UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC)
RELIABILITY CORPORATION)
) Docket No. RM06-22-000
STAFF PRELIMINARY ASSESSMENT FOR)
EIGHT CYBER SECURITY STANDARDS)
FOR THE BULK-POWER SYSTEM)

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON THE STAFF PRELIMINARY ASSESSMENT FOR EIGHT CYBER SECURITY STANDARDS FOR THE BULK-POWER SYSTEM

Rick Sergel
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
rick.sergel@nerc.net
david.cook@nerc.net

Owen E. MacBride
Debra Ann Palmer
Schiff Hardin LLP
1666 K Street, N.W.
Suite 300
Washington, DC 20036-4390
(202) 778-6400
(202) 778-6460 – facsimile
omacbride@schiffhardin.com
dpalmer@schiffhardin.com

February 12, 2007

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation[1] ("NERC") is providing comments on the FERC Staff Preliminary Assessment for eight cyber security standards for the Bulk-Power System ("Staff Assessment"), issued in the above-captioned docket.[2]

In a separate rulemaking[3] the Commission is proposing to approve 83 proposed reliability standards, including six of the eight regional differences, and the NERC *Glossary of Terms Used in Reliability Standards*, and to also recognize as "good utility practice" 24 proposed standards that are pending approval subject to NERC's submittal of additional information.[4] NERC acknowledges that the Commission is taking an appropriate approach by proposing in the NOPR to direct NERC to complete the necessary improvements to the proposed reliability standards through the established NERC standards development process.[5]

The Commission has elected to separately consider the eight proposed cyber security standards that NERC filed for approval on August 28, 2006. Considering these standards separately is a reasonable approach, given that the proposed cyber security standards are new to

[1] On January 1, 2007, the North American Electric Reliability Council merged with its affiliate, the North American Electric Reliability Corporation, with NERC being the surviving organization. NERC was formed to serve as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act ("FPA"). The Commission certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000. 116 FERC ¶ 61,062 (July 20, 2006) (the "ERO Certification Order").

[2] *Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, December 11, 2006, Docket RM06-22-000 ("Staff Assessment").

[3] *Notice of Proposed Rulemaking: Mandatory Reliability Standards for the Bulk-Power System* (Docket No. RM06-16-000), issued October 20, 2006 ("NOPR").

[4] NOPR, PP 1 and 7-9.

[5] NOPR, P 10.

the industry and represent a substantive change from historical practices. These standards are especially important to the security of the Nation's electricity infrastructure.

NERC appreciates the careful review of the proposed standards by the Commission Staff. Staff's perspective is invaluable as NERC strives to improve the quality and usefulness of these standards over time. It is clear from the assessment that Staff and the Commission take the issue of cyber security seriously – as do NERC and the industry. The comments in the Staff Assessment will serve to bring further attention to the issue of cyber security, and will result in stronger standards over time.

NERC is providing comments in this filing on a number of general issues raised by the Staff Assessment. Responses to specific points made in the Staff Assessment are provided in **Attachment 1**. NERC has prepared its comments in close consultation with representatives from the cyber security standards drafting team, which consists of recognized experts in many facets of cyber security, including information system security, physical security, auditing, and control system operations.

In addition to providing comments on the Staff Assessment, NERC requests that the Commission, in accordance with its authority under Section 215(d)(1) of the FPA[6] and Section 39.5 of its regulations[7], approve the current set of proposed cyber security standards as soon as practical. NERC also requests that the Commission direct that all proposed modifications and improvements to these standards be referred to the NERC standards development process. The proposed cyber security standards were recently adopted through the standards development process after several years of development by a diverse team of experts. The standards are being

[6] 16 U.S.C. 824o.

[7] 18 C.F.R. § 39.5.

implemented in stages over several years. It is important to allow that implementation to be completed so that the industry can learn from the experience of putting the initial set of proposed standards into place. This approach is superior to delaying implementation of the currently proposed standards while waiting to incorporate additional improvements that may be directed by the Commission. The approach proposed by the Commission in the NOPR will also work well for the cyber security standards. This approach will allow the proposed standards to be placed into effect immediately as mandatory and enforceable, while allowing modifications and improvements identified by the Commission to be made in accordance with priorities established by the Commission.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to these comments may be addressed to the following:

Rick Sergel
President and Chief Executive Officer
David N. Cook*
Vice President and General Counsel
North American Electric Reliability
Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
rick.sergel@nerc.net
david.cook@nerc.net

Owen E. MacBride
Debra Ann Palmer*
Schiff Hardin LLP
1666 K Street, N.W.
Suite 300
Washington, DC 20036-4390
(202) 778-6400
(202) 778-6460 – facsimile
omacbride@schiffhardin.com
dpalmer@schiffhardin.com

*Persons to be included on the Commission's service list are indicated with an asterisk.

III. BACKGROUND

A. Reliability Policy Framework

Title XII of the Energy Policy Act of 2005[8] entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk-power system. Title XII added Section 215 to the FPA requiring the Commission to issue rules for the certification of an ERO that would be charged with developing and enforcing mandatory reliability standards, subject to Commission approval. Section 215 also gave the Commission the regulatory responsibility to approve standards that protect the reliability of the bulk-power system. In executing its responsibilities to review, approve and enforce mandatory reliability standards, the Commission is authorized to approve those proposed standards that meet the criteria detailed by Congress:

> The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest.[9]

The Commission launched its implementation of Section 215 by issuing Order No. 672 on February 3, 2006, establishing criteria for the certification of a single ERO and the procedures under which the ERO may propose new or modified reliability standards for Commission review.[10] Section 39.5(a) of the Commission's regulations requires the ERO to file with the Commission for approval each reliability standard the ERO proposes to become mandatory and

[8] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005).

[9] Section 215(d)(2) of the FPA.

[10] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 71 FR 8662 (Feb. 17, 2006), FERC Stats. & Regs. Regulations Preambles ¶ 31, 204 (2006), *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006).

enforceable in the United States, and each proposed modification to a reliability standard. When evaluating proposed reliability standards, the Commission is to give "due weight" to the technical expertise of the ERO, but not to defer to the ERO with regard to the impact of reliability standards on competition. The Commission provided guidance in Order No. 672 on the factors the Commission will consider when determining whether proposed reliability standards meet the statutory criteria.[11]

The Commission has made substantial progress in evaluating reliability standards proposed by NERC to determine if the standards should be made mandatory and enforceable in the United States. NERC filed a petition for approval of 102 existing reliability standards on April 4, 2006.[12] Anticipating the filing of these standards, in September 2005 the Commission had directed its Staff to begin evaluating NERC's existing standards. On May 11, 2006 the Commission issued the *Staff Preliminary Assessment of Proposed Reliability Standards* ("Staff Assessment of Reliability Standards") and solicited comments from bulk-power system owners, operators and users and other stakeholders.[13] NERC filed comments in support of the Staff Assessment of Reliability Standards and indicated in those comments how NERC was addressing the issues identified in the Staff Assessment of Reliability Standards through its standards development process.[14]

[11] *See* Order No. 672 at PP 320-36.

[12] North American Electric Reliability Council and North American Electric Reliability Corporation, *Petition for Approval of Reliability Standards*, filed April 4, 2006 (Docket RM06-16-000).

[13] *Notice of Comment Period*, Docket No. RM06-16-000 (May 11, 2006).

[14] *Comments of the North American Electric Reliability Council and North American Electric Reliability Corporation on Staff Preliminary Assessment* (Docket No. RM06-16-000).

On August 28, 2006, NERC filed a second petition for the approval of proposed reliability standards, submitting 16 new standards for approval and revisions to 11 of the reliability standards previously submitted on April 4, 2006.[15] Of the 16 new standards submitted, eight were the Critical Infrastructure Protection cyber security standards that are the subject of the current Staff Assessment. The Commission is proposing to address the Critical Infrastructure Protection cyber security standards through a separate rulemaking, and on December 11, 2006 issued the Staff Assessment as a basis to solicit industry comment on those proposed standards.[16]

B. Background of Proposed Cyber Security Standards

The initial work on the cyber security standards dates back to 2002 when NERC's Critical Infrastructure Protection Advisory Group ("CIPAG")[17] drafted cyber security language that ultimately appeared in Appendix G of the Commission's "Standard Market Design NOPR."[18] Since then, NERC has continued to raise the bar on cyber security, first by adopting Cyber Security Urgent Action Standard 1200 in 2003, and again with the proposed standards filed with the Commission in August 2006.

The development record of the proposed cyber security standards, which was included with the filing of the proposed cyber security standards in August 2006, shows they have been

[15] *Petition of the North American Electric Reliability Council and North American Electric Reliability Corporation for Approval of Proposed Reliability Standards*, filed Aug. 28, 2006 (Docket RM06-16-000).

[16] *Notice of Comment Period*, Docket No. RM06-22-000 (December 11, 2006).

[17] The CIPAG was a predecessor organization to NERC's current Critical Infrastructure Protection Committee ("CIPC").

[18] FERC Docket RM01-12-000.

crafted with significant industry input and debate of key issues. The Standard Authorization Request ("SAR") for the cyber security standards was submitted to NERC on May 2, 2003. After two public comment periods, the industry reached a consensus on the scope and justification for the standards. The Standards Authorization Committee ("SAC") appointed a drafting team of security experts to begin development of these standards in May 2004. Drafting team members brought significant experience and expertise from a broad spectrum of security-related disciplines including information technology security, physical security, compliance auditing, personnel and training, and energy management systems ("EMS") and system control and data acquisition ("SCADA") system operations. Drafting team members also brought expert knowledge of existing government regulations affecting security such as Sarbanes-Oxley and the Federal Information Security Management Act of 2002 ("FISMA"), as well as existing security-related standards such as International Standards Organization ("ISO") Standard 17799 and the body of work promulgated by the National Institute of Standards and Technology ("NIST"). A number of members of the drafting team held professional security certifications. Membership on the drafting team fairly represented ownership segments in the industry and a balance between U.S. and Canadian participation.

Throughout the development process, the drafting team insisted on looking beyond generally accepted "best practices." Rather, they sought to establish relevant, thorough requirements with unambiguous measures for determining compliance.

During the development process, three versions of the cyber security standards were posted to solicit input from the industry and other interested parties. More than 2,500 pages of comments and responses to the comments were provided in response to the three postings of the draft standards. The fourth and final version was submitted to ballot of the stakeholders. The number and volume of comments received represented an extraordinary level of involvement by the industry during the development process.

Initial balloting on the proposed cyber security standards was conducted in the period February 17–27, 2006. Because there were negative votes with comments on the initial ballot, in accordance with the standards development procedure a recirculation ballot was conducted in the period March 14–24. Of 294 total votes cast, 13 entities changed a negative vote to an affirmative vote in the recirculation ballot; and one entity changed an affirmative vote to a negative vote. In the final vote, stakeholders approved the cyber security standards by a sector-weighted vote of 88.8%, with 91.9% of those who joined the ballot pool actually voting.

The drafting team successfully resolved the vast majority of issues raised during the development of these standards. However, there were several unresolved minority objections with which the drafting team and the majority of stakeholders disagreed:

- Some requirements imposed by the standards are too costly to implement and may have little return on investment.
- The scope of the requirements should be limited to critical cyber assets within bulk-power system control centers.
- Levels of non-compliance are too high for some requirements that seem to be primarily administrative.
- The definition of critical asset leaves room for ambiguity in interpretation.

Nonetheless, the approved set of cyber security standards provides a set of firm requirements that are capable of being implemented by all participants in the electricity sector regardless of size, staffing levels, or levels of sophistication. Compliance with many of the requirements in the standards (and, indeed, many practices recommended by the Staff Assessment) may already be achieved or exceeded by some members of the electricity sector. On the other hand, the standards may be a significant burden on some entities that have not heretofore been required to implement cyber security programs. Throughout the development process, the drafting team attempted to push the bar beyond the generally accepted industry best practices, and to ensure that every link has at least the minimum protection necessary to protect the reliability of the bulk-power system as a whole. The resulting standards represent a balanced set of outcomes in a diverse industry, and provide a set of standards that are rigorous yet for which compliance can be achieved by all participants in the electricity sector.

In addition, the proposed cyber security standards fulfill relevant portions of Recommendations 32 and 32.A of the *United States/Canada Power System Outage Task Force* report. These recommendations state, in part, that NERC should finalize and implement the CIP-002-1 to CIP-009-1 standards, that NERC standards related to physical and cyber security should be made mandatory and enforceable, and that NERC should take actions to better communicate and enforce these standards. To help the industry understand and implement these standards, NERC has just completed a series of ten industry workshops on the standards for bulk-power system owners, operators, and users that were conducted across North America.

IV. DISCUSSION OF MAJOR ISSUES OUTLINED IN THE STAFF ASSESSMENT

This section addresses seven overarching issues relevant to the proposed cyber security standards that are raised in the Staff Assessment. **Attachment 1** contains NERC's detailed responses to specific items cited in the Staff Assessment.

A. Need to Make the Proposed Standards Mandatory as Soon as Practical

The development of cyber security standards for the electricity industry has demonstrated a continuous cycle of improvement. The progression has resulted in a set of practical, achievable, measurable standards that are sufficiently flexible to apply to the spectrum of bulk-power system owners, operators, and users, from the largest to the smallest and covering all applicable entities. The standards embody some of the most comprehensive requirements ever created for use on a widespread basis in the industry, yet provide the ability for entities to rapidly adapt to ever-changing threats and to embrace advances in protective technologies and processes.

The proposed standards greatly expand both the number of entities that must comply, as well as the scope of assets that must be protected. In many cases, capital investments to meet the requirements are necessary. For this reason, the NERC Implementation Plan for the proposed standards calls for compliance to be phased in over a three-year period. This approach ensures significant, progressive improvements in cyber security, culminating in full compliance to a robust set of requirements by mid-2009. During this three-year period, NERC will conduct various evaluations and monitor the progression of compliance to ensure the bulk power system is protected. The Commission should approve the proposed cyber security standards as mandatory and enforceable as soon as practical, subject to the implementation schedules in the implementation plan, to allow NERC and the industry to proceed towards meeting the milestones (some of which have long lead times) necessary to achieve compliance with the standards.

B. Direct All Comments for Modifications and Improvements to the Standards to the Standards Development Process

Implementing the requirements of the proposed cyber security standards will significantly improve the industry's resiliency to malicious cyber attacks. NERC fully expects that, over time, more enhancements will be made. Until the industry gains experience with these proposed standards, however, it will be difficult to understand where to introduce changes that can significantly improve cyber security within the industry. As the progression from the Cyber Security Urgent Action Standard 1200 to these proposed standards demonstrates, NERC's standards development process is an effective vehicle for introducing and debating the merits of such improvements.

Therefore, NERC requests any concerns the Commission may have with the proposed standards be directed for resolution in the NERC standards development process. NERC eagerly anticipates this opportunity, and indeed believes it is NERC's responsibility in accordance with its own Rules of Procedure to consider all comments suggesting improvements to the standards. NERC concurs with the Commission's statement in the October 20, 2006 NOPR in Docket RM06-16-000 that:

> the responsibility for the technical adequacy of the proposed Reliability Standards falls squarely on the ERO, and we expect the ERO to monitor the effectiveness of the proposed Reliability Standards and inform us if any Reliability Standard proves, in practice, to be inadequate in protecting and improving Bulk-Power System reliability.

Referring all comments and proposals for modifications and improvements to the NERC standards process for resolution is consistent with NERC's obligation to facilitate an open stakeholder process for the development of reliability standards. Creating optimum standards is not a goal that can be achieved in a short time period. Rather, NERC's Standards Development Process provides for and ensures a continuous succession of improvements.

C. Discretion and Business Judgment

Evident throughout the Staff Assessment is a concern that the proposed cyber security standards are not sufficiently explicit and directive and that they allow too much leeway for both interpretation and implementation, which would therefore result in inconsistent or even substandard application across the electricity industry. This area of the Staff Assessment focuses on the provision of each proposed cyber security standard that responsible entities should interpret and apply the standards using "reasonable business judgment."[19]

[19] Staff Assessment at 2 and 8-10.

NERC agrees that the standards are not prescriptive. NERC disagrees, however, with the Staff's assessment that this will result in inconsistent and substandard levels of application. Rather, the proposed standards recognize the diversity of cyber assets currently in place in the industry, the diversity of the operating, regulatory and economic environments of bulk-power system owners, operators, and users across North America, and the diversity of technology solutions currently available to meet the requirements as well as the anticipated availability of new, more advanced solutions in the future. The standards recognize the importance of providing the management of each responsible entity the flexibility to assess all possible options within its operating and business context to allow the best possible choices to be implemented and improvements to be made over time. The direction in the proposed Cyber Security standards that responsible entities apply "reasonable business judgment" in determining how to implement the standards provides for such flexibility.

Imposition of a more specific and prescriptive set of requirements would be both undesirable and unworkable, for several reasons. Such a set of standards would need to encompass and address all possible scenarios that could affect all possible assets belonging to all possible entities and attempt to prescribe exactly what the expected and required response to each of these scenarios must be. This approach is not viable. First, the diversity of the industry and of the technology infrastructure currently in place makes it impossible to identify and describe all potential scenarios, define all probable outcomes, and identify the most appropriate solutions for all situations. Even if it this were possible, the resulting document would be unmanageably voluminous and cumbersome. Second, a prescriptive set of requirements may be capable of implementation by the largest and most sophisticated participants in the industry, but not by smaller and less sophisticated owners, operators and users of the bulk-power system.

Third, the resulting document would be out of date before it was published due to the ever-changing nature of critical cyber asset technology and the continuously evolving cyber security environment. Fourth, creating such a restrictive list of solutions would prohibit the introduction of newer, better alternatives to meet rapidly changing threats, effectively making assets less secure over time. Fifth, promulgating a specific list of requirements for critical cyber asset protection would create a road map to be targeted by those seeking to engage in malicious cyber attacks.

The wide range of sizes and sophistication of owners, operators and users of the bulk-power system to which the cyber security standards will apply cannot be ignored. A single set of prescriptive requirements simply would not be workable. They would need to be either set low enough that compliance could be achieved by the smallest, least sophisticated organization, resulting in an inadequate level of protection for the critical cyber assets of larger organizations with more complex cyber asset infrastructures; or if set at a level necessary to adequately protect the critical cyber assets of the largest organizations, they would be incapable of being complied with by smaller organizations.

Staff expresses concern that the requirement of the standards to use "reasonable business judgment" to determine how to implement them will allow responsible entities to evade their obligations to adhere to the intent of the standards. However, the requirement to exercise reasonable business judgment does not mean a responsible entity may simply ignore taking action; it is not a license to ignore the entity's responsibilities or to do nothing. Rather, it requires responsible entities to analyze the role of each asset within the scope of the standards, the cost of the asset, and the impacts of its loss, weighed against the costs of possible protection strategies. NERC anticipates that such analyses will require considerable time and effort by responsible entities. Management will be required to exercise due diligence in reaching its decisions as to how to implement the standards to achieve their intent. This type of decision-making results in optimal solution sets that maximize and protect the value of the assets and the interests of the responsible entity.

In its compliance audit function, NERC intends to hold responsible entities to a standard of effective management oversight to ensure that all requirements of the proposed standards are met to substantial levels of quality. As discussed in §IV.D below, the proposed standards are performance-based standards, meaning that the standards require specific *outcomes* that, taken together, will constitute a comprehensive set of cyber security activities. However, for the reasons discussed above, the standards do not prescribe specific means of achieving the outcomes. NERC intends to audit compliance with the proposed cyber security standards against the intended set of outcomes. Responsible entities will be required to demonstrate the thoroughness and rationality of their management decision-making processes that have resulted in their specific choices of implementation techniques to achieve the outcomes intended by the standards.

Another layer of quality control for responsible entities' implementation decisions will be provided by NERC's Reliability Readiness Evaluation and Improvement Program. This program provides for the systematic, periodic evaluation of entities' preparedness to comply with the requirements of NERC standards, including the proposed cyber security standards.[20] These readiness evaluations will help management assess the quality of its decision making, the resulting programs, and the adequacy and appropriateness of the specific solutions the

[20] At this time, the readiness evaluation program encompasses the most significant entities from a reliability standpoint; not all responsible entities are included within the scope of the current program.

responsible entity has adopted. These evaluations will help ensure consistent interpretation of the requirements of the standards as well as promote consistency of the quality of solutions and implementation across entities.

Through the Reliability Readiness Evaluation and Improvement Program, NERC can review the status and quality of the proposed actions by the responsible entity, and can recommend and discuss changes where appropriate. This use of the Reliability Readiness Evaluation and Improvement Program will allow NERC and responsible entities to engage in substantive discussions concerning implementation without the consequences associated with a compliance audit.

Staff asks whether there are good alternatives to the principle of allowing entities to use reasonable business judgment to implement the standards that would permit both the necessary flexibility and yet prevent inappropriate decisions. The short answer is "no." This principle was exhaustively vetted and alternatives were examined in the development of the standards. While the "reasonable business judgment" principle may not be perfect, it should not be dismissed simply on the possibility that it might be abused. In any event, if, over time, experience indicates that greater specificity is needed in the standards, the NERC standards development process is the most appropriate mechanism for determining how to modify the standards.

Finally, Staff is concerned that there is no oversight as to how management determines which assets are "critical cyber assets" that are subject to the requirements of the standards. NERC believes that application of the requirement for entities to use "reasonable business judgment" to determine implementation solutions, coupled with oversight of management's decisions through the NERC compliance audit function, supplemented by NERC's Reliability

Readiness Evaluation and Improvement Program, will yield effective cyber security programs that comprehensively meet the rigorous requirements of the proposed standards.

D. Level of Specificity

Staff expresses concern that the lack of specificity within the proposed standards will result in sub-par implementation and inconsistent results. NERC agrees that the standards are not prescriptive, but believes, for the reasons stated in §IV.C above, that the level of specificity is entirely appropriate.

As noted in §IV.C, the proposed cyber security standards are performance standards. The use of performance standards, as opposed to standards that impose specific process or implementations steps, is widely accepted. For example, as the Department of Homeland Security noted in its recent notice concerning chemical security regulations (71 Fed. Reg. 78275, at 78282-3), "[t]he term[] 'performance standards' carries significant meaning."

> The term "performance standards" has a long and well-known history. See Cary Coglianese et al., Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection, 55 Admin. L. Rev. 705, 706-07 (2003). The term has repeatedly been defined:
>
> > Performance standards * * * state[] requirements in terms of required results with criteria for verifying compliance but without stating the methods for achieving required results. A performance standard may define functional requirements for the item, operational requirements, and/or interface and interchangeability characteristics.
>
> A performance standard may be viewed in juxtaposition to a prescriptive standard which may specify design requirements, such as materials to be used, how a requirement is to be achieved, or how an item is to be fabricated or constructed. OMB Circular A-119 (Feb. 10, 1998); see also Coglianese, Performance-Based Regulation, 55 Admin. L. Rev. at 709:
>
> > A performance standard specifies the outcome required, but leaves the specific measures to achieve that outcome up to the discretion of the regulated entity. In contrast to a design standard or a technology-based standard that specifies exactly how to achieve compliance, a performance

> standard sets a goal and lets each regulated entity decide how to meet the CIP standards.

Executive Order 12,866 also specifies the use of performance standards:

> Each agency shall identify and assess alternative forms of regulation and shall, to the extent feasible, specify performance objectives, rather than specify the behavior or manner of compliance that regulated entities must adopt. Exec. Order 12,866, 58 FR 51,735 (Oct. 4, 1993), as amended by Exec. Order 13258, 67 FR 9385 (Feb. 28, 2002).

The proposed performance-based cyber security standards reflect this well-recognized and long-used method for achieving a high level of performance while preserving flexibility and simplicity.

As performance standards, the proposed cyber security standards require specific outcomes that, when taken together, constitute a comprehensive set of cyber security activities. They do not identify the specific means of achieving those outcomes. It matters more that a pre-defined, desirable outcome is achieved rather than how it is achieved. For example, standard CIP-005-1, when specifying the requirements for the Electronic Security Perimeter, requires that the perimeter only allow *required* ports and services be granted access. The standard cannot "know" what a particular responsible entity needs to perform its business functions. However, if, during a compliance audit, the responsible entity cannot demonstrate that a particular port or service is *required*, it will be found in noncompliance with that requirement.

Many requirements throughout the standards are in fact specific. For example, CIP-005-1 describes with a great deal of specificity the required characteristics of the Electronic Security Perimeter surrounding a collection of Critical Cyber Assets:

- "ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter" (Requirement R1).

- "access points … shall include *any* externally connected device" (Requirement R1.1, emphasis added).

- “any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be … protected” (Requirement R1.4).
- “use an access control methodology that denies access by default” (Requirement R2.1).
- “at *all* access points … enable only ports and services required” (Requirement R2.2, emphasis added).

Additional specificity in the standard would result in defining the means of implementation rather than the outcome. This could unnecessarily hamper a responsible entity’s ability to maximize its resources to actually achieve the desired outcome, or to adapt to changes in its environment, with consequences that could be deleterious to reliability.

Moreover, as discussed in §IV.C above, if the requirements of the standards were more specific or prescriptive, they would be either irrelevant or impossible to achieve for smaller entities, or too watered-down to be effective for larger entities. Instead, focusing on specific outcomes ensures that each entity, regardless of its size or its existing cyber security initiatives, is held responsible for achieving a pre-defined level of performance deemed necessary to protect critical bulk-power systems assets from cyber attacks.

E. Technical Feasibility

Staff also raises concerns about references to “technical feasibility” within the requirements of the cyber security standards. This term is intended to be very limited in scope. It defines the physical ability of in-place equipment or software to directly conform to some requirement specified in the standards; or the ability of in-place equipment or software to perform its required function if modified in a way that would most directly conform to some requirement specified in the standards. The introduction of this concept into the standards was intentional to prevent penalizing responsible entities unnecessarily for situations beyond their ability to immediately or prudently change simply in order to comply with a requirement. The "caveat" for technical feasibility most often arises where existing equipment or software may satisfy the requirement in part, or a particular aspect of the requirement, but not meet the measure of full compliance without significant upgrades or perhaps complete replacement. In some cases it would not be prudent to implement a fully compliant solution, because doing so would cause a decrease in reliability or functionality. While it may be necessary to implement protection surrounding a Critical Cyber Asset to meet a requirement of the proposed cyber security standards, it should not be a requirement to *replace* a Critical Cyber Asset to comply with a requirement, unless there is a compelling reliability-based reason to do so.

Similarly, the principle of technical feasibility can apply in cases where the resources (staff, time, money) required to implement a fully compliant solution would exceed the expected life of the system, or dilute the resources necessary for replacing the current system with one that fully meets the requirements. For example, it may take three years to retro-fit the best possible, but still incomplete, protection for a legacy system; whereas it may only take two years to completely replace the legacy system with a new and fully compliant system. It is thus possible that some significant portion of any resources spent attempting to "fix" the existing system would merely prevent implementation of a better solution, leaving the overall system vulnerable for longer than necessary.

Application of the principle of technical feasibility does not mean that a responsible entity can do nothing. In those situations where technical feasibility encumbers full compliance to a requirement, the responsible entity should document the technical issue as well as the entity's mitigation plans or strategies. The technical feasibility surrounding the requirement should be reviewed routinely and if found to still exist, the appropriateness of the implemented mitigation strategies should be reviewed and approved. At a minimum, the responsible entity will need to have a credible explanation for why it is not in compliance with the standards.

F. Risk Acceptance

The concept of risk acceptance is similar in many ways to the principles of reasonable business judgment and technical feasibility. The concept of risk acceptance recognizes that flexibility and judgment are required to make prudent, rational decisions, but does not allow an entity to do nothing. Acceptance of risk is a fundamental tenet of an audit process, in which it is acknowledged that not all systems or implementations can be perfect, and that there will always be some level of risk associated with any approach to implementation of a standard. CIP-003-1 Requirement R3 illustrates a common way that the principle of risk acceptance is recognized. The requirement calls for the responsible entity to write an exception to its cyber security policy, explaining and formally acknowledging its acceptance of risk, and documenting compensating measures. The exception must be signed by a senior manager and reviewed annually to ensure the conditions that required the exception are still viable.

The language in these proposed standards is stronger than that in the predecessor standard, Urgent Action Cyber Security Standard 1200. The language in the proposed standards does not allow an entity to take exception to a requirement of the standards, whereas doing so was allowed previously under Urgent Action Cyber Security Standard 1200.

G. Defining Compliance

The Staff Assessment raises the concern that the proposed cyber security standards do not establish requirements regarding such issues as quality, adequacy, or appropriateness. These are subjective qualities, and as such are exceedingly difficult to describe in a standard, much less to measure. This difficulty in measurement could result in the uneven application of compliance between audits. As previously discussed, the cyber security standards leave such subjective matters to the exercise of reasonable business judgment by each responsible entity through effective management oversight, subject to compliance audits and NERC readiness evaluations.

As discussed earlier, the cyber security standards are performance standards, in which specific outcomes are required, but the specific means of achieving those outcomes are not specified. The expected performance requirements of the cyber security standards are unambiguous and, therefore, compliance to them can be assessed objectively and unequivocally. Moreover, the proposed standards map each requirement to a specific and separate measure (e.g., Requirement R1 is measured by Measure M1), thereby allowing a responsible entity or a compliance auditor to rapidly determine how compliance to each performance requirement will be assessed. This mapping of requirements and measures mandates each individual requirement be quantitatively measured by a specific, repeatable, and irrefutable measure; no subjective determinations are required or allowed. An example of a quantitative measure of compliance is evidence that a document was updated or approved within a specified timeframe. An objective measure does not require the auditor to render an “opinion” about the acceptability of the “evidence.” The use of objective measures provides for consistent audit results cross all regions and responsible entities, independent of the specific individuals on and skill sets of an audit team.

H. Applicability

Applicability in the context of the NERC reliability standards refers to who must comply with the standards. The applicability of a particular standard is determined in the NERC standards development process. As the Staff Assessment points out, all eight of the standards apply to the same applicable entity classes. Because of the nature of the cyber security subject matter, there are no variances across regional or functional entity lines.

The cyber security standards are unique in that they also have been designated to apply to the offices of NERC and of the Regional Reliability Organizations. This designation was made as a result of industry comments, and in recognition that cyber security issues are present with certain of the applications that NERC maintains. In an order issued January 18, 2007, on a compliance filing that NERC made in response to the ERO Certification Order, the Commission ordered NERC to amend its rules of procedure to require that NERC comply with any reliability standard that identifies NERC as an applicable entity.[21] NERC intends to comply with that order.

V. NEXT STEPS

NERC believes that implementation of the proposed cyber security standards that have been developed and adopted by the industry through the NERC standards development process will significantly improve the resiliency of the bulk-power system to cyber attacks over and above its current levels of protection. Certainly these standards are not perfect. However, given the diversity of industry participants, and the differing levels of sophistication of cyber asset protection from which they are starting, the best way to approach what surely will be a long-term process to achieve adequate protection of the nation’s bulk-power system from cyber-attack or other malicious actions is to apply these standards as written, observe their impact over time, and improve them through the NERC standards development process as necessary.

Additionally, NERC requests the following of the Commission:

1. The Commission should refer any additional work deemed to be needed on these standards to NERC to implement through the standards process.

[21] *Order on Compliance Filing*, 118 FERC ¶ 61,030 (2007), at P 65.

2. The Commission should frame directives to improve the standards in the form of an objective to be achieved or an issue or concern to be addressed in the standard. The Commission should refrain from requiring specific language or a particular metric or solution to be used in a standard, because such a directive would circumvent the standards process and may result in less than optimal solutions, or standards that adversely impact reliability through unintended consequences.

3. The Commission should allow NERC to continue to work on further development and improvement of reliability standards in accordance with the NERC *Reliability Standards Work Plan 2007 – 2009* that was filed with the Commission on December 1, 2006.

Respectfully submitted,

/s/ Rick Sergel_______________________
President and Chief Executive Officer
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5731
(609) 452-8060
(609) 452-9550 – facsimile
rick.sergel@nerc.net
david.cook@nerc.net

/s/ Owen E. MacBride____________
Owen E. MacBride
Debra Ann Palmer
Schiff Hardin LLP
1666 K Street, N.W.
Suite 300
Washington, DC 20036-4390
(202) 778-6400
(202) 778-6460 – facsimile
omacbride@schiffhardin.com
dpalmer@schiffhardin.com

ATTACHMENT 1

RESPONSES TO SPECIFIC COMMENTS IN THE STAFF PRELIMINARY ASSESSMENT

This Attachment 1 provides NERC's comments to specific concerns, questions, and requests in the Staff Assessment. The NERC responses are provided in the same order as they are raised in the Staff Assessment.

Response to III.A.1: Nature of Cyber Threats

Staff Assessment:

> "Commission staff believes that defense in depth is a widely accepted, effective strategy to address cyber threats that is both comprehensive and flexible."[1]

NERC Response:

NERC agrees that defense in depth is an effective "best practice", however, the cyber security standards are written as a minimum set of mandatory requirements. A complete defense in depth strategy may not be practical at all locations containing Critical Cyber Assets. NERC does, however, deem the cyber security standards, when viewed in their entirety, to represent a defense-in-depth strategy: there are requirements for physical security perimeters, electronic security perimeters, asset protections, training programs, and management oversight. In addition, the standards are written to protect the Critical Cyber Assets from all hazards, and do not specifically require a threat analysis, although such a threat analysis could be included in the risk-based assessment.

[1] Staff Assessment at 7.

Response to III.A.2: Cyber Security Strategies

Staff Assessment:

> "However, the cyber security standards themselves must embody a reasonable balance. If they are too specific or prescriptive they tend to become a "one size fits all" solution, which means they will be of little use in an environment where systems vary greatly in architecture, technology, or risk profile. … One of the goals of this Assessment is to evaluate and solicit comments on how well the CIP Reliability Standards have achieved this balance, and whether they allow for a degree of flexibility in implementing security strategies that improve cyber security." [2]

NERC Response:

The development record of the cyber security standards drafting team's responses to comments supports the balanced consensus process used to arrive at the final standards. After considering the many and diverse industry comments, an appropriate balance was achieved. This conclusion is supported by the results of the industry ballot on the cyber security standards, which resulted in approval by an 88.8% affirmative weighted-sector vote.

Response to III.B.1: Business Judgment

Staff Assessment:

> "[S]taff is concerned that the language [of business judgment] unduly compromises the effectiveness of the CIP Reliability Standards and the ability to enforce compliance with them since each responsible entity would have discretion to determine how to implement the CIP Reliability Standards. This goes well beyond the discretion necessary for effective cyber security. [3]

NERC Response:

As discussed in the general section of these comments, NERC believes the "reasonable business judgment" provision of the standards is necessary and appropriate. This provision does

[2] Staff Assessment at 8.

[3] Staff Assessment at 9.

not compromise the effectiveness of the standards; rather, it provides for flexibility in the implementation by a diverse group of industry participants of solutions which meet the requirements of the standards.

Staff Assessment:

> "In addition, invoking the reasonable business judgment rule appears out of place in the context of mandatory Reliability Standards. As the name implies, the rule applies to business decisions, i.e., decisions on how best to promote the economic interests of the corporation and its shareholders. … Moreover, NERC provides direction on technical, not business, matters." [4]

NERC Response:

The "reasonable business judgment" provision is essential to providing the balance in the implementation of the standards. NERC agrees that the proposed standards are "technical" and not "business" in nature. However, this distinction refers to market or business practice issues -- it should not be implied that meeting reliability requirements should involve no consideration of cost or business implications. It is impossible to separate a responsible entity's internal business decisions from technical reliability concerns. If this were so, then all NERC standards would describe an impossibly high level of technical content (e.g., 100% guarantee of 100% reliable operation of the bulk power system). However, the cost of implementing such a solution would approach an infinite amount of time, money and resources. Obviously, reasonable business judgment must be applied to determine the appropriate level of resources to be devoted to achieving an adequate level of reliability.

Staff Assessment:

> "Staff seeks comment on: (1) specific examples of the differing roles of entities in relationship to their potential impact on cyber security risks to Bulk-Power System reliability; (2) alternatives to reliance on the reasonable business judgment rule that would allow for recognition of differing roles of entities, vulnerability of

[4] Staff Assessment at 10.

> assets and exposure to risk that also would permit effective enforcement of the CIP Reliability Standards; and (3) the ramifications of removing the "reasonable business judgment" language from the proposed CIP Reliability Standards while an alternative approach is developed using the ERO's Reliability Standards development process." [5]

NERC Response:

Bulk-power system owners, operators, and users function in widely varying business environments. For example, some entities own and maintain their own telecommunications infrastructure, while others do not. Responsible entities therefore must have flexibility in defining Critical Cyber Assets and Electronic Security Perimeters. Entities that own their own communications infrastructure could choose to protect it all, while entities who lease their infrastructure are to some degree subject to actions taken by others on that equipment, and therefore must make different decisions as to how to protect their Critical Cyber Assets. The reasonable business judgment rule provision provides entities facing differing problems the flexibility to develop solutions that will be effective in their particular circumstances.

NERC intends for the reasonable business provision to be applied so as to ensure that decisions regarding securing Critical Cyber Assets are made prudently and consider the entire environment in which the decisions are made. This environment includes not only infrastructure protection and security, but also the value of the asset(s) being protected, and the cost to protect those assets. Without application of reasonable business judgment, imprudent and unjustified solutions could be imposed which would dilute the efforts to properly implement appropriate solutions with respect to other assets, for example by devoting an excessive portion of the organization's resources to protecting particular assets at the expense of devoting sufficient resources to protecting other assets.

[5] Staff Assessment at 10.

Response to III.B.2: Defining Compliance

Staff Assessment:

> "As discussed in greater detail at various points below, many of the proposed CIP Reliability Standards provide limited, general direction in their Requirements on what constitutes adequate cyber security practice. This can suggest that the Measures and Levels of Non- Compliance, which focus largely on possession of documentation, play a greater role than they should. In particular, it may suggest possession of documentation regardless of the quality of the information or guidance contained in that documentation can demonstrate compliance. For this reason it is important to stress again the central role played by the Requirements in defining compliance, and it is the content of the Requirements that will be the focus of this Assessment." [6]

NERC Response:

NERC acknowledges the extensive use of documentation in the requirements, measures and levels of non-compliance throughout the standards. The majority of this documentation is used to demonstrate that required actions which satisfy the requirements have indeed been performed. The concept that mere "possession of documentation" can demonstrate compliance is misplaced. In most cases with regard to the cyber security standards it would not be possible to demonstrate compliance without some form of documentation or written records.

Documentation serves to prove requirements were met. For example, Standard CIP-007-1 Requirement R1 requires testing be performed to ensure changes do not adversely affect existing cyber security controls. Requirement R1.3 requires test results be documented. The measures and levels of non-compliance can only be based on the documented test results, because there are no "full-time on-site inspectors" to ensure that testing has been done. Thus, while the documentation is the measure, it is in direct support of proving compliance with the requirement.

[6] Staff Assessment at 11.

Documentation is required because of the methods employed during the NERC compliance audit process. The audit process uses an information gathering phase, a brief site visit, and a post-visit findings and report phase. Without the documentation requirements, the audit phase would require an excessive amount of time be spent gathering the information provided in the documents, and performing extensive testing in order to re-construct the approvals and process checks contained in the documentation. Using the documentation as required in the standards, the auditor only needs to cross-check the supplied documentation to verify the processes have been followed.

Response to III.B.3: Implementation Plan Compliance

Staff Assessment:

> "We seek comment whether it would be beneficial to audit a responsible entity at the "Begin Work" and "Compliant" stages even though it may not have the full 12 month accumulation of records available." [7]

NERC Response:

NERC agrees with the Staff there is benefit to ensure entities responsible for complying with the cyber security standards are moving toward full Auditable Compliant status, prior to achieving the full 12 months of auditable records. Though it is impossible to "audit" a responsible entity until it has reached an "auditable" state, the NERC Compliance Monitoring and Enforcement Program does include the CIP standards in its 2007 compliance program plan for monitoring through self-certification without penalties or sanctions. Through this approach, NERC will be able to assess intermediate progress towards compliance with the cyber security standards. NERC is considering additional efforts to further assist and assess the industry in achieving its compliance.

[7] Staff Assessment at 11.

The Reliability Readiness Evaluation and Improvement Program will also look at the industry's activities in implementing programs during each current review year to identify and share industry best practices, as well as to assess the quality of the programs.

NERC has recently completed a series of 10 workshops designed to educate the industry on what is required by the standards. These workshops received positive reviews. Additional education activities are under consideration by NERC, the regions, and other interested parties. It is anticipated that these additional activities will provide suggestions and guidance on how responsible entities can meet the requirements of the cyber security standards.

Response to III.B.4: Applicability

Staff Assessment:

> "To the extent that a Regional Entity or Regional Reliability Organization has cyber connections with any user, owner or operator of the Bulk-Power System, it is important that it also abides by the same CIP Reliability Standards. However, as discussed above, there is concern whether a Reliability Standard is enforceable against a Regional Entity or Regional Reliability Organization. Consistent with the approach suggested in the October 2006 Reliability Standards NOPR, the delegation agreements could require Regional Entities to comply with the CIP Reliability Standards."
>
> "These are the only proposed Reliability Standards that explicitly apply to NERC."
>
> "As a potential alternative, instead of ERO compliance being required pursuant to the Reliability Standards, ERO compliance could be required pursuant [sic; to] the NERC Rules of Procedure."
>
> "Staff seeks comment on whether it is appropriate that NERC adheres to the CIP Reliability Standards and, if so, the appropriate mechanism by which to direct such compliance." [8]

[8] Staff Assessment at 12-13.

NERC Response:

As ordered by the Commission on January 18, 2007 in Docket RR06-1-003[9], NERC will be modifying its Rules of Procedure to provide that the ERO will comply with each reliability standard that identifies the ERO as an applicable entity.

Similarly, the delegation agreements with the regional entities that have been filed with the Commission for approval hold the regions responsible for following approved reliability standards.[10] This provision effectively holds the regions responsible for following each reliability standard that identifies the regional entities as an applicable entity.

Staff Assessment:

> "While the assets and operations of a smaller entity may not have a major day-to-day operational impact on the Bulk-Power System, they can provide a gateway to compromise larger entities and, when attacked simultaneously with the facilities of other small entities, in the aggregate have an adverse impact on the Bulk-Power System… Staff believes that a key to any determination of whether an entity should be covered by the CIP Reliability Standards is whether or not it is a user, owner, or operator of the Bulk-Power System that has a cyber connection to other users, owners or operators of the Bulk-Power System… In light of this fact, we seek comment on how the impact of the CIP Reliability Standards might be addressed for smaller entities." [11]

NERC Response:

The proposed standards do not make the distinction of "small" or "large", but require that every applicable responsible entity must conduct a risk-based analysis to determine which of its assets are Critical Assets. NERC agrees with Staff that a responsible entity's size has no bearing

[9] *Order on Compliance Filing*, 118 FERC ¶ 61,030 (2007), at P 65.

[10] *See* paragraph 4(c) of the pro forma delegation agreement filed by NERC on November 29, 2006, in Docket No. RR06-1-004, and the equivalent section in each individual proposed delegation agreement that have been filed for approval in Docket Nos. RR07-1-000 through RR07-8-000.

[11] Staff Assessment at 13-14.

on whether or not it has Critical Assets. While there is some concern that "small" entities will reach the conclusion that they have no Critical Assets and only "large" entities will reach the conclusion that they have Critical Assets, this is not a presumed outcome of the process. It is a requirement of Standard CIP-002-1 that each responsible entity produce a risk-based assessment methodology and use that methodology to generate lists of critical assets and critical cyber assets (if applicable) for approval. Thus, the standards as written apply both to "large" and "small" entities.

Cyber connectivity to other owners, operators, and users of the bulk power system should not be the determining factor in identifying Critical Assets for applicability of the standards. Cyber connectivity has no bearing on the determination of what are Critical Assets. Whether or not a responsible entity has cyber connectivity to another responsible entity is no more important to protecting the integrity of the bulk-power system than is its cyber connectivity to its own assets. There is potential for intrusion into that connectivity in either case. Any responsible entity with Critical Cyber Assets is required to protect them from compromise or disruption (whether that compromise attempt is from an internal source or an external source).

The standards as written focus the responsible entity's efforts where their impact is greatest: at the identified Critical Assets. The loss of other assets which are not identified as Critical Assets cannot have an adverse impact on bulk power system reliability (otherwise they would be classified as Critical Assets). The standards prescribe a minimum set of assets that must be considered during the application of a responsible entity's risk-based methodology. The list of assets prescribed represents a significant cross-section of assets used to ensure reliable operation of the bulk power system. Each asset must be assessed by the responsible entity using a methodology best suited to the asset and the responsible entity's use of that asset in the bulk power system.

The Staff Assessment raises a concern that a number of small entities may be attacked simultaneously and in concert these attacks would have an adverse impact on the bulk-power system. The same can be said for attacks against a number of non-critical facilities within a large entity. The only alternative is to consider every asset as *requiring* protection, implying that *every* asset is therefore a Critical Asset, which is counterintuitive and not reasonable. Additionally, it would likely lead to a decrease in the overall reliability of the bulk power system due to diluted resources and diverted attention to the additional, less significant assets.

The Staff Assessment would seem to extend coverage by the standards to every asset and entity that is a user, owner, or operator of the bulk-power system and that has a cyber connection to another user, owner, or operator of the bulk-power system, and preclude other entities that do not meet this statutory definition, e.g., vendors and marketing partners. This leads to the undesirable consequence of requiring that the Cyber Assets only be protected from a small range of potential attack vectors which can readily be mitigated through the proper application of Electronic Security Perimeters as defined in CIP-005-1. Properly designed and implemented Electronic Security Perimeter access control devices serve to protect the identified Critical Cyber Assets from all external attacks, whether from other assets (critical or not) within a responsible entity, or from other entities.

Response to IV.B: CIP-002-1 Issues Identified

Staff Assessment:

> "The methodology and process developed by a Reasonable Entity must be stringent and rigorous. … [Standard CIP-002-1] does not provide direction on the nature and scope of that methodology, its basic features or the issues it should address. … [W]e emphasize the importance of utilizing an appropriate

> assessment methodology because the subsequent Requirements … depend on the adequate identification of the responsible entity's Critical Cyber Assets."[12]

NERC Response:

The standards are specifically written to allow each responsible entity the flexibility to implement them as they apply to the specific circumstances within each organization, and at each location containing Critical Cyber Assets, subject to the requirements contained in the standards. During the standards development process, a great deal of industry input and debate led the drafting team to the requirements as specified in the standards. While some argued for additional direction, others argued that the standards as written were already too prescriptive. Thus, the final version reflected the intended balance provided by the industry input. Additional direction would be counter to the implementation of the standards, providing both irrelevant and unobtainable detail for some entities, or allowing other entities to ignore truly Critical Assets.

NERC agrees with Staff that the assessment methodology is critical to the implementation of the remaining cyber security standards. However, during the development process, requiring additional specificity in the methodology proved problematic. The approved language accommodates the diversity of the industry and regional practice. Additional levels of specificity would only serve to invalidate existing risk management programs at some entities, while simultaneously unduly burdening others with levels of rigor that are not justified due to their configuration or their potential impact on the reliability of the bulk-power system.

Staff Assessment:

> "CIP-002-1 does not address the issue of interdependency with other infrastructures. There may be occasions where an electric sector asset, while not in and of itself critical to the Bulk-Power System, may be crucial to the operation of another critical infrastructure. Under the CIP Reliability Standards, such an

[12] Staff Assessment at 16.

> asset would not necessarily be identified in the responsible entity's analysis of Critical Assets." [13]

NERC Response:

All NERC Standards deal with the reliability of the bulk power system, and as such, focus solely on that issue. Assets from other infrastructures are, by their nature, not bulk power system assets, and are therefore not in scope for NERC reliability standards.

Interdependencies between electric sector assets and the assets of other infrastructures are not well understood. A significant additional amount of cross-sector coordination and study would be necessary to determine exactly what assets would need to be included. Because the responsible entities are accountable for determining the list of Critical Assets, the assets selected must be those which are under the control or jurisdiction of the responsible entity. Ultimately, the list of Critical Cyber Assets must be produced and given to NERC in order to achieve compliance with the remaining cyber security standards.

This is one of the reasons that telecom facilities are excluded.[14] In a significant number of implementations, responsible entities rely on telecom infrastructures which are leased, and therefore not owned or controlled by the responsible entity. As a practical matter, the responsible entity/lessee lacks the ability to control and direct all the activities of the vendor/lessor.

Staff Assessment:

> "We seek input whether the identification of other critical infrastructure assets that should be protected is appropriate for inclusion in CIP-002-1. We also ask

[13] Staff Assessment at 17.

[14] "The following are exempt [:] … Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." (Section A.4.2.2 of each standard.)

> whether this topic is an area for coordination and cooperation with other industries and government agencies." [15]

NERC Response:

The issue of assets to be included in CIP-002-1 must be strictly limited to those supporting the reliable operation of the bulk power system. Therefore, consideration of other assets must be out of scope for these standards. NERC acknowledges that additional areas for coordination and cooperation with other industries and governmental agencies would be advantageous. But this language has no place in mandatory reliability standards. NERC notes, however, that there is already extensive information sharing among the infrastructures through organizations such the Partnership for Critical Infrastructure Security ("PCIS") and the Information Sharing and Analysis Center ("ISAC") Council.

Staff Assessment:

> "…a relatively small entity whose operations may not have a major, day-to-day operational impact on the Bulk-Power System can have critical importance from a cyber security perspective, especially as a gateway to larger entities or when attacked simultaneously with other entities." [16]

NERC Response:

As indicated in the response to Staff Assessment section III.B.4 above, the standards are written to focus the efforts of the industry on protecting Critical Cyber Assets, those with the most critical value to the reliability of the bulk power system. The standards do not prejudge that small entities are not critical and large entities are critical. While other assets could serve as a "gateway" to Critical Cyber Assets of a larger entity, proper implementation of the Electronic

[15] Staff Assessment at 17.

[16] Staff Assessment at 17.

Security Perimeter surrounding the Critical Cyber Assets, as required in CIP-005, should provide effective protection from such attacks.

Similarly, Staff is concerned that an attacker may use a non-critical asset as an attack vector to a Critical Asset. Again, the Electronic Security Perimeter surrounding the Critical Cyber Assets should block all non-required ports and services from any source outside the perimeter, thereby severely limiting the risk of a potential attack scenario. The Electronic Security Perimeter effectively implements a *model of mutual distrust* between any collection of Critical Cyber Assets within an Electronic Security Perimeter, and any and all other Cyber Assets (whether they be other collections of Critical Cyber Assets or non-critical Cyber Assets, and regardless of the ownership of those external assets). If the attacker were able to use the existing communication pathway from the non-critical Cyber Asset through the defined Electronic Security Perimeter, and attack an identified Critical Cyber Asset, then the Electronic Security Perimeter implemented by the responsible entity has proved insufficient, and the responsible entity should be found non-compliant with the requirements of CIP-005-1.

While it would be difficult to detect and mitigate corrupt data at the Electronic Security Perimeter (which would pass unencumbered through it), effective use of other tools and processes commonly found in SCADA and Energy Management Systems, such as state estimation, limit checks and rate-of-change limit checks should mitigate the damage that can be propagated through such a mechanism.

The issue of simultaneous attack has already been discussed above in the responses to section III.B.4 of the Staff Assessment.

Staff Assessment:

> “The absence of adequate direction on what constitutes a proper risk-based assessment methodology may potentially result in entities improperly identifying

> a limited or "null set" of Critical Assets or Critical Cyber Assets. This result could have serious adverse effects for Bulk-Power System reliability." [17]

NERC Response:

As the Staff Assessment points out, the "size" of an entity (however size is measured) has no bearing on its potential impact to bulk system reliability. Because of this, as discussed above, the risk-based assessment methodology approach is used in standard CIP-002 to determine which assets (if any) are in fact critical to bulk-power system reliability, and, of those, which have Cyber Assets essential to their reliable operation.

Staff Assessment:

> "UA 1200 required updates to be completed within 90 days for any changes to either Critical Assets or Critical Cyber Assets, a deadline for updates has been eliminated in CIP-002-1. We seek comment on whether there should be a deadline." [18]

NERC Response:

Urgent Action 1200 was self-limiting in its scope, being only applicable to Control Centers, while the cyber security standards (CIP-002-1 through CIP-009-1) apply to a significantly larger group of assets, namely substations and power plants. With the significant increase in the number of assets which must be analyzed, a restrictive timeframe becomes rapidly unmanageable. Some entities may have several thousand substations requiring analysis, and would require the efforts of several full-time staff simply to maintain a list at the expense of actually securing the system.

The balance reached by the drafting team requires an annual re-assessment for all entities rather than an update deadline. This annual reassessment is required for entities that have not

[17] Staff Assessment 17.

[18] Staff Assessment 17.

made any changes to their systems, as well as for entities that have made significant changes to their systems. By requiring this annual reassessment, the standard is made more rigorous, and will capture potentially more updates to the lists than required by Urgent Action 1200. NERC therefore does not support the re-imposition of the deadline as specified in Urgent Action 1200.

Staff Assessment:

> "This senior management involvement is important and should be extended to approving the risk assessment methodology adopted under Requirement R1. … Therefore, staff believes that senior management awareness and approval of the chosen risk assessment methodology is of critical importance." [19]

NERC Response:

As discussed in §IV.E, Applicability, in the general comments in this filing, the NERC standards are performance based. The goal of CIP-002-1 is to produce an approved list of Critical Assets and Critical Cyber Assets. The requirement for senior management approval of the lists is sufficient, because the approval encompasses due diligence to develop a correct list.

Response to V.B: CIP-003-1 Issues Identified

Staff Assessment:

> "This Requirement [for a risk acceptance process] allows for broad discretion. Further, this requirement may act as a disincentive for upgrading to a control system that can meet all of the features of the security policy without exceptions."[20]

NERC Response:

Responsible entities must be given the ability to continue to operate their systems in spite of not being able to implement an industry accepted, or even internally mandated security posture. There are many cases within a responsible entity's implementation where upgrades are

[19] Staff Assessment at 18.

[20] Staff Assessment at 20.

either impractical or impossible due to legacy equipment configurations or out-of-business suppliers. The required annual review of all risk assessments serves to ensure that accepted risks are continually highlighted to management, and that they do not become permanent.

Staff Assessment:

> "The concern is that there does not seem to be any oversight that would allow for the determination of the cyber security posture for an interconnected control network." [21]

NERC Response:

The purpose of establishing policy and procedure is to protect oneself from the "outside world" wherever that outside world is. It does not matter if the "outside" is an internally connected corporate network, or a completely separate entity. The standards address an individual responsible entity's area of responsibility – the equipment it owns and controls. All "interconnection control network" connections use electronic access points; therefore, there is "security" on the interconnection points.

Staff Assessment:

> "… there is no oversight or regional perspective of the risks or vulnerabilities that are allowed to exist." [22]

NERC Response:

It is not the function of the standards to implement an oversight or hierarchical organization for determining risks or vulnerabilities. A responsible entity can only meet requirements of standards on assets of which it has direct ownership or control; because regional

[21] Staff Assessment at 20.

[22] Staff Assessment at 21.

perspective is performed outside of this direct ownership and control, no individual responsible entity can be required to achieve this regional perspective.

The risks and vulnerabilities the Staff appears to be discussing are addressed by the standards. Regional perspective is gained through the Electricity Sector ISAC ("ES ISAC"), Critical Infrastructure Protection Committee ("CIPC") and other information sharing activities and tools.

Staff Assessment:

> "This Requirement [R5] appears necessary, but as written it does not specify when access authorization should be modified. For instance, it does not indicate how soon after an employee has been terminated or changes jobs his access should be revoked and the access list updated. An annual review of the personnel access privileges appears insufficient and could result in unnecessary vulnerability, especially when there is no requirement to update the list immediately upon employee termination or job reassignment." [23]

NERC Response:

This requirement is for the establishment of "a program for managing access to protected Critical Cyber Asset information." The requirement relates to the governance and approval process, not the implementation and review of individual access (this lies in the responsibility of the Senior Manager of the responsible entity). The implementation provisions are in CIP-007-1 R5, while the revocation requirements are in CIP-004-1 R4. This requirement deals with management review and approval which allows the provisions required in CIP-007-1 to be implemented. The review provisions in this standard are meant as a check that the revocation provision in CIP-004-1 have been implemented, and provides management oversight that the information and account access granted are still valid and necessary.

[23] Staff Assessment at 21.

Staff Assessment:

> "An effective configuration management system should allow an entity to verify after the fact that any emergency modifications did not adversely impact the cyber security posture of the control system. It is not clear that the Requirement provides sufficient direction to address such modifications." [24]

NERC Response:

As with the Account Management requirement discussed above, this requirement is for the establishment of a Change Management program within the responsible entity. The issues raised in the Staff Assessment are addressed by the testing requirements found in Standard CIP-007 R1.

Response to VI.B: CIP-004-1 Issues Identified

Staff Assessment:

> "However, the Reliability Standard provides little direction concerning the elements of an appropriate awareness program… it does not identify minimum expectations regarding the content of an awareness program." [25]

NERC Response:

The awareness training program is "on-going reinforcement in sound security practices," and is intentionally non-specific to allow for adaptability and flexibility on the part of the responsible entity. The Frequently Asked Questions document provides guidance on the characteristics of an awareness and training program. The program which is intended to have "minimum expectations" is the training program described in Requirement R2.

[24] Staff Assessment at 21.

[25] Staff Assessment at 22-23.

Staff Assessment:

> "NIST special publications 800-16 and 800-50 provide excellent guidance on training of personnel and practices that enhance the security posture of information systems." [26]

NERC Response:

NERC agrees the NIST publications provide excellent guidance as reference documents. However, any elements of or references to NIST publications that would be made mandatory under Section 215 must first go through the standards development process.

Staff Assessment:

> "[I]t is not clear whether the Requirement takes the interconnectivity of systems into account or whether it focuses solely on Critical Cyber Assets themselves as opposed to those assets plus any networking hardware or software linking them."[27]

NERC Response:

The applicability section of the standards specifically excludes communication networks and data communication links between discrete Electronic Security Perimeters. However, because active communications hardware and software may reside within the defined Electronic Security Perimeter, and hardware and software acts as an Electronic Access Control (which defines the Electronic Security Perimeter), a subset of networking hardware and software is included in this requirement.

Staff Assessment:

> "Non-critical Cyber Assets … can impact the security of Critical Cyber Assets, yet this relationship may not be addressed if training is limited to the Critical Cyber Assets themselves." [28]

[26] Staff Assessment at 23.

[27] Staff Assessment at 23.

[28] Staff Assessment at 23.

NERC Responses:

The requirement is to train all personnel with "access to Critical Cyber Assets." Training is required for authorized personnel regardless of whether their access is unescorted physical or electronic access. This requirement applies to all who have access, regardless of their individual function, from those granted administrative access to Critical Cyber Assets to those performing a janitorial function who would have unescorted physical access to the Critical Cyber Assets. Electronic access would include those personnel who use the same network connection to access non-critical Cyber Assets within the same Electronic Security Perimeter as the Critical Cyber Assets. Some of the examples referenced by the Staff Assessment (e.g., switches, routers) may in fact be "essential to the reliable operations" of the designated Critical Asset, and therefore be Critical Cyber Assets. As such, personnel authorized access to those networking devices would be subject to the same training requirements as all others granted access to the Critical Cyber Assets.

The drafting team's intent was to train *all* personnel who *could* access a Critical Cyber Asset. As indicated above, networking equipment within the Electronic Security Perimeter is a likely a Critical Cyber Asset; therefore, under the existing language of the standard, anyone who accesses a non-critical Cyber Asset within the Electronic Security Perimeter will be accessing the network, and therefore will be required to be trained.

Staff Assessment:

> "Moreover, while the requirement specifies the minimum topics that training should cover, CIP-004-1 does not provide criteria for assessing the quality and adequacy of the training." [29]

[29] Staff Assessment at 23.

NERC Response:

The sub-requirements of R2 in CIP-004-1 list specific expected outcomes from the training. This is a more effective approach than describing the qualities of the training program itself, which is how the training results are achieved.

Staff Assessment:

> "Staff questions whether authorization should be granted for a period of up to 90 days without security training." [30]

NERC Response:

The 90-day period was provided in recognition that in order to maintain reliable operations of the bulk power system, it may be necessary to grant an individual access to the assets before formal training can be delivered. Many organizations already have regularly scheduled quarterly training, which would meet the 90-day requirement.

As discussed above, the diversity of field installations and infrastructure substantiates the need for less prescriptive standards, and the reliance in the standards on each responsible entity's exercise of reasonable business judgment and adherence to guidelines.

Staff Assessment:

> "Requirement R2 does not specify that successful completion of training and all required follow-up training within a stated timeframe is a *condition* of access to Critical Cyber Assets." [31]

NERC Response:

While it would be desirable to train all personnel prior to their access to any Critical Cyber Assets, certain conditions may require that personnel must be granted access prior to

[30] Staff Assessment at 23.

[31] Staff Assessment at 23.

specific additional training in Cyber Security processes and procedures in order to maintain or restore the reliable operation of the bulk power system as discussed above. Standard industry practice for many years has been to ensure anyone with access to sensitive systems has received adequate training; however, that training may not have been specific to the systems or environment where the access is provided. For example, in an emergency restoration, personnel with specialized knowledge may be required to access systems outside of their general assignments. Invoking mutual aid programs will bring personnel with adequate general training and knowledge from outside utilities to perform restoration functions.

The standard is clear that if access is granted, training *is required* within 90 days.

Staff Assessment:

> "[S]taff is concerned that Requirement R3 would allow access to Critical Cyber Assets during the investigative process." [32]

NERC Response:

As with training, the reliable operation of the bulk power system may require personnel be allowed to access the Critical Cyber Assets prior to the completion of the assessment process.

Staff Assessment:

> "[T]he lists [of personnel with authorized access] do not serve to keep un-cleared personnel from Critical Cyber Assets prior to completion of a personnel risk assessment." [33]

NERC Response:

While the list itself does not prevent access, it does provide for identification of personnel for which additional levels of review and escort may be assigned. As with training, the reliable

[32] Staff Assessment at 23.

[33] Staff Assessment at 24.

operation of the bulk power system may require that personnel be allowed to access the Critical Cyber Assets prior to the completion of the personal risk assessment process. Additionally, personnel who have access may be subject to escort and review during the investigative period. It is the method used to prove implementation of the access control policy for compliance purposes.

Staff Assessment:

> "Staff also notes that it may be appropriate for CIP-004-1 to include a provision that would direct a responsible entity to establish a categorization of access according to the exposure level or frequency of exposure to Critical Cyber Assets in the language of the standard." [34]

NERC Response:

The standard does not make this distinction. If the standard did make such a distinction it would not serve a useful purpose. Were the standards concerned with this level of granularity, the other timing requirements would not have been placed in the requirements. The standard is written to allow responsible entities to perform their primary function (maintaining reliable delivery of electricity), while concomitantly providing for the security of the information and systems.

The CIP-004-1 standard states in the purpose section "that [all] personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, … have an appropriate level of personnel risk assessment, training, and security awareness."[35] While not specific in the requirement, it is clear that the training provided to custodial staff would be very different than training provided to root-level system administrators for the same Critical Cyber

[34] Staff Assessment at 24.

[35] NERC Standard CIP-004-1, Section A.3: Purpose.

Assets. We believe this is captured in the "appropriate level" language of the standard's purpose.

Response to VII.B: CIP-005-1 Issues Identified

Staff Assessment:

> "The Measures and Compliance sections of CIP-005-1 focus on the applicable entity's documentation of the mapping of Cyber Assets, i.e., establishing an electronic security perimeter, and not the adequacy of the mapping or perimeter identification." [36]

NERC Response:

The establishment and documentation of the perimeter is clearly described in the requirements section; the measures and compliance sections are merely the method used to demonstrate during a compliance audit that the perimeter is defined and documented. The documentation serves to demonstrate that the perimeter is established and identified.

Staff Assessment:

> "To the extent that a non-critical Cyber Asset outside the Electronic Security Perimeter is interactive with a Critical Cyber Asset, Requirement R2 applies, which requires a responsible entity to control electronic access of all electronic access points to the Electronic Security Perimeter. This approach appears to be cumbersome in some instances, for example, where the non-critical Cyber Assets reside outside the Electronic Security Perimeter yet in the same room as the Critical Cyber Assets."[37]

NERC Response:

The Staff appears to equate physical proximity with electronic access. Physical co-location without electronic connectivity will enhance the overall security without compromising operational functionality. For example, a control room operator will, by necessity, have access

[36] Staff Assessment at 25.

[37] Staff Assessment at 25.

to HMI workstations which are within the Electronic Security Perimeter. The same control room operator may also need to have access to an Internet-connected workstation for the purposes of access to OASIS information. By necessity, both of these workstation terminals must be collocated with each other, but by allowing them to be on completely separate networks with widely varying levels of access controls, the control room operator can efficiently perform his job.

Requirement R2 only applies when access must be granted across the electronic security perimeter for access between a Critical Cyber Asset and a non-critical Cyber Asset outside the Electronic Security Perimeter. In this case, the physical location of the non-critical Cyber Assets in question is irrelevant. The Electronic Access Controls must be implemented to protect the Critical Cyber Asset; if the controls do not protect the Critical Cyber Asset, then the controls are not sufficient.

Staff Assessment:

> “Although CIP-002-1 and CIP-005-1 allow for discretion when identifying Critical Cyber Assets and Electronic Security Perimeter, such discretion across these Reliability Standards may result in inefficiencies or, worse, vulnerabilities in cyber security.” [38]

NERC Response:

While there is some discretion in the establishment of the Electronic Security Perimeter, there is no discretion involved in the selection of Critical Cyber Assets (as they are defined), or in the requirement that *all* Critical Cyber Assets are required to be located within a defined Electronic Security Perimeter. Most of the discretion involves the inclusion of non-critical Cyber Assets within the Electronic Security Perimeter. This discretion allows the responsible

[38] Staff Assessment at 25-26.

entity to exercise reasonable business judgment in deciding whether to re-locate the non-critical Cyber Asset or to protect it as defined in the standards. The compliance program will determine if a Responsible Entity exercised reasonable business judgment so as to satisfy the requirement.

Staff Assessment:

> "Staff, however, does not believe that the implementation of strong controls at access points to ensure authenticity of the access party is a matter of "technical feasibility." Such technology currently exists and every responsible entity that has identified Critical Cyber Assets should be able to implement such controls. Balancing an appropriate mix of protections and technology is part of achieving effective cyber security. However, Requirement R2.4 inappropriately suggests that a responsible entity may not have to implement **any** procedural or technical controls (or appropriate use of banners in Requirement R2.6) based on feasibility." [39]

NERC Response:

NERC disagrees with the generalized Staff assessment that "such technology currently exists," particularly for legacy implementations and substation environments. While NERC agrees that the Staff statement may be generally true in a modern Control Center environment, where common IT systems and implementations have been migrated into the control environment, it is not true for many existing field systems. In many cases, the Critical Cyber Assets are closed systems implementing closed and proprietary operating systems, software and protocols which do not support strong authorization controls or access control banners. The technical feasibility clause is included to accommodate the vast majority of systems that cannot be upgraded due to the nature of their legacy configurations, but still must be afforded some level of protection.

[39] Staff Assessment at 26.

Staff Assessment:

> "Logs should be reviewed frequently because automated alerts do not detect every attempt or breach." [40]

NERC Response:

NERC agrees with the Staff that logs should be reviewed frequently; however, a hard requirement for the review period cannot be specified due to the varied technologies used to gather and review the logs. Additionally, such a requirement is not consistent with the specificity issues discussed above. For example, geographically remote locations with slow telecommunications may not be able to support the kinds of review that can easily be accomplished at control centers which use high speed Local Area Network ("LAN") technology.

Moreover, the specific technology used in automated alerts can detect many attempts and breaches. Rather than looking for specific evidence of an attack or breach, the automated review can look at all events, and ignore the valid accesses, leaving a much smaller set of "questionable" events which can readily be analyzed. Ultimately, any detected event must be manually analyzed to determine if it was a real attempt or breach. NERC will focus on these alerts and associated documents in its readiness evaluations and compliance audits.

Staff Assessment:

> "Staff believes that a review every 90 calendar days is too infrequent." [41]

NERC Response:

There are potentially significant technical hurdles involved in the acquisition of logs from remote substation environments which cannot support high-speed communications technology,

[40] Staff Assessment at 26.

[41] Staff Assessment at 26.

much less the review of them. In some cases, it may be necessary to physically visit a remote site in order to extract the logs for review. It is not unusual for the process of visiting remote substations, extracting logs, and reviewing them to require more than two months to cycle through all of the remote locations.

Staff Assessment:

> "Further, for the reasons discussed above, the provision of "where technically feasible" in Requirement R3.2 suggests that an entity may not necessarily implement a monitoring process that detects and alerts on attempts or actual unauthorized access. Such technology appears to be available and if so, no entity should be exempt due to technical infeasibility." [42]

NERC Response:

As discussed above, while the Staff generalization may be true for a Control Center environment, NERC disagrees that such technology is readily available for a substation environment. Furthermore, as discussed above, there are potentially significant technical and logistical hurdles involved in the acquisition and review of logs from remote substation environments which cannot support high-speed communications technology.

Staff Assessment:

> "This Requirement [R4] is ambiguous in that it does not provide sufficient specificity to determine if a live vulnerability assessment is required as opposed to a paperwork assessment." [43]

NERC Response:

The requirement intentionally is written to allow either of the approaches the Staff suggests. While NERC acknowledges that some responsible entities do perform live testing, the testing performed is a subset of all possible testing. It is limited to testing issues that are specific

[42] Staff Assessment at 27.

[43] Staff Assessment at 27.

to the responsible entity's systems and circumstances, and is finely tuned following months of testing in a mirrored test environment. The drafting team was well aware of the dangers in performing any kind of active testing on a live system, and could not make such live testing a *requirement* of the standard. Live testing is known to cause software malfunctions in several widely-deployed EMS and SCADA systems, resulting in potential risk to the reliable operation of the bulk power system. Because the standard is written to allow a number of valid approaches to the assessment requirement, the responsible entity must determine the approach it will implement based on its own level of sophistication and its internal tolerance for risk.

Staff Assessment:

> "Ninety days appears to be an unacceptably long window because current and up-to-date documentation allows an entity the knowledge of how to handle an incident if one would occur." [44]

NERC Response:

NERC agrees with Staff that a shorter time frame for documentation update would be desirable; however, due to the number and kind of assets to be included in the update, as well as the geographical locations of some of the assets, the 90-day time period is appropriate, and a shorter mandatory timeframe would be unreasonable.

Response to VIII.B: CIP-006-1 Issues Identified

Staff Assessment:

> "This may imply that the Cyber Security Incident Response Plan should cover responses to physical security incidents, but CIP-008-1, which addresses the response plans, does not seem to address physical security aspects such as preservation of physical evidence." [45]

[44] Staff Assessment at 27.

[45] Staff Assessment at 28.

NERC Response:

The rules and requirements for the preservation of evidence, presumably in anticipation of legal action, are onerous and beyond the scope of most entities in the electricity sector. What are really necessary are extensive storage facilities, certifications and constant training and exercise of procedures. In addition, the preservation of such physical evidence does not have a direct impact on the reliability of the bulk power system, and in fact, may potentially cause new or additional reliability and power delivery problems during the evidence preservation and collection periods. The primary goal of the responsible entity must be to ensure the safe and reliable delivery of electric power to its customers, and to maintain a reliable and functioning bulk power system. Any restoration plans must address the delicate balance between performing security functions such as preserving evidence and rapidly and safely restoring service.

Staff Assessment:

> "While CIP-006-1 in general does identify topics that should be addressed in a Physical Security Plan, it does not include action(s) to be taken in response to a physical security breach. The plan should specify responsibilities and required communications in such an event." [46]

NERC Response:

These standards are cyber security standards, and as such are not intended to cover all aspects of physical security. The physical security requirements embodied in CIP-006-1 are for the physical protection of Critical Cyber Assets. Specific response plans are a requirement of CIP-008-1, not CIP-006-1. While these may be included in the Physical Security Plan, their requirement is not within the scope of CIP-006-1. For example, the Physical Security Plan is required in CIP-006-1 Requirement 1.

[46] Staff Assessment at 28-29.

Staff Assessment:

> "However, it [R1.1] does not provide guidance on how to address this problem, i.e., how an "alternative measure" would be identified or determined to be adequate." [47]

NERC Response:

As has been discussed previously, the NERC standards are performance based "what" standards, not "how" standards. The range of acceptable "alternative measures" is very broad, and each responsible entity is required to ensure appropriate protection while meeting the requirements of the standards. For example, personnel safety concerns governing acceptable accesses to equipment in a switch yard or power plant may require unique and creative solutions. The fundamental requirement remains, however, to "have" an alternative measure, not to specify what the alternative is.

Staff Assessment:

> "The ninety-day response time appears to be an excessively long window for adjusting the Physical Security Plan to account for any changes. … [I]t should not be burdensome to update the Physical Security Plan within a much shorter period of implementing a physical security change." [48]

NERC Response:

As discussed above, due to the nature and type of the facilities and their locations, the 90-day time period is appropriate. The need for a number of internal reviews and approvals by various people or groups of people in order to adopt any changes also supports the 90-day period as appropriate.

[47] Staff Assessment at 29.

[48] Staff Assessment at 29.

Staff Assessment:

> "Requirement R2 does not require or suggest that the method(s) employed to control physical access should consider the characteristics of an access point and the criticality of the protected assets." [49]

NERC Response:

Throughout the standards, assets are classed as either critical or non-critical, with no subjectivity involved in determining their "level" of criticality. As such, all assets classed as "critical" must be afforded the same level of protection, regardless of their location or perceived "level" of criticality. The specific implementation of protection must be functionally equivalent and sufficient at all locations. Additionally, as discussed above, the determination of "level" of criticality is subjective, and cannot be readily measured or assessed for compliance.

Staff Assessment:

> "The logging requirements of Requirement R4, along with the access log retention provisions of Requirement R5 should support the incident reporting and response planning required by Reliability Standards CIP-001-1 and CIP-008-1. If a computerized access screening and logging is performed, it appears important that the resulting data should be on a system that is periodically saved, backed up and stored in a retrievable fashion separate from the machine recording the information. However, neither Requirement R4 nor Requirement R5 addresses this issue. In addition, there is no requirement to review logs within a specified timeframe (e.g., daily, every-other day, or weekly)." [50]

NERC Response:

The log monitoring and retention requirements of R4 and R5 *are* intended to be used in support of the incident response requirements of CIP-001-1 and CIP-008-1. The "review" requirement is included in Requirement R3, and therefore does not need to be repeated in Requirement R4. Requirement R4 is used to collect logging data for use after a suspected

[49] Staff Assessment at 29.

[50] Staff Assessment at 29.

incident has been detected during the monitoring process. Furthermore, there is no *requirement* for computerized logging (although computerized logging is an acceptable solution to the log collection requirement).

Additionally, the Staff Assessment incorrectly assumes that any generated logs from remote locations can be readily collected and stored for a frequent review. In many cases, the telecommunications infrastructure connecting these remote locations cannot support the rapid and frequent collection of log data, especially if it is voluminous. Additionally, the remote location of some sites makes frequent visits to collect and store log data impractical as discussed above.

Staff Assessment:

> "Staff believes that document retention should not be limited to reportable incidents and that all physical access logs should be retained for at least one year. Thus, two different responsible entities may suffer the same physical intrusion against similar assets and one could consider it "reportable" while the second does not." [51]

NERC Response:

Due to the varied logging methodologies employed, maintaining all logs for the one-year period is impractical. The requirement to capture and review logs within the 90-day period, and keep logs related to reportable incidents serves to keep the most important logs without imposing an undue burden on the responsible entities. Additionally, keeping logs for a longer period of time (in response to Requirement R5), without continuous review of them, serves no useful purpose. Implementing a continual review of logs is resource intensive and would not be justified.

[51] Staff Assessment at 30.

Staff Assessment:

> "[Standard] CIP-008-1 … does not provide guidance as to what constitutes a "reportable incident." While CIP-008-1 specifies that cyber security incidents are to be reported to Electricity Sector Information Sharing and Analysis Center (ES ISAC), there exist no such directive in the CIP's standards concerning physical security incidents. *See* CIP-001-0 and CIP-008-1 (R1.3)."[52]

NERC Response:

These standards are cyber security standards, and were never intended to fully address physical security requirements. However, CIP-008-1 deals with reporting all manner of "reportable incidents" against Critical Cyber Assets, including physical security issues. Standard CIP-001-1 deals with "sabotage events", and is not specific as to the type and nature of the reportable events; therefore because CIP-001-1 is not limiting, both physical and cyber "sabotage" are included in its requirements.

Staff Assessment:

> "Staff questions whether consideration should be given to testing the higher level critical physical security mechanisms and systems more frequently, with testing and maintenance records maintained for the full 3 year testing cycle." [53]

NERC Response:

As discussed above, the standards do not make a distinction between levels of criticality. Therefore, testing of "higher level critical" systems cannot be performed, because all Critical Assets have the same "level" of criticality.

[52] Staff Assessment at 30.

[53] Staff Assessment at 30.

Response to IX.B: CIP- 007-1 Issues Identified

Staff Assessment:

> "One potential improvement would be to require in Requirement R1.2 that the responsible entity document how each significant difference between the operation and testing environments is considered and addressed." [54]

NERC Response:

Any test environment that has a "significant difference" from the production environment is not a true "reflection" of the production requirement, as required in R1.2.

Staff Assessment:

> "Staff seeks comment on whether this option [the acceptance of risk where ports and services cannot be disabled] is appropriate. In any event, if it is appropriate, clear guidance is needed that explains the limited circumstances in which it is appropriate." [55]

NERC Response:

Many situations exist where ports and services must be left enabled due to operating system or Original Equipment Manufacturer (OEM) / vendor support requirements or lack of information from vendors describing the rationale for leaving a port or service enabled, for instance where the underlying operating system requires a range of ports to remain open, and that operating system software cannot be modified or disabled. In these cases, the risk associated with leaving the ports or services enabled must be balanced against the function performed by the operating system, or the ability to maintain a supported and supportable configuration. In these cases, the definite reliable and supportable operation of the system outweighs the potential cyber security impact of an undetermined breach of security. The explanation of the "limited

[54] Staff Assessment at 32.

[55] Staff Assessment at 32.

circumstances" is captured in the requirement to document compensating measures. Moreover, documentation of the acceptance of risk highlights for management the potential impacts and rational balancing judgment made.

Staff Assessment:

> "Staff is concerned that this requirement [for a patch management program] permits a wide variation of processes for patching a system because, in Requirement R3.2, it allows for either "compensating measures" or "acceptance of risk" in lieu of mitigating risk exposure through a patch program."
>
> "Again, staff is concerned regarding the implications of an "acceptance of the risk" option. An effective Reliability Standard clearly cannot simply offer a responsible entity a choice between installing a patch or accepting the risk of not doing so. In addition, staff is not aware of any situation where at least some form of mitigation would not be possible. Staff seeks comment on whether there are situations where such mitigation is impossible and/or situations where an acceptance of the risk would be the reasonable alternative." [56]

NERC Response:

NERC is aware of at least one instance of a patch that cannot be installed because of a large chain of other upgrades and prerequisite patches that would result in the loss of critical and required functionality in a control system. NERC also believes that the "acceptance of risk" is not a permanent solution but would be used during a period where testing and other required upgrades may be accomplished. Further, NERC is concerned about unintended consequences of the patch installation process requirements (e.g., downtime, reboot, performance impacts, etc).

NERC is also concerned that a stricter requirement may require the installation of unnecessary patches for software that is either not installed or non-functional in the implementation of the patched system. In this case the risk of unnecessary modifications to a

[56] Staff Assessment at 33.

functioning system must be balanced against the potential security vulnerability mitigated by the patch.

Further, NERC is concerned about implementing language in the standard which would seem to require installation of patches on platforms where patches cannot be implemented due to architecture, operating environment, or warranty issues. If a platform provides no provision for updating its operating software, then patches *cannot* be installed. If any modification to the software would void the warranty and eliminate reasonable support from the vendor, it would be imprudent for a responsible entity to install a patch.

Staff Assessment:

> "However, CIP-007-1 [R4] does not provide any direction on how to implement this type [anti virus] of protection or where it should be deployed."
>
> "Moreover, the Reliability Standard does not suggest the use of a multi-layered, defense in depth strategy through the use of various products from multiple vendors."
>
> "As discussed elsewhere, staff is concerned that the use of the phrase "where technically feasible" creates unnecessary discretion for exception to Requirement R4."
>
> "No explanation is provided as to why anti-virus or malicious software prevention tools could not be implemented, and no standards are provided for assessing those situations. We seek comment on what types of compensating measures are available to protect from the attacks that the malicious software prevention and the anti-virus tools are meant to stop. Also, what would be the basis for justifying an "acceptance of risk" option and what would be the consequences of a documented "acceptance of risk" should a successful cyber attack occur?" [57]

NERC Response:

As discussed above, the standards are performance based: they do not specify how to perform a function, only that the requirement must be met. The responsible entity must

[57] Staff Assessment at 33-34.

implement a solution that meets the requirement, but is not restricted with regard to how to do so. Achieving the required outcome is not restricted by whether the anti-virus solution is implemented at a border, on an in-line device, or on the Critical Cyber Asset itself, so long as the implemented solution meets the stated requirements.

The Staff's comment concerning lack of a "suggestion" to use a multi-layered strategy is not appropriate to these standards. A multi-layered defense, as described by the Staff, may be appropriate in a best practice document, but not in these mandatory standards. Moreover, the use of the term "suggestion" is inappropriate when discussing requirements: either something is required, and therefore written into the standards and measured; or something is not required, and there is noting in the standards that makes it required.

NERC is aware of one specific control system vendor that has publicly stated in an open forum that, while *allowing* the installation of anti-virus, it does not support its use if performance or other problems arise as a result of its use. Additionally, many control systems are implemented using hardware and/or software for which no anti-virus software is commercially available, or which use proprietary closed systems (e.g., many Intelligent Electronic Device ("IED") protective relays).

During the development of the standards, the drafting team was concerned that a blind implementation of the requirement would result in noncompliance findings in cases where anti-virus products either did not exist (e.g., embedded operating systems), or where their performance impacts were known to be detrimental. These industry comments led to the technical feasibility clause in the requirement.

The "acceptance of risk" balances the required functionality of the system affected against the implication of a forced installation of anti-virus software. The "acceptance of risk" must also balance a known functionality loss (e.g., a loss of performance) with the *potential* loss due to a virus infection.

An example of a compensating measure is a border defense scanning process (i.e., virus scanning in a firewall), which allows the Critical Cyber Assets to be protected without any direct impact on their function or performance. Many other examples or implementations exist. Not all compensating measures are appropriate in all circumstances. Implementation of a compensating measure is not intended to be a primary or universal solution.

Staff Assessment:

> "The Requirement [R6.3], however, is limited to situations where this action is "technically feasible." While understanding that logs can grow to a burdensome size, we question the need for the phrase "technically feasible" in Requirement R6.3, and seek comments on what circumstances would make it infeasible to maintain logs." [58]

NERC Response:

The size of the log is irrelevant to technical feasibility. The Staff Assessment incorrectly assumes that all devices of interest have the capability to create logs, or that the devices provide the capability to capture "security related" information. For many installed devices in power plants and substations, there is no log generation capability. If there is no capability to generate logs, then it is technically infeasible to maintain logs.

Staff Assessment:

> "If an entity is frequently (1 to 5 days) reviewing system event logs then maintaining them for 90 days may be adequate. However, if an entity infrequently reviews these logs, then holding them for only 90 days seems inadequate. … If audits take longer than 90 days to initiate, the non-reportable incident data will be lost. This undercuts the effectiveness of audits and forensic work." [59]

[58] Staff Assessment at 34.

[59] Staff Assessment at 34.

NERC Response:

The language of R6.1 and R6.5 includes the requirement to review the logs prior to their disposal. The industry has been informed of this during the NERC Cyber Security Training sessions.

The Staff Assessment incorrectly assumes that any generated logs from remote locations can be readily collected for such a frequent review. In many cases, the telecommunications infrastructure connecting these remote locations cannot support the rapid and frequent collection of log data, especially if it is voluminous. Additionally, the remote location of some sites makes frequent visits to collect and store log data impractical. Additionally, there are no requirements for "forensics" in the standards.

Staff Assessment:

> "CIP-007-1 [Requirement 6.5] nowhere specifies how frequently this review should occur and what should be considered in the review. In addition, there is no specific guidance on how data should be saved, backed up and stored in cases where computerized cyber incident monitoring and logging is performed. … We seek comment on this perspective." [60]

NERC Response:

The review period is within ninety days (Requirement R6.4). As discussed above, the standards are performance based, and do not specify how a requirement is to be implemented, only the results.

Staff Assessment:

> "Effective protection requires that discarded or redeployed assets undergo high quality degaussing. Staff seeks comments on this issue." [61]

[60] Staff Assessment at 34.

[61] Staff Assessment at 35.

NERC Response:

"High quality degaussing" is an option which meets the requirement to "destroy or erase the data storage to prevent unauthorized retrieval of sensitive cyber security or reliability data"; however, many other options are also available. Specifying that degaussing be performed would not be applicable to non-magnetic media (such as paper tape, or semiconductor memory). Any method that does not result in "prevent[ing the] unauthorized retrieval of sensitive cyber security or reliability data" does not meet the requirement.

Staff Assessment:

> "[Requirement R8] provides no direction on what features, functionality, quality, adequacy, appropriateness, capabilities and vulnerabilities upon which the vulnerability assessment process should focus." [62]

NERC Response:

As discussed in the response to the Staff comment to Standard CIP-005 Requirement R5, each responsible entity must determine the approach it will implement based on its own level of sophistication and its internal tolerance for risk. Each environment and implementation is different: making use of different external connections with differing security postures; different border protections; and implementing different internal solutions. Any additional specificity would be impossible to describe for all possible situations, and would not be productive.

Furthermore, as discussed in the general comments section, "quality, adequacy [and] appropriateness" are subjective quantities, and cannot be objectively described in requirements or measures, and are therefore not auditable.

[62] Staff Assessment at 35.

Staff Assessment:

> "Requirement R8.4 directs that an action plan be formulated to remedy or mitigate the vulnerabilities identified in the assessment. However, there is no timeframe for completion of the action plan." [63]

NERC Response:

Requiring a specific timeframe for completion of an action regardless of its complexity serves no useful purpose because the timeframe will depend on the actions required. The range of potential mitigations can range from a simple "five-minute" fix to a complete re-architecture or replacement of the entire system. The requirement to document the "execution status" of the action plan serves to keep the action plan on track.

Staff Assessment:

> "It [Requirement R9] specifies that documentation should be updated within ninety days, which appears to be an excessively long timeframe." [64]

NERC Response:

Due to the nature and type of the facilities to which the documentation updating requirement relates, and their locations, the 90-day time period is appropriate, particularly in light of the potential need for internal reviews and approvals by a number of people or groups of people before a documentation change can be effected.

Response to X.B: CIP-008-1 Issues Identified

Staff Assessment:

> "Requirement R1 … does not provide definition on the characteristics of a "reportable" incident. … [I]t is possible that two different entities could experience the same cyber attack on similar assets; one would report it and the

[63] Staff Assessment at 35.

[64] Staff Assessment at 35.

> other would not, depending upon each entity's interpretation of a "reportable" incident." [65]

NERC Response:

Each responsible entity is required to develop the required procedures. The definition of a "reportable incident" is currently undergoing extensive industry debate and discussion.

Staff Assessment:

> "[T]here is no defined time frame for sending the report."
>
> "However, compliance with ESISAC Indications, Analysis and Warnings Program's (IAW) Standard Operating Procedure (SOP) is only voluntary, leaving the Standard unclear as to which events should be reported as critical cyber security incidents and with uncertainty of appropriate reporting time period. Staff seeks comment whether CIP-008-1 should incorporate ESISAC's one hour reporting limit or some other deadline that would provide adequate time for another responsible entity to take meaningful precautions." [66]

NERC Response:

During an event, the primary responsibility of the responsible entity is to restore the reliable operation of the bulk power system, and to restore power delivery to its customers. Filing a report of the incident is secondary to this primary mission.

NERC agrees that rapid reporting is desirable; however, imposing a requirement that a report be filed within a specific time period is inadvisable because when an event occurs, the need to file a report within a specific time frame should not be the entity's primary concern. A requirement to submit a report within a specific time period may result in a responsible entity needing to decide whether to be non-compliant by not restoring reliable operations, or being non-

[65] Staff Assessment at 36.

[66] Staff Assessment at 37.

compliant due to a missed reporting deadline. Clearly, restoration of operations must take precedence over filing a report within a specific timeframe.

The IAW procedures are intentionally not part of this standard. They are classified as a guideline because they have not been through the ANSI approved standards development process. The requirement is to report incidents to the ES ISAC, with the implication that the incidents are to be reported using an established ES ISAC reporting protocol, which includes, but is not limited to, following the IAW procedures.

Staff Assessment:

> "The paper drill option [allowed in Requirement R1.6], however, may not reveal flaws or weaknesses in the Response Plan. Staff seeks comment as to whether full operational exercises should be required by the Reliability Standard. The benefit gained from uncovering unexpected complications may only be realized through full operational exercises." [67]

NERC Response:

There are many instances in substations or power plants where backup or fully functional test systems do not exist, making a "full operational exercise" an extremely risky proposition. A universal requirement for a "full operational exercise" therefore may be unduly disruptive and burdensome to reliable operations, and represent a threat to the overall reliability of the bulk power system. NERC, therefore, believes that table-top exercises are sufficient to test the effectiveness of the Response Plan. This is consistent with the long accepted practice of table-top drills to test blackstart procedures, for many of the same reasons.

Staff Assessment:

> "Requirement R1.6 makes no references to follow-up steps, such as the need to maintain a collection of "lessons learned" as a result of testing the CSIRP and to

[67] Staff Assessment at 37.

> apply them to plan improvement. Staff seeks comment about documentation and implementing "lessons learned."" [68]

NERC Response:

Collection and maintenance of lessons learned, and "plan improvement" is included in the "update" language of requirement R1.4.

Response to XI.B: CIP-009-1 Issues Identified

Staff Assessment:

> "Requirement R1 … does not provide or require a definition of what constitutes a precipitating event or condition that triggers the need to implement the plan. … Staff seeks comment on whether more description would ensure that responsible entities implement recovery plans that are designed to address a wide enough range of recovery scenarios." [69]

NERC Response:

The determination of "precipitating events" is intentionally left up to the responsible entities. Providing additional detail will limit the scope of the potential "precipitating events" to only those specified, and will not provide for the required flexibility. The requirement for "events or conditions of varying duration and severity" allows the responsible entity to develop a range of plans, which may not be very specific to individual events, but which will be readily adaptable when the plans need to be invoked in response to a specific incident.

Staff Assessment:

> "In addition, there is no directive regarding whether forensics collection should occur prior to, contemporaneously with, or after recovery of the Critical Cyber Assets." [70]

[68] Staff Assessment at 37.

[69] Staff Assessment at 38.

[70] Staff Assessment at 38.

NERC Response:

There are no bulk power system reliability issues associated with forensic data collection; therefore this cannot be a requirement of the standard. Furthermore, there exists the distinct possibility that the collection of forensic data could impede the restoration of the Cyber Asset, thereby directly affecting the reliable operation of the bulk power system. Each responsible entity must implement procedures which consider the balance between any data collection and actions required to perform a rapid restoration of electric power transmission. Staff makes the improper assumption that, in the likely event that restoration takes precedence over data collection, after-the-fact recovery of incident data is technically possible on most legacy equipment. Because there are no guarantees that this after-the-fact data collection is possible, it cannot be made a requirement.

Staff Assessment:

> "Staff seeks comment on whether full operational exercises should be required by this Reliability Standard to aid in identifying potential problems and in realizing opportunities for improving recovery plans." [71]

NERC Response:

NERC believes that table-top exercises are sufficient for the same reasons discussed above for the response plan. In many cases in substations or power plants, backup or fully functional test systems do not exist, making a "full operational exercise" an extremely risky proposition. A universal requirement for a "full operational exercise" therefore may be unduly disruptive and burdensome to reliable operations, and represent a threat to the overall reliability of the bulk power system. NERC, therefore, believes that table-top exercises are sufficient to

[71] Staff Assessment at 38.

test the effectiveness of the response plan. This is consistent with the long accepted practice of using table-top drills to test blackstart procedures.

NERC also questions the exact definition of a "full operational exercise." Most exercises, including the vast majority of government-run and government-sponsored industry exercises, include a significant amount of table-top components, rather than relying solely on actual or simulated invocation of the plans.

Staff Assessment:

> "We therefore question whether a 90-day time lag [for the update of recovery plans] is consistent with this objective." [72]

NERC Response:

Due to the number, kind and location of the assets, in particular field assets, to which the recovery plans apply, a shorter timeframe is impractical. Internal reviews and approvals by a number of people or groups of people may be required before a change in a response plan can be effected.

Staff Assessment:

> "However, Requirement R4 does not require the backup to be tested before it is stored and relied upon for restoration purposes. Staff believes the Requirement should specify that, when significant changes are made to the operational control system, a backup should be made for recovery purposes and that it should be tested as part of the system change before it is stored and assumed to be operational." [73]

NERC Response:

NERC believes that a universal testing of all backup prior to storage is impractical, and that the need for such universal testing is mitigated by the generally accepted practice of

[72] Staff Assessment at 38.

[73] Staff Assessment at 38-39.

maintaining multiple generations of backup for this express purpose. Further, the general use of backups for routine recovery purposes, as well as the annual testing requirement, serves to verify that the backup process and equipment is working properly.

The "backup made for recovery purposes" is contained in the "supporting configuration management activities" located in CIP-003-1 Requirement R6.

Staff Assessment:

> "There are no specifications as to what actions should be taken in the event of a failure in testing. … Due to the impact and importance of backup media, staff requests comments on this issue and whether testing should also be conducted on a more frequent basis." [74]

NERC Response:

Due to the varied nature of backup technology, the standards cannot predict what technology will be used, and cannot therefore be prescriptive in requiring specific actions in response to testing. It is obvious that if a failure of the backup is encountered, the backup should be recreated. The one-year time frame was developed from industry consensus, and as indicated in the immediately preceding response, routine use of backups, as a matter of course, exercises selected media more frequently that the minimum one-year specified.

Response to XII: NERC Security Guidelines

Staff Assessment:

> "Staff believes that the Security Guidelines provide a useful enhancement to the implementation of the CIP Reliability Standards. However, because they are not referenced in the CIP Reliability Standards, the Security Guidelines may be overlooked and not be used to enhance reliability." [75]

[74] Staff Assessment at 39.

[75] Staff Assessment at 40.

NERC Response:

The Security Guidelines (and the Frequently Asked Questions document) are provided by NERC to the industry to increase the overall security posture of the industry, and to aid the implementation of security practices, including providing “best practice” type guidance to the implementation of the cyber security standards. However, as *guidance*, the recommendations and practices are not and cannot be made mandatory as the reliability standards are. As previously discussed concerning the NIST SP-800 series guidelines, the guidance and recommendations cannot be incorporated by reference into a NERC standard, because they have not gone through the ANSI approved standards development process. Even if the process allowed for referencing external documents, their inclusion would require that lack of adherence to each and every suggestion, recommendation, or provision of the external documents would potentially be a noncompliance.

The primary benefit that the Guidelines can provide is by providing “how” guidance, where the standards cannot, as previously discussed. Since the Guidelines are not mandatory, the guidance contained therein is merely a suggestion or recommendation, not a mandate. Responsible entities are encouraged to review the recommendations in the Guidelines and implement them, or to use the information contained therein to develop new and novel approaches that were not considered or envisioned during the development of the Guideline.

Guidelines are much more fluid than the standards, and can be updated or re-written on a much faster track than the standards process allows. Since the Guidelines are not mandatory, their approval process is much more streamlined than the process for a standard. As a result, Guidelines can easily be adapted to emerging and evolving technologies, to provide additional relevant assistance to the industry. As lessons are learned through implementation, they can readily be captured as revisions to the Guidelines. However, since the provisions in the Guidelines are not mandatory, any additions or changes to them will not require a complete review and overhaul of solutions implemented using a previous version of the Guidelines.

There is a concern that if the Guidelines (or any "how" provisions in the standards) are made mandatory, then the industry will be incented to only implement from a limited set of solutions, and only implement the documented minimum solution. NERC believes this would be counterproductive and not in keeping with the intent of the Guidelines.

Submission Contents