSL. None of the severity levels are based on more than one violation. Failure to take required action (in this case updating documentation of a delegation) within a specified time is a single violation,

the severity of which increases based on the amount of time before the required action is eventually taken, if ever. If a responsible entity failed to update the documentation for two different delegations, that would be two distinct violations subject to different VSLs. Also, the failure to have a process for delegation or to implement such a process in a manner that identifies, assesses, and corrects deficiencies is a single violation.

CIP-004-5, Requirement R1. The proposed VSL for CIP-004-5, Requirement R1 is also based on the amount of time the entity was non-compliant, not the number of violations. CIP-004-5, Requirement R1 requires entities to implement a documented process for security awareness that, at least once a calendar quarter, reinforces cyber security practices. A Lower VSL is assigned where the responsible entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the next quarter. A Medium VSL is assigned where the reinforcement did not occur until 30 days after the start of the subsequent quarter and a High VSL is assigned if the reinforcement occurred within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. A Severe VSL is assigned where the entity did not document or implement any process or did not reinforce cyber security practices for as long as two consecutive quarters. The standard drafting team views the failure to reinforce cyber security practices over a period of time longer than one quarter as a single violation of Requirement R1, the severity of which is informed by the length of time the entity has not reinforced its cyber security practices.

CIP-007-5, Requirement R4, Part 4.4. For proposed CIP-007-5, Requirement R4.4, which requires entities to "review a summation or sampling of logged events … at no greater than 15 days," the Commission notes that the High VSL gradation states that an entity must miss "two or more intervals" (i.e., 30 days) for the violation to reach High severity over the specified

time period. Similar to the calendar quarter interval in the VSL assignment for CIP-004-5, Requirement R1, the failure to review a summation or sampling of logged events over a period of time greater than 15 days is a single violation, the severity of which is informed by the length of time before such summaries are reviewed.

CIP-007-5, Requirement R5. CIP-007-5, Requirement R5 requires responsible entities to implement, in a manner that identifies, assesses, and corrects deficiencies, documented processes for system access controls. Although not entirely clear, it appears that the Commission's concern relates to the VSL assignment for Part 5.6 of Requirement R5. Part 5.6 states that "for password-only authentication for interactive user access," entities "either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months." The proposed VSL for Part 5.6 is as follows: (1) a Lower VSL is assigned when the entity did not enforce the obligation to change the password within 15 months but did so in 16 months; (2) a Medium VSL is assigned where the obligation to change the password was not enforced within 16 months but was enforced within 17 months; (3) a High VSL is assigned where the obligation to change the password was not enforced within 17 months but was enforced within 18 month; and (4) a Severe VSL is assigned where the obligation to change password was not within 18 months. Again, the proposed VSL assignment is not based on cumulative violations but on the length of time that the entity was non-compliant. The other VSL assignments for the other parts of Requirement R5 relate to a failure to identify, assess or correct a deficiency or, if a deficiency was identified, the failure to assess and correct that deficiency. The standard drafting team considers a failure to identify, assess, and correct a deficiency as a single violation.

CIP-009-5, Requirement R3. Like those discussed above, CIP-009-5, Requirement R3, which addresses the maintenance of recovery plans, requires a responsible entity to take certain actions within a specific time frame after a triggering event.[79] The VSL assignments are not based on the number of times that the entity failed to take the required action, but the lapse in time following the triggering event before that action was taken, if ever. As explained above, this constitutes a single violation.

For the VSLs that are unclear and/or contain typographical errors, NERC will make the necessary errata change for Commission approval. Finally, in the event that the Commission directs changes to the "identify, assess, and correct" language in the proposed CIP Version 5 Reliability Standards, NERC will undertake the necessary revisions to the VSLs as well as to ensure that the VSL Guidelines are met.

VII. Other Technical Concerns

While proposing to approve proposed CIP Version 5, the Commission also seeks comments on three general areas that the Commission states could enhance cyber security protection: (1) communications security; (2) remote access; and (3) differences between CIP Version 5 and the NIST Risk Management Framework.[80] Based on the comments it receives, the Commission states that it may direct NERC to develop modifications to certain aspects of the CIP Reliability Standards or, in the alternative, consider these issues in preparing the next version of CIP Standards.[81]

---

[79] Part 3.1 of Requirement R3 requires entities to take certain action (e.g., document lessons learned) within 90 days after the completion of a recovery plan test or actual recovery. Part 3.2 of Requirement R3 requires entities to take certain action (e.g., update the recovery plan) within 60 days of a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan.

[80] NOPR at P 105.

[81] *Id.*

As discussed below, the initial step for considering these areas should be through a Commission and/or NERC-sponsored technical conference, as opposed to a Commission directive in a final rule in this proceeding. Because the three areas involve significant technical considerations, a technical conference would provide the appropriate forum to begin discussing these issues. A directive to modify the proposed CIP Version 5 Reliability Standards could threaten timely implementation of the proposed CIP Version 5 Reliability Standards and the improvements therein if further work in the Reliability Standards development process is necessary.

a. Communication Security

The Commission has invited comments on whether the adoption of communication security protections, namely cryptography and protections for non-routable protocols, would improve the CIP Reliability Standards.

Additionally, the Commission expressed concern related to NERC's proposal to exempt communication networks from protection based solely on specific types of technology.[82] While proposed CIP-002-5 removes the prior blanket exemption for non-routable protocol, the Commission seeks comment regarding whether the resulting proposed Reliability Standards adequately protect non-routable communication systems.[83] The Commission maintains that limiting the CIP protections to only routable systems adds additional risk to the Bulk Electric System.[84] Lastly, the Commission is concerned that by "effectively locking the CIP Reliability

82 *Id*. at P 108.

83 *Id*.

84 *Id*.

Standards into a specific technology…any future technology which is non-routable in nature will not be addressed by the CIP Reliability Standards."[85]

i. Cryptography

As the Commission notes, the proposed CIP Version 5 Reliability Standards already require cryptography for interactive remote access.[86] The standard drafting team concluded that requiring cryptography in that instance is appropriate because the reliability benefits were well understood and the use of cryptography would not degrade reliability. NERC has concerns, however, with mandating a broader application of cryptography in the CIP Reliability Standards at this time. Although the selective incorporation of cryptography may improve cyber security in specific instances, there are a number of unanswered questions on the reliability impact of cryptography, where cryptography could be used to benefit reliability, where cryptography has the potential to adversely impact reliable operations and how to measure its impact. A broader application of cryptography in the CIP Reliability Standards would benefit from further evaluation by NERC and the industry through technical conference that address these questions.

Among other things, NERC has concerns that the use of cryptology could result in: (1) delays in the timeliness of communications necessary for reliable operation of the Bulk Electric System; (2) the obfuscation of data for testing and diagnosis; and (3) additional communication errors due to complex implementations of cryptography, as discussed below.

With respect to the delay issue, the Department of Homeland Security's ("DHS") *Catalog of Control Systems Security: Recommendations for Standards Developers* warns that the use of cryptography within a control system may introduce latency to control system

---

85 *Id.*

86 *See* NOPR at P 107, fn. 98. Proposed CIP-005-5, Requirement R2, for instance, requires responsible entities to use an Intermediate System, use encryption that terminates at an Intermediate System, and implement multi-factor authentication for all Interactive Remote Access sessions associated with high and medium impact BES Cyber Systems that allow Interactive Remote Access.

communication that could impact reliable operations.[87] Many data collection and control processes used throughout the Bulk Electric System must be completed in a very short time period to provide for reliable operation.[88] The use of cryptography has the potential to introduce delays that may prevent such processes from happening within the requisite time period. Additional analysis is required to ensure that the latency introduced from the use of cryptographic technology would not degrade the operational performance of the control system or impact personnel safety.

NERC is also concerned that the use of cryptography could make it more difficult for utilities to conduct field testing and diagnosis because the use of cryptography may conceal the data collected for testing and diagnosis from other systems, which could result in reliability issues.

Relatedly, NERC has concerns that the use of complex implementations of cryptography could cause additional communication errors. Additional study is needed to ensure that the technology used to implement cryptography is effective and could be implemented in a manner that does not adversely affect the communication necessary for reliable operation of the Bulk Electric System

Given these concerns, and consistent with the DHS Catalog of Control Systems Security, cryptography needs to be evaluated on a case-by-case basis. A technical conference would provide the appropriate forum to begin discussing these issues.

---

[87] DHS Catalog of Control Systems Security, *available at* http://ics-cert.us-cert.gov/sites/default/files/CatalogofRecommendationsVer7.pdf.

[88] For instance, many data collection and control processes for sets of field devices rely on very tight time windows to complete polling and control cycles.

ii. Non-routable Protocols

With respect to the Commission's concern regarding protections for non-routable protocol, proposed CIP Version 5 takes an important step to better protect non-routable protocol. As the Commission notes, prior versions of the CIP Reliability Standards excluded all non-routable protocol from protection. The requirements in proposed CIP Version 5 now apply to both routable and non-routable protocol, unless specifically excluded. Although there are certain requirements in proposed CIP Version 5 that apply only to systems with External Routable Connectivity, that limitation generally applies to requirements that either require or can take advantage of the high speed connections that are typically associated with routable connectivity. To the extent that implementation experience indicates a need for additional protections for non-routable technologies, NERC looks forward to working with the industry on these issues through the Reliability Standards development process.

b. Remote Access

The Commission expressed concern that the flexibility provided by remote access also "creates new security risks by allowing a potentially unsecured device access into an entity's network."[89] The Commission states that because "the communication network used for remote access is a pathway that can be used to spread malware, the secure implementation of remote access is another step in protecting the confidentiality, integrity, and availability of the data and functions used to support the reliable operation of the bulk electric system."[90] The Commission notes that a number of organizations, including NERC, have developed guidance documents for securing remote access connections.[91] While the Commission notes that some of this guidance is

89 NOPR at PP 110-11.

90 *Id*. at P 111.

91 *Id*. at P 112.

reflected in the proposed CIP Version 5 Reliability Standards, the Commission asserts that the controls adopted in proposed CIP Version 5 are not as stringent as those in the guidance documents or the controls required under the NIST Risk Management Framework.[92] The Commission seeks comment on whether the adoption of more stringent controls for remote access would improve the CIP Reliability Standards.

In developing proposed CIP Version 5, the standard drafting team focused on adopting those protections applicable to remote access that are auditable and enforceable for purposes of mandatory Reliability Standards, as opposed to a guidance document, which could recommend different and, in some cases, more stringent types of controls. Proposed CIP Version 5 includes a number of significant protections for remote access. For example, proposed CIP-004-5, Requirement R4, Part 4.1, requires responsible entities to implement an authorization process for electronic access to ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored have been properly authorized for such access. This requirement includes all types of electronic access, including remote access. The Rationale section of proposed CIP-004-5, Requirement R4 explains:

> Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

Proposed CIP-004-5, Requirement R5 addresses remote access revocation.

Further, as the Commission notes, proposed CIP-005-5, Requirement R2 requires responsible entities to use an Intermediate System, use encryption that terminates at an Intermediate System, and implement multi-factor authentication for all Interactive Remote

---

92 *Id*. at P 113.

Access sessions associated with high and medium impact BES Cyber Systems that allow Interactive Remote Access. The Commission states that this requirement is not as stringent as the recommendations in NERC's advisory or the controls provided in the NIST Risk Management Framework because both the NIST Risk Management Framework and NERC's advisory recommend authorization for each individual, person or system, granted remote access. NERC notes, however, that proposed CIP-004-5, Requirement R4, Part 4.1, described above, requires electronic authorization for each individual and CIP-005-5, Requirement R1, Part 1.3 covers access permission justifications applicable to systems.

To the extent that implementation experience indicates a need for additional protections for remote access, NERC looks forward to working with the industry on these issues through the Reliability Standards development process.

c. Differences Between CIP and the NIST Risk Management Framework

Lastly, the Commission invites comment on whether, and in what way, adoption of certain aspects of the NIST Risk Management Framework could improve the security controls proposed in CIP Version 5.[93] The Commission states that "[i]t appears that the CIP version 5 Standards do not address certain aspects of cyber security in as comprehensive a manner as the NIST Risk Management Framework addresses the same topics." In the NOPR, the Commission provides examples of such instances. Although the Commission is not proposing to direct NERC to address these instances at this time, the Commission is inviting comments on this issue.

NERC supports the Commission's proposal not to direct changes at this time. The proposed CIP Version 5 Reliability Standards generally cover the same subject areas as the NIST

[93] NOPR at PP 114-17.

Framework, along with the standards that the NIST Framework also references.[94] As noted in NERC's petition, proposed CIP Version 5 includes NIST Framework concepts such as:

1) ensuring that all BES Cyber Systems, based on their function, receive some level of protection;

2) using a tiered approach to security controls, which specifies the level of protection appropriate for BES Cyber Systems based on their importance to the reliable operation of the BPS;

3) tailoring protection to the mission and operating environment of the cyber systems subject to protection;

4) defining the concept of the BPS cyber system; and

5) including "Assess" and "Monitor" steps by adding requirement language for "identifying, assessing, and correcting" deficiencies in controls as part of the requirements' expected performance.

The CIP Reliability Standards have been mapped against the existing NIST Framework, as expressed in NIST Special Publication 800-53,[95] and the technical requirements of both sets of standards largely address the same areas. The DHS Control Systems Security Program developed one example of a mapping document in 2009. The area where the NIST Framework does not overlap is in the reporting and administrative areas (*e.g.*, certification and accreditation), which are not required in the civilian private sector. Reliability Standards generally address these areas via the NERC compliance and audit program.

Because the CIP Reliability Standards and the NIST Framework substantially cover the same areas, NERC suggests that NERC hold a technical conference to discuss any remaining differences between the CIP Reliability Standards and the NIST Framework and determine

---

94 *See* NERC's responses to the NIST's notice and request for information on *"Developing a Framework to Improve Critical Infrastructure Cybersecurity"* (Docket No. 130208119–3119–01), 78 Fed. Reg. 13,024 (Feb. 26, 2013), *available at* http://csrc.nist.gov/cyberframework/rfi_comments.html.

95 NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, updated May 1, 2010, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

whether any of the remaining areas are appropriate for inclusion in the CIP Reliability Standards. Whether to incorporate additional elements should be further discussed in a technical forum and include industry, NERC, and Commission staff. The CIP Reliability Standards have been in a constant state of revision over multiple versions of the Reliability Standards and time is needed for entities to focus on the proposed CIP Version 5 implementation prior to the addition of additional controls. NERC supports allowing the implementation of proposed CIP Version 5 without modification.

The following examples of controls provided for in the NIST Framework illustrate that some of the areas cited by the Commission will be covered by, or have affect on, the proposed CIP Version 5 Reliability Standards:

- Control MA-2 from the NIST Framework is administrative in nature, and is concerned with scheduling maintenance and the control of information contained within BES Cyber Systems. Adding a requirement that "[s]anitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs" would, if implemented, limit the use of off-site troubleshooting of operational problems, which could significantly increase maintenance costs, and increase the time required to troubleshoot operational problems, investigate the cause of unexpected operations, and impede rapid response to reliability-based operational issues encountered daily on the system.

- Control MA-3 would, in part, proscribe how to implement the proposed CIP Version 5 requirement to protect BES Cyber Systems from the introduction of malware. Control MA-3 describes one of many possible approaches to this, but proposed CIP Version 5 describes the desired end-state of protecting the BES Cyber System from malware regardless of how it would be introduced.

- Controls MA-4 and MA-5 are already largely included in the CIP Version 5 requirements surrounding remote access. Further alignment would add administrative requirements and specify how to implement the control.

- Control AC-5 may require multiple staff members to "prevent malevolent activity without collusion." Entities would be required to hire additional staff to accomplish this duplicity and may be burdensome, particularly on small entities. In addition, collusion, while a fundamental concern for fraud prevention, is less of a concern for control systems and the CIP Reliability Standards cover the vulnerabilities through access management and personnel risk assessments.

- The SA family of controls is largely administrative, and describes approaches and methods that can be used in the procurement of systems in a secure manner. The CIP Reliability Standards already describe the expectations of entities for the cyber security performance of their systems, so this language is duplicative and administrative in nature.

These are just a few examples that further support the need for additional discussion in a technical forum to ensure any additional controls are appropriate for inclusion in the CIP Reliability Standards and not as a final conclusion on the value the controls may have within the CIP Reliability Standards.

VIII. Conclusion

For the reasons stated above, NERC respectfully requests that the Commission consider NERC's comments when it issues its final rule and approve the proposed CIP Version 5 Reliability Standards as filed.

Respectfully submitted,

/s/ William H. Edwards
/s/ S. Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
William H. Edwards
Counsel
S. Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
william.edwards@nerc.net
shamai.elstein@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: June 24, 2013

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 24th day of June, 2013.

/s/ William H. Edwards

William H. Edwards
Counsel for North American Electric Reliability Corporation