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

RM06-22-000

(This page intentionally left blank)

Table of Contents

(This page intentionally left blank)

I. EXECUTIVE SUMMARY

This Staff Preliminary Assessment (Assessment) addresses the eight proposed Critical Infrastructure Protection (CIP) Reliability Standards (CIP-002-1 through CIP-009-1) that the North American Electric Reliability Corporation[1] filed with the Commission on August 28, 2006 for approval under section 215 of the Federal Power Act (FPA). Pursuant to section 215, a proposed Reliability Standard must be approved by the Commission for it to be mandatory and enforceable. The CIP Reliability Standards primarily address cyber security and, in one standard, physical security. The Commission intends to address the CIP Reliability Standards in a separate rulemaking proceeding, in Docket No. RM06-22-000.[2]

The purpose of this Assessment is to analyze the proposed CIP Reliability Standards and solicit industry comment on them. The Assessment is limited to a technical review, and it makes no final determinations on whether the proposed CIP Reliability Standards satisfy the legal standard for approval set forth in section 215 of the FPA and the Commission's regulations. This review provides industry and affected stakeholders the opportunity to review Commission staff's analysis in advance of any proposed action. Such an open and inclusive process will ensure that all interested persons have an opportunity for comment and that the Commission has an adequate record upon which to discharge its statutory responsibilities.

Computer and communication network interconnection brings with it the potential for cyber attacks on these systems. The problem becomes particularly critical when several entities come under attack simultaneously. Staff's approach to analyzing the CIP Reliability Standards recognizes "defense in depth," a widely accepted strategy to address cyber threats that is both comprehensive and flexible. Defense in depth involves the layering of various defense mechanisms in a way that either discourages an adversary from continuing an attack or creates hurdles.

The following three common concerns pertain to many of the proposed CIP Reliability Standards:

---

[1] The August 28, 2006 filing (August 2006 Filing) was submitted by the North American Electric Reliability Council (NERC Council) and its affiliate, the North American Electric Reliability Corporation (NERC Corporation), which is the Electric Reliability Organization (ERO) (collectively NERC).

[2] *See* September 18, 2006, "Notice Announcing Rulemaking Process," Docket No. RM06-22-000.

- Discretion and Business Judgment: Each CIP Reliability Standard includes language that "Responsible Entities," i.e., entities to which the standard applies,[3] should interpret and apply the Reliability Standard using "reasonable business judgment." While individual applications are an important consideration when implementing a successful cyber security strategy, use of the term "business judgment" incorporates a degree of individual discretion into the CIP Reliability Standards that is inconsistent with the overall effectiveness of those Reliability Standards.

- Defining Compliance: Compliance with the CIP Reliability Standards must be understood in terms of compliance with their Requirements. Many of the proposed CIP Reliability Standards provide limited direction in the Requirements, and the Measures and Levels of Non-Compliance focus largely on proper documentation. This could be interpreted to suggest that possession of documentation, regardless of the quality of its contents, can demonstrate compliance.

- Applicability: Each of the CIP Reliability Standards applies to the same 11 classes of Responsible Entities, including NERC and Regional Reliability Organizations. As the Commission has expressed previously, it is doubtful whether the ERO, a Regional Entity[4] or a Regional Reliability Organization[5] is a user, owner or operator of the Bulk-Power System subject to mandatory compliance with an approved Reliability Standard. However, to the extent that they have network connections with Responsible Entities, it is important that NERC, Regional Entities and Regional Reliability Organizations comply with the substance of the CIP Reliability Standards. Also, from a cyber security

[3] The Reliability Standards CIP-002-1 through CIP-009-1 each specify the following Responsible Entities to which the Reliability Standard applies: Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

[4] A Regional Entity is an entity authorized to enforce the Reliability Standards on a regional basis pursuant to a delegation agreement with the ERO that has been approved by the Commission.

[5] The NERC Glossary of Terms Used in Reliability Standards (approved by the NERC Board of Trustees on August 2, 2006) (NERC Glossary) defines a Regional Reliability Organization as "(1) An entitiy that ensures that a defined area of the Bulk Electric System is reliable, adequate and secure. (2) A member of the North American Electric Reliability Council. The Regional Reliability Organization can serve as the Compliance Monitor."

perspective, there is no direct correlation between a Responsible Entity's size and its potential impact on Bulk-Power System reliability.

We highlight the fundamental importance of Reliability Standard CIP-002-1 (Critical Cyber Asset Identification). It requires a Responsible Entity to identify its Critical Assets and Critical Cyber Assets using a risk-based methodology. This requirement can be viewed as the decisive first step that can affect the chances for successful implementation of the remaining CIP Reliability Standards. An inadequate risk-based methodology may fail to capture some facilities that are essential to effective cyber protection. If that occurs, the effectiveness of the remaining CIP Reliability Standards will be diminished. In particular, CIP-002-1 does not provide specific direction on the nature and scope of a proper methodology and thus does not provide a basis for evaluating whether the selected methodology will result in the identification of all Critical Assets.

The Requirements in several of the CIP Reliability Standards allow a Responsible Entity the option of accepting the risk rather than complying with the technical provisions of the Requirement. For example, Requirement R3.2 in CIP-003-1 allows a "statement accepting risk" to justify an exception to the Responsible Entity's security policy. Also, as discussed in detail in the standard-by-standard assessment that follows, the lack of specific direction is a common issue throughout the CIP Reliability Standards. Without sufficient specificity, the Reliability Standards will not be effective and enforceable. A central purpose of this Assessment is to seek input on the proper balance between the need for specific guidance and allowing adequate flexibility and discretion to address evolving technologies and changing cyber threats.

Finally, under NERC's proposed Implementation Plan for the CIP Reliability Standards, it appears that Responsible Entities will not be audited for compliance until the second quarter of 2009 at the earliest. Staff is concerned about this delay and believes that it may be possible to begin assessing compliance at an earlier point in time.

II. BACKGROUND

The Energy Policy Act of 2005[6] (EPAct 2005), enacted in August 2005, included a new section 215 of the FPA to create a system of mandatory and enforceable Reliability Standards for the nation's Bulk-Power System. Section 215 of FPA authorizes the Commission to approve mandatory and enforceable Reliability Standards applicable to users, owners and operators of the Bulk-Power System. The statute authorizes the Commission to certify one entity as the ERO responsible for developing and enforcing mandatory Reliability Standards, subject to Commission oversight. Section 215(a) explicitly defines the term "Reliability Standard" to include requirements for the operation of existing Bulk-Power System facilities, including cyber security protection. The Commission adopted rules implementing FPA section 215 in Order No. 672, including rules for the development of Reliability Standards by the ERO and review by the Commission.[7]

In July 2006, the Commission certified NERC as the ERO.[8] In April 2006, NERC submitted a petition for approval of an initial set of proposed Reliability Standards. Commission staff issued its Staff Preliminary Assessment of those proposed Reliability Standards in May 2006.[9] In October 2006, the Commission issued a notice of proposed rulemaking addressing the NERC proposal.[10]

NERC began development of the CIP Reliability Standards in June 2002, well before passage of EPAct 2005. As an interim measure, NERC adopted an urgent action cyber security standard referred to as Urgent Action 1200 (UA 1200) in 2003. It was more limited in scope and applicability than the proposed CIP Reliability Standards. Development of the CIP Reliability Standards has taken place using NERC's standards

---

[6] Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005), to be codified at 16 U.S.C. § 824o (2000).

[7] *Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards,* Order No. 672, FERC Stats. & Regs. ¶ 31,204 (2006), *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[8] *See North American Electric Reliability Corporation*, 113 FERC ¶ 61,062 (July 20 2006), *order on reh'g*, 117 FERC ¶ 61,126 (October 30, 2006) (ERO Certification Order).

[9] *Federal Energy Regulatory Commission Staff Preliminary Assessment of the North American Electric Reliability Council's Proposed Mandatory Reliability Standards* (May 11, 2006) (May 2006 Staff Preliminary Assessment).

[10] *Mandatory Reliability Standards for the Bulk-Power System, Notice of Proposed Rulemaking*, 117 FERC ¶ 61,084 (2006); 71 Fed. Reg. 64,769 (2006). (October 20, 2006) (October 2006 Reliability Standards NOPR).

development process accredited by the American National Standards Institute. The CIP Reliability Standards were approved by the NERC Board of Trustees in May 2006 to supersede UA 1200.

Each proposed CIP Reliability Standard follows a consistent outline.[11] The outline topics most at issue in this Assessment fall under the following headings in the outline format: Purpose, Applicability, Requirements, Measures, and Compliance (including the sub-heading, Levels of Non-Compliance).[12]

As with the May 2006 Staff Preliminary Assessment, this Assessment is limited to a technical review, and it does not seek to determine whether the proposed CIP Reliability Standards meet statutory and regulatory criteria. The purpose of this Assessment is to solicit industry comment on the CIP Reliability Standards, including potential deficiencies and the appropriate process and timetable for addressing them. The goal is to provide a comprehensive and objective review in light of the guidance provided in EPAct 2005, Order No. 672 and the ERO Certification Order. Responsive comments to this Assessment will assist in informing and guiding the Commission in its future rulemaking on the CIP Reliability Standards.[13]

[11] *See* May 2006 Staff Preliminary Assessment at 11-12.

[12] Capitalized terms in this Staff Preliminary Assessment either refer to these Reliability Standard categories or are defined in the Commission's regulations or in the NERC Glossary.

[13] For more background information on the Commission's role in the approval of mandatory Reliability Standards and its use of staff analyses, *see* October 2006 Reliability Standards NOPR at P 12-32 and May 2006 Staff Preliminary Assessment at 1-16.

III. INTRODUCTION TO CYBER SECURITY ISSUES

A. The Challenge of Cyber Security

1. The Nature of Cyber Threats

The CIP Reliability Standards represent the most thorough attempt to-date to address cyber security issues for the Bulk-Power System. For many years the control systems for the electric grid have operated in a stand-alone environment without computer or communication links to the external Information Technology (IT) infrastructure. However, over the past ten years such stand-alone enclaves have been increasingly connected to both the corporate environment and the external world, and the Bulk-Power System is no exception. Computer and communication network interconnection brings with it the potential for cyber attacks on these systems by adversaries. The problem is particularly critical because such an attack can affect several entities across the country simultaneously. Such attacks have the enhanced potential to impact the Bulk-Power System rather than to simply disrupt the operation of some components.

Electronic access is the key to any successful cyber attack. Gaining physical access constitutes a major step toward achieving electronic access, but many other means are available. If an adversary can gain electronic access to a computer system, he may be able to gain control over that system and use it for his purposes. In today's environment, many infrastructure control systems have an electronic pathway that leads to the outside world, which can create a potential for access that is vulnerable to exploitation by an adversary.[14] We are aware that various industries have experienced computer exploitation of infrastructure control systems. To date, the majority of these intrusions have resulted in minimal disruption to the infrastructure itself, mainly because they can be attributed to hackers who probably did not realize that they had subverted a control system computer versus a standard office computer. However, these episodes clearly illustrate that electronic pathways do exist that lead to the control systems of our most critical infrastructures.

---

[14] A "control system" is a device or set of devices to manage, command, direct or regulate the behavior of other devices or systems. It is typically a specialized computer system or programmable logic controller that manages, commands, directs or regulates the behavior of other devices or systems in a physical environment, e.g. open or close switches or relays, start or stop motors, or control motor speed.. In the case of the Bulk-Power System, control systems consist primarily of sophisticated computer hardware and software designed to process the mass of real-time data associated with the Bulk-Power System and enable its reliable operation by, among other things, monitoring the grid through remote sensors, sounding alarms when grid conditions warrant, and operating equipment in field locations.

One threat to entities connected by these electronic pathways is an adversary who is capable of winding his way through various network connections to access computers, such as those used by control systems, and acquiring control of those computers. Once in control, an adversary can direct and perhaps damage physical assets. Another variation of such threats could include simultaneous attacks on multiple entities, perhaps through pre-positioned malicious code.

2. Cyber Security Strategies

The potential solution to such cyber threats is a strong cyber security posture by the entities that may be vulnerable to such attacks. A major challenge to preserve system protection is that system architectures change, technology changes, and threats change, all of which means that defenses must change. Traditionally, threats can change faster than defenses. To meet or minimize these risks, one widely recognized cyber security strategy is defense in depth.[15] While other strategies exist, Commission staff believes that defense in depth is a widely accepted, effective strategy to address cyber threats that is both comprehensive and flexible. This strategy involves layering of defense mechanisms in a way that discourages an attack and increases the potential that an entity will be alerted to the attack.

The development of a family security system provides a useful analogy for understanding the defense in depth strategy. For example, a home security system might include the following defenses: (i) a motion sensor light that goes on whenever someone gets close to the house, (ii) a video camera that records the approaches to the house, (iii) a door with a deadbolt lock and a chain, (iv) an alarm system that activates if a door or window is opened (along with the decals notifying a potential intruder that the system exists), and (v) a dog inside the house. Several of these items are designed to keep an intruder out, some are designed to activate if an intruder gains access, and some are designed to record the event if it occurs. Each of these measures provides some degree of protection and, in combination, they substantially increase the chances of successfully deterring a burglary. Moreover, whatever their shortcomings, they discourage attempted burglaries simply by

---

[15] In the context of information security, defense in depth represents the use of multiple computer security techniques to mitigate the risk of one component of the defense being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment. Varying security products from multiple vendors may be installed on different locations within the network, aimed at preventing a shortfall in any one defense leading to a wider failure. *See* National Security Agency Guide *Defense in Depth, available at* http://nsa2.www.conxion.com/support/guides/sd-1.pdf; *see also* Department of Homeland Security External Report # INL/EXT-06-11478, *Control Systems Cyber Security: Defense in Depth Strategies*, May 2006, *available at* http://csrp.inl.gov/documents/Defense%20in%20Depth%20Strategies.pdf.

suggesting to potential burglars that their time is better spent at the neighbor's entirely unprotected house.

Cyber defenses work in a similar manner. Some defenses, like firewalls, are designed to keep intruders out. Others, like intrusion detection systems, are designed to activate if someone gains access. Still others, like audit logs, are designed to inform the computer operator whether another person has gained access. The combination of all of these technologies, and how they are combined and implemented, determines whether the computer security personnel have effectively protected the Cyber Assets.

Whereas grid operations usually involve readily measured quantities and activities, cyber security involves a careful balance of the technologies available with the existing control equipment and the functions they perform. Compared to general grid operations, cyber security is in many ways as much, or even more, a matter of subjectively balancing physical and technical options rather than a purely objective task of achieving a single, steady, physical state. It does have a purely technical objective component, however, which consists of the various technologies that exist to defend computer systems. The task of balancing technical options comes into play as one selects and combines the various available technologies into a comprehensive architecture to protect the specific computer environment. The key to success is possessing cyber security standards that provide reliable direction on how to choose among alternatives to achieve an adequate level of security.

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. However, if standards lack sufficient specificity, they will provide little useful direction and may lead to flawed implementation of security mechanisms that provides inadequate protection. 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.

B. CIP Reliability Standard Common Issues

Before assessing each individual CIP Reliability Standard, we address certain matters common to many or all of the CIP Reliability Standards.

1. Business Judgment

As described above, cyber security is dependent upon variables such as the equipment and role of the entity and, for this reason, a successful security strategy cannot be

implemented without flexibility and some discretion. The proposed approach to the issue reflected in the CIP Reliability Standards could allow a degree of discretion that undermines their effectiveness. That approach involves reliance on "reasonable business judgment." The basic premise of the approach is set forth in the Purpose statement of Reliability Standard CIP-002-1, which provides that:

> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Each of the subsequent CIP Reliability Standards begins with a caveat that "Responsible Entities should interpret and apply the Reliability Standard using reasonable business judgment."

NERC states in its Frequently Asked Questions (FAQ) document[16] interpreting the CIP Reliability Standards that this phrase is meant "to reflect — and to inform — any regulatory body or ultimate judicial arbiter of disputes regarding interpretation of these Standards — that Responsible Entities have a significant degree of flexibility in implementing these Standards." The FAQ document notes that there is a long history of judicial interpretation of the business judgment rule and suggests that this history is relevant to the use of this rule in the context of the CIP Reliability Standards.

Staff notes as a general matter that the business judgment rule as interpreted by the courts permits corporate officers broad discretion to make business decisions that they consider to be in the best interest of the corporation. In some states, officers and directors will be deemed to have violated the rule only in cases of gross negligence. Moreover, the meaning of "reasonable business judgment" varies by jurisdiction, which could lead to different interpretations of whether an entity is in compliance based on venue. Thus, staff is concerned that the language 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.

---

[16] NERC included the FAQ document as part of its August 28, 2006 filing in Commission Docket No. RM06-16-000. The FAQ document is also available at ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf.

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. The rationale for the rule is that officers and directors, not judges, are best qualified in matters of business management. This point is reflected in NERC's FAQ document, which defines a reasonable business judgment in part as one "based on a rational belief that the decision is in the entity's business interest." However, the focus of all Reliability Standards is reliability of the Bulk-Power System. Moreover, NERC provides direction on technical, not business, matters. Therefore, the individual latitude in interpretation and application that would be allowed by assertion of the business judgment rule may undermine the effectiveness of the proposed CIP Reliability Standards.

As discussed above, NERC explains that it proposed to allow Responsible Entities to use reasonable business judgment when interpreting and applying the CIP Reliability Standards in recognition of "the differing role of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of assets needed to manage reliability, and the risks to which they are exposed." 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 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.

2. Defining Compliance

It is important to stress that compliance with the CIP Reliability Standards must be understood in terms of compliance with their Requirements. The Commission noted in its October 20, 2006 Reliability Standards NOPR that the "most critical element of a Reliability Standard is the Requirements."[17] This is because, "[a]ccording to NERC, the 'Requirements' within a Reliability Standard define what an entity must do to be compliant and establish an enforceable obligation . . . ."[18] The Commission explained that "[w]hile Measures and Levels of Non-Compliance provide useful guidance to the

[17] October 2006 Reliability Standards NOPR at P 105.

[18] *Id.* at P 104.

industry, compliance will in all cases be measured by determining whether a party met or failed to meet the requirement under specific facts and circumstances . . . ."[19]

These statements were made in the context of a rulemaking that has not been completed. They are particularly apposite to an analysis of the CIP Reliability Standards. 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.

3. Implementation Plan Compliance

According to the NERC Implementation Plan that accompanies the CIP Reliability Standards, Responsible Entities will not be required to be "Auditably Compliant," as defined by the Implementation Plan, until the second quarter 2009 (e.g., facilities of certain Transmission Operators) or second quarter 2010 for other facilities.[20] It may be possible to assess a Responsible Entity's level of compliance prior to it achieving full "Auditably Compliant" status. For instance, if a Responsible Entity is in the "Begin Work" phase, it has: (1) developed and approved a plan to address the requirements of a standard; (2) identified and planned for necessary resources; and (3) implemented the requirements. These are specific steps that can be examined and audited. The difference between "Compliant" and "Auditably Compliant" for many of the requirements is the accumulation of 12 months of records. 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.

---

[19] *Id.* at P 106.

[20] The Implementation Plan states that "To provide time for Responsible Entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin in 2007." The Implementation Plan is contained in NERC's August 28, 2006 Filing as Exhibit B, and is accessible at: ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Revised_Implementation_Plan_CIP-002-009.pdf.

4. Applicability

The CIP Reliability Standards raise several applicability issues. Each CIP Reliability Standard lists the same 11 Responsible Entities in its applicability section, as follows: Reliability Coordinators, Balancing Authorities, Interchange Authorities, Transmission Service Providers, Transmission Owners, Transmission Operators, Generator Owners, Generator Operators, Load Serving Entities, NERC, and Regional Reliability Organizations.

Reliability Standards approved under section 215 of the Federal Power Act apply to users, owners, and operators of the Bulk-Power System. The Commission, in the October 2006 Reliability Standards NOPR expressed concern whether a Regional Reliability Organization is a user, owner or operator of the Bulk-Power System and thus whether a Reliability Standard would be enforceable against a Regional Reliability Organization.[21] However, the Commission stated that it expects that the Regional Entities would become responsible, through delegation by the ERO, for the functions currently performed by the Regional Reliability Organizations.[22]

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. If Regional Entities and Regional Reliability Organizations do not also observe these cyber security precautions, their connections to users, owners or operators of the Bulk-Power System could introduce vulnerability to the grid. Such a connection could become a 'weak link' facilitating an adversarial attack focused on exploiting that communication path to the owners, operators and users of the Bulk-Power System.

The proposed applicability of the CIP Reliability Standards to NERC raises similar issues. These are the only proposed Reliability Standards that explicitly apply to NERC. It is questionable whether NERC as the ERO could be characterized as a user, owner or operator of the Bulk-Power System and, thus, that a Reliability Standard would be enforceable against NERC. As a potential alternative, instead of ERO compliance being required pursuant to the Reliability Standards, ERO compliance could be required pursuant the NERC Rules of Procedure. Nonetheless, as in the case of a Regional

---

[21] October 2006 Reliability Standards NOPR at P 56.

[22] *Id.* at P 57.

Reliability Organization or Regional Entity, cyber security concerns can arise to the extent that NERC has cyber connections with any user, owner or operator of the Bulk-Power System. 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.

Finally, there is the issue of the applicability of the CIP Reliability Standards to small entities. The widespread use of Cyber Assets creates the potential for broad applicability of the CIP Reliability Standards.

In Order No. 672, the Commission declined to adopt a formal definition for the term "user of the Bulk-Power System."[23] In the October 2006 Reliability Standards NOPR, the Commission indicated that it would determine applicability on a standard-by-standard basis.[24] It also stated that, while it is important to examine the impact a particular entity may have on the Bulk-Power System in determining applicability, a blanket waiver that exempted an entity below a certain size threshold from compliance with a Reliability Standard would not be appropriate. As an example, the Commission noted that "the reporting of a sabotage event required by CIP-001-0 may be important regardless of the size of the entity since such reporting helps others by putting them on notice of potential attacks to their own systems."[25]

The same consideration should apply to the other CIP Reliability Standards. As suggested above, the concept that some entities are too small to have a "material impact" on the Bulk-Power System does not necessarily apply to matters in the realm of cyber security. In particular, as described above, cyber oriented attacks can occur simultaneously over a geographically dispersed area. 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. For the user, owner, or operator that possesses such a connection, the possibility exists that the connection may be vulnerable to an adversarial attack that

---

[23] Order No. 672 at P 99.

[24] October 2006 Reliability Standards NOPR at P 43.

[25] *Id.* at P 51.

exploits that communication path to other users, owners, or operators of the Bulk-Power System. It is not the size of an entity that is critical but rather the potential for an entity to become a vector of vulnerability to the security posture of interconnected control systems. Since less-than-complete cyber security (i.e., weak links) can appear throughout a system, a cyber attack is not wholly determined by the size of the attacked entity. In light of this fact, we seek comment on how the impact of the CIP Reliability Standards might be addressed for smaller entities.

IV. CIP-002-1 – CRITICAL CYBER ASSET IDENTIFICATION

A. Description

Proposed Reliability Standard CIP-002-1 deals with the identification of Critical Cyber Assets. The NERC Glossary defines "Cyber Assets" as "programmable electronic devices and communication networks including hardware, software, and data." It defines "Critical Cyber Assets" as "Cyber Assets essential to the reliable operation of Critical Assets." Finally, the NERC Glossary defines "Critical Assets" as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

The Purpose statement of CIP-002-1 states that the Reliability Standard requires the identification - through a "risk-based assessment" - of the Critical Cyber Assets associated with Critical Assets that support the reliable operation of the Bulk Electric System. The Purpose statement also indicates that NERC intends that CIP-002-1 be understood as operating in conjunction with all the other CIP Reliability Standards to create a cyber security framework for identifying and protecting Critical Cyber Assets to support reliable operation of the Bulk Electric System. The Purpose statement notes that business and operational demands for maintaining a reliable grid increasingly rely on Cyber Assets supporting critical reliability functions and communications processes, across functions and organizations, for services and data, resulting in increased risks to Cyber Assets.

CIP-002-1 requires the Responsible Entity to develop a risk-based assessment methodology for identifying Critical Assets. It specifies certain types of assets that must be considered and also allows the Responsible Entity to consider other assets that support reliable operation. Once a list of Critical Assets has been developed, the Responsible Entity must identify which associated Cyber Assets qualify as Critical Cyber Assets essential to the operation of the Critical Assets. The Reliability Standard provides examples of select Critical Cyber Assets and some general guidance on Critical Cyber Asset identification. Finally, CIP-002-1 requires annual re-evaluation and approval by senior management of the lists of Critical Assets and Critical Cyber Assets.

The Reliability Standard contains one Measure for each Requirement. Each Measure requires documentation of the results of the actions specified in the corresponding Requirement. The compliance monitoring provisions specify the required frequency for updating Critical Asset and Critical Cyber Asset information and data retention requirements. The Levels of Non-Compliance are cast in terms of possession of documentation required by the Measures.

B. Issues Identified

While CIP Reliability Standards CIP-002 through CIP-009 function as an integrated whole, CIP-002-1 is a key to the success of the cyber security framework that these Reliability Standards seek to create. Because CIP-002-1 addresses the assessment methodology and process for identifying Critical Assets and Critical Cyber Assets, it represents the critical first step that can fundamentally affect the chances for successful implementation of the remaining CIP Reliability Standards. The methodology and process developed by a Responsible Entity must be stringent and rigorous. Otherwise, it may fail to capture some facilities that are critical to effective cyber protection and, as a consequence, leave them vulnerable to an attack that could threaten the reliability of the Bulk-Power System.

Specifically, Requirement R1 requires the Responsible Entity to use a risk-based assessment methodology to identify its Critical Assets. This approach is an improvement over the UA 1200 standard, which simply required that the Responsible Entity identify its Critical Assets without further guidance on how to perform this task. However, while CIP-002-1 requires use of a risk-based assessment methodology, it does not provide direction on the nature and scope of that methodology, its basic features or the issues it should address. The absence of more direction can result in the Requirement being unevenly executed, which may result in inconsistency and inefficiency. As a result, CIP-002-1 does not provide a basis for evaluating whether the risk-based assessment methodology adopted by a particular entity will permit effective identification of all Critical Assets. Again, we emphasize the importance of utilizing an appropriate assessment methodology because the subsequent Requirements of CIP-002-1, as well as those in CIP-003-1 through CIP-009-1, depend on the adequate identification of the Responsible Entity's Critical Cyber Assets.

Further, Requirement R1 of CIP-002-1 sets forth a list of assets that a Responsible Entity is to consider when identifying its Critical Assets. This represents an improvement over UA 1200, which provided no similar guidance and specifically excluded process control systems and electronic relays installed in generating stations, among other things, from the definition of Critical Cyber Assets. Earlier drafts of CIP-002-1 specified that assets enumerated in Requirement R1 must be included as Critical Assets. The final NERC-approved version provides that the enumerated list of assets must be considered, but not necessarily included, as critical. Depending upon the methodology chosen, the list of assets that must be considered may or may not result in any identified Critical Assets. In addition, CIP-002-1 explicitly excludes the communication networks and data

communication links between discrete Electronic Security Perimeters (e.g., to other entities).[26]

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 asset would not necessarily be identified in the Responsible Entity's analysis of Critical Assets. 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 whether this topic is an area for coordination and cooperation with other industries and government agencies.

Proper risk-based assessment methodology is essential in order to achieve sufficient scope and implementation of critical infrastructure protection. Requirement R4 states, in part, that a "Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets" and requires all Responsible Entities to "keep a signed and dated record of the senior manager or delegate's approval of the list of Critical Assets and Critical Cyber Assets (even if such lists are null)." However, 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. Thus, the number of Responsible Entities that do not have Critical Assets and Critical Cyber Assets is likely to be quite small. 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.

Keeping risk assessments timely and asset identification current is at issue in Requirements R2 and R3 of CIP-002-1. They require an annual risk assessment of assets and updates of the Responsible Entity's list of Critical Assets and Critical Cyber Assets "as necessary." However, there is no guidance on what would necessitate an update. In addition, while 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.

Lastly, senior management oversight is addressed by Requirement R4, which requires a senior manager or delegate(s) to approve the lists of Critical Assets and Critical Cyber

[26] Each CIP Reliability Standard specifically exempts "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." *See, e.g.*, CIP-002-1, Section Paragraph A.4.2.2.

Assets. This senior management involvement is important and should be extended to approving the risk assessment methodology adopted under Requirement R1. As noted above, the adequacy of the risk-based assessment methodology will determine the completeness of the Critical Asset and Critical Cyber Asset lists. A poor risk assessment methodology will likely result in an inadequate identification of critical assets and Critical Cyber Assets. Therefore, staff believes that senior management awareness and approval of the chosen risk assessment methodology is of critical importance.

V. CIP-003-1 – SECURITY MANAGEMENT CONTROLS

A. Description

Proposed Reliability Standard CIP-003-1 seeks to ensure that each Responsible Entity has minimum security management controls in place to protect Critical Cyber Assets identified pursuant to CIP-002-1. To achieve this goal, a Responsible Entity first must implement a cyber security policy that addresses the Requirements set forth in Reliability Standards CIP-002-1 through CIP-009-1. The Responsible Entity must also designate a senior manager to lead the Responsible Entity's cyber security program, and to authorize any exception to the cyber security policy. Further, a Responsible Entity must develop an information protection program to classify and protect sensitive information concerning Critical Cyber Assets, as well as an access control program to designate who may have access to the Critical Cyber Asset information. Finally, the Responsible Entity is responsible for developing a change control and configuration management program to oversee changes made to the Critical Cyber Assets' hardware or software.

B. Issues Identified

CIP-003-1 requires the Responsible Entity to prepare and implement a cyber security policy and procedures. This represents an improvement over UA 1200 because it provides some direction on what should be included in the cyber security policy and requires an annual review by senior management. Significantly, CIP-003-1 adds a requirement for a Responsible Entity to develop and maintain procedures for controlling changes and configuration of Critical Cyber Assets.

Requirement R1 requires the Responsible Entity to "document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets." The main substantive direction provided for developing such a policy is found in Requirement R1.1, which provides that the policy must address the Requirements set forth within standards CIP-002-1 through CIP-009-1. The requirement that senior management be involved and approve this policy should improve the prioritization of control system security within the entity, including allocation of resources. However, since many of the Requirements in the CIP Reliability Standards leave considerable discretion to each Responsible Entity, the scope and thoroughness of the cyber security policies developed could vary widely. Because Requirement R1 does not address the policy's adequacy, it is possible that this aspect of the Reliability Standard could actually mask certain security vulnerabilities by not requiring the development of cyber security policies that may have addressed these vulnerabilities. At best, it is difficult to determine whether this Requirement actually will result in an

improvement in control system security, and thereby improve the reliability of the Bulk-Power System.

A beneficial feature of Requirement R1's cyber security policy provision is that the policy must be readily available to all personnel who have access to the Critical Cyber Assets. It also requires that the policy must be reviewed and approved annually by the same senior manager who is assigned leadership responsibilities for implementation of the cyber security policy under CIP-003-1 (Requirement R2). This is notable because it seeks to ensure that those who must oversee application and use of the policy regularly review it.

Requirement R2 of CIP-003-1 requires that a senior manager be assigned overall responsibility for leading and managing the Responsible Entity's implementation of its cyber security policy. This manager also may approve any exception from the requirements of the cyber security policy. Having management involved in implementing the policy is critical to its success.

Requirement R3 of CIP-003-1 directs the Responsible Entity to document every instance where the Responsible Entity cannot conform to the security policy. Each exception must be authorized by the same senior manager assigned the responsibility for managing and implementation of the cyber security standards. That person must either explain why each exception is necessary and provide any compensating measures, or issue a statement of acceptance of risk for non-conformance. The exceptions to the security policy must be documented within 30 days of senior management approval, and be reviewed and approved annually to ensure that the exceptions are still required and valid. This Requirement 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.

Acceptance of risk in a cyber environment poses an additional issue. For interconnected control systems of various entities, an acceptance of a cyber risk by one entity is actually an acceptance of risk for all of those connected entities because the entity that initially accepted the risk is now the weak link in the chain. 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. For instance, if an entity has a control system that does not allow for the account passwords to be changed, the entity may accept that risk. However, if this entity's control system is attached to the corporate network and then to other entities, the fact that the system uses default passwords is a major vulnerability in the traditional IT environment and this vulnerability is present in the interconnected networks within the electric industry. It is not clear how reliability may be impacted if one entity "accepts the risk" while other entities on an interconnected network are not even aware of the vulnerability that may result from the first entity's

exception policy. Nor is it clear whether an entity can be aware of the actual risk it is "accepting" in an interconnected environment where its external partners may also "accept risk" (e.g., allow vulnerabilities to remain) when there is no oversight or regional perspective of the risks or vulnerabilities that are allowed to exist.

Requirement R5 of CIP-003-1 directs the Responsible Entity to implement a program for managing access to the protected Critical Cyber Asset information. The Responsible Entity must maintain and verify at least annually a list of personnel responsible for authorizing logical access[27] or physical access to the protected information as well as a list of personnel who are allowed to access the protected information. This Requirement 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.

Requirement R6 of CIP-003-1 requires the Responsible Entity to establish a process for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software. In IT infrastructure, an upgrade or patch of the operating system can actually undo the previous security patches. Since many control systems are installed on commercially available operating systems, this possibility becomes increasingly likely. While the Responsible Entity should be fully aware of the potential impact that vendor "emergency" modifications may have to the security of the control system prior to such modifications, balancing the interests of grid operations with the cyber security of the control systems may not always allow this. 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.

[27] Logical access in the Information Technology arena typically refers to cyber or electronic access.

VI. CIP-004-1 – PERSONNEL AND TRAINING

A. Description

Reliability Standard CIP-004-1 seeks to ensure that personnel having authorized cyber access or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training and security awareness. To achieve this goal, the Reliability Standard first requires Responsible Entities to establish a cyber security awareness program that provides ongoing reinforcement in sound security practices. This program must include security awareness reinforcement using various types of communications on at least a quarterly basis.

Responsible Entities must establish a cyber security training program for affected personnel that addresses policies, access controls, and procedures for the proper use of Critical Cyber Assets, physical and electronic access to Critical Cyber Assets, handling of asset information and recovery methods after an incident. Responsible Entities must develop a personnel risk assessment program for all personnel having access to Critical Cyber Assets. The risk assessment must be conducted within thirty days after the person in question receives access authorization. The program must, at a minimum, include an identity verification process, a seven-year criminal background check with updates every seven years, and documentation of findings. Finally, Responsible Entities must develop a list of authorized personnel with access to Critical Cyber Assets, including their specific access rights. This requirement mandates timely modification of access rights based on changes in authorization status and change of employment.

B. Issues Identified

CIP-004-1 makes several improvements over UA 1200. It adds a requirement for quarterly security awareness reinforcement sessions in addition to mandatory cyber security training. It also adds a requirement that the Responsible Entity develop and maintain a personnel risk assessment process in the course of granting access to Critical Cyber Assets.

Requirement R1 implements a fundamental element of any serious security effort when it requires the Responsible Entity to "establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices." However, the Reliability Standard provides little direction concerning the elements of an appropriate awareness program. While the Requirement identifies various formats for conveying information, e.g., email, computer-based training, posters and presentations, it

does not identify minimum expectations regarding the content of an awareness program. Identification of substantive categories of material to be conveyed, however, could be readily developed and could be based on available employee awareness models. For example, 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.[28]

The training requirements specified in Requirement R2 apply to all personnel authorized to have cyber access or unescorted physical access to Critical Cyber Assets. However, it 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. If the networking of Critical Cyber Assets is omitted, the network may not be covered by network infrastructure fundamental awareness training. This lack of training can lead to a lack of awareness of the importance of the network support in the security of the environment as a whole. Non-critical Cyber Assets (support infrastructure) such as bridges, switches and routers 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. 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.

Requirement R2.1 provides that a cyber security training program should ensure that all personnel having access to Cyber Security Assets are trained within 90 days of such authorization. Staff questions whether authorization should be granted for a period of up to 90 days without security training. Some lesser interval, such as 30 days, would provide sufficient time for training and lessen the period during which authorized personnel may not be aware of important cyber security policies and concerns. Ideally, personnel would receive cyber security training *prior* to allowing access to Cyber Security Assets. Also, 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.

Requirement R3 requires each Responsible Entity to have a documented personnel risk assessment program. While that is an improvement over the UA 1200 standard, which did not require such a program, staff is concerned that Requirement R3 would allow access to Critical Cyber Assets during the investigative process. Requirement R4 directs

[28] *See* National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (1998); and NIST Special Publication 800-50, Building an Information Technology Security Awareness Training Program (2003), *available* at http://csrc.nist.gov/publications/nistpubs/.

the Responsible Entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets." These lists must contain each individual's specific electronic and physical access rights, and they must also address any changes in the individual's status and revocation of access to Critical Cyber Assets. However, the lists do not serve to keep un-cleared personnel from Critical Cyber Assets prior to completion of a personnel risk assessment. Thus, a person could be given access and fail a risk assessment but have had access to critical assets for up to 30 days with no required additional oversight or limitations. 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.

Requirement R4 requires a current listing of personnel who have authorized access to Critical Cyber Assets and timely revocation of access. In staff's view, this Requirement is beneficial because restricting access to Critical Cyber Assets significantly decreases the likelihood of a major breach in security.

VII. CIP-005-1 – ELECTRONIC SECURITY PERIMETER(S)

A. Description

Proposed Reliability Standard CIP-005-1 states that the purpose of the Reliability Standard is to require identification and protection of the Electronic Security Perimeter inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. The Reliability Standard requires that the Responsible Entity establish an Electronic Security Perimeter which encompasses all the Critical Cyber Assets that were identified using the risk-based assessment methodology required by CIP-002-1. Once the Electronic Security Perimeter has been established, the Responsible Entity must develop mechanisms to control and monitor electronic access to all electronic access points to the Electronic Security Perimeter. Furthermore, the Responsible Entity must develop a cyber vulnerability assessment and test every electronic access point to the Electronic Security Perimeter at least annually.

B. Issues Identified

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. The establishment of an Electronic Security Perimeter is a necessary starting point because it serves as a first line of defense. The Electronic Security Perimeter is the outer shell. It should stop the vast majority of intrusion attempts. Going back to the defense in depth strategy, a cyber security protection program should have additional security steps within the Electronic Security Perimeter to detect and perhaps stop intrusions that have made it past the outer shell of the defense.

Requirement R1 requires the Responsible Entity to create an Electronic Security Perimeter where every Critical Cyber Asset resides. Further, it requires that a non-critical Cyber Asset within a defined Electronic Security Perimeter must be protected as well. However, a non-critical Cyber Asset outside the Electronic Security Perimeter is not required to be protected pursuant to CIP-005-1. 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. 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.

Pursuant to Requirement R2, all access points inside the Electronic Security Perimeter must be controlled. Access points to the Electronic Security Perimeter include "…any externally connected communication end point terminating at any device within the Electronic Security Perimeter." It appears that Requirement R2 has generally been formulated soundly to address the need to control access to the Electronic Security Perimeter. However, Requirements R2.4 and R2.6 are conditioned by the phrase "where technically feasible." Specifically, Requirement R2.4 specifies that, where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity must implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party where technically feasible. Likewise, Requirement R2.6 specifies that, where technically feasible, electronic access control devices should display an appropriate use banner on the user screen upon all interactive access attempts. Keeping pace with advances in cyber security is a necessary part of strategies to protect against intrusion by an adversary, as discussed above with regard to the defense in depth strategy. 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.

Requirement R3 requires the Responsible Entity to monitor and log access at access points to the Electronic Security Perimeter. Access points must be monitored and logged twenty-four hours a day, seven days a week to detect and alert the Responsible Entity of attempts or actual breaches of the Electronic Security Perimeter. It is not sufficient simply to monitor and log the access points. Logs should be reviewed frequently because automated alerts do not detect every attempt or breach. However, the only direction supplied by Requirement R3 for reviewing logs provides that "[w]here alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days."[29] Staff believes that a review every 90 calendar days is too infrequent. Under this structure, an applicable entity could retain an access log for 90 days, review it for the first time on the 90th day, and immediately discard it. It is commonplace in the IT industry

[29] CIP-005-1, Requirement R3.2. CIP-005-1 also states a data retention policy (Compliance 1.3.1) that generally requires a Responsible Entity to keep a log for a minimum of 90-days.

for logs to be reviewed every one or two days. 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[30] and if so, no entity should be exempt due to technical infeasibility.

Requirement R4 instructs the entity to perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually and develop an action plan to remediate or mitigate any vulnerability identified in the assessment. This Requirement 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. The average amount of time required for an unprotected computer that is connected to the Internet to become infected) for a Windows operating system computer is about 20 minutes.[31] Therefore, permitting a one year window without any specificity to perform the assessment if equipment has been replaced, updated, or added to the network, seems to be an inadequate security practice.

Requirement R5 specifies that the Responsible Entity must review, update, and maintain all documentation to support compliance with the Requirements of CIP-005-1. It allows a 90-day window to update the documentation to reflect the modification of the network or controls. 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. As the Electronic Security Perimeter and its access controls are the first lines of electronic defense for protecting Critical Cyber Assets, this is a matter of particular concern.

[30] Current technology that is available for monitoring access (e.g., network servers, firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, etc.) have alarm capability built in to them.

[31] For more information on this calculation, *see* http://www.isc.sans.org/survivalhistory.php.

VIII. CIP 006-1 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

A. Description

Proposed Reliability Standard CIP-006-1 addresses the physical security of the Critical Cyber Assets identified through the procedures specified in CIP-002-1. It requires a Responsible Entity to create and maintain a physical security plan that ensures that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.[32] The Physical Security Plan must be approved by senior management and must contain processes for identifying, controlling and monitoring all access points and authorization requests, as well as procedures for keeping the plan up to date.

The Reliability Standard addresses operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter at all times. These controls must include one or more of the following physical access methods: key cards, special locks, security personnel, or other means to control physical access to the Critical Cyber Assets, such as Biometric, keypad, and token devices. CIP-006-1 provides process specifications for monitoring physical access at all access points to the Physical Security Perimeter, including the use of alarm systems and/or human observation or video monitoring. All unauthorized access attempts must be reviewed immediately. In addition, logging of physical access must occur at all times, and the information logged must be sufficient to uniquely identify individuals crossing the perimeter. Access logs must be retained for 90 days, while outage records regarding access controls, logging and monitoring must be kept for at least a year. Responsible Entities must test and maintain all physical security mechanisms on a cycle no longer than three years.

B. Issues Identified

The NERC Glossary defines Cyber Security Incident to include an event that "compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset." 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. While CIP-006-1 in general

[32] As defined in the NERC Glossary, an Electronic Security Perimeter means "The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled"… and a Physical Security Perimeter is "the physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets means are housed and for which access is controlled…."

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.

Requirement R1 of CIP-006-1 lays out the elements of a physical security plan. Requirement R1.1 anticipates that there may be instances where a completely enclosed border cannot be established and, in such an instance, "the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." However, it does not provide guidance on how to address this problem, i.e., how an "alternative measure" would be identified or determined to be adequate.

Requirement R1.7 specifies that a process must be in place "for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration…." The ninety-day response time appears to be an excessively long window for adjusting the Physical Security Plan to account for any changes. Typically, changes to physical security will not be frequent, and that the details of such changes will in general be known well in advance of their implementation. Under those circumstances, it should not be burdensome to update the Physical Security Plan within a much shorter period of implementing a physical security change.

Requirement R2 requires the use of at least one of four listed physical access control methods. However, 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. Requirement R3 requires monitoring at each access point to the Physical Security Perimeter, including alarm systems and/or human monitoring. For both Requirements R2 and R3, a Responsible Entity can choose whether to implement a single or multiple access control methods and monitoring devices. Consistent with the defense in depth strategy, a layered approach will increase the complexity of an intrusion by requiring that multiple security provisions be circumvented. Such an approach would also provide redundancy in case one system requires maintenance or unexpectedly fails to function as expected.

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).

While Requirement R5 requires that logs related to reportable incidents be retained longer than the minimum 90 days specified in the Requirement in order to conform with the requirements of CIP-008-1, it does not provide guidance as to what constitutes a "reportable incident."[33] 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.[34]

Requirement R6, which requires a "maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly," is critical for the overall success of CIP-006-1. If a policy fails to secure a system's outer physical security perimeter once assets are identified, all other protections regarding electronic access control may be rendered ineffective. 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.

[33] The issue of what constitutes a "reportable incident" is discussed in further detail in the context of CIP-008-1.

[34] In addition, there exists no guidance as to whom the Responsible Entities are to report these "reportable" incidents. While CIP-008-1 specifies that cyber security incidents are to be reported to Electric Sector Information Sharing and Analysis Center (ESISAC), there exist no such directive in the CIP's standards concerning physical security incidents. *See* CIP-001-0 and CIP-008-1 (R1.3).

IX. CIP-007-1 – SYSTEMS SECURITY MANAGEMENT

A. Description

NERC states in the Purpose Statement of CIP-007-1 that the Reliability Standard requires Responsible Entities to define methods, processes and procedures for securing the systems identified as Critical Cyber Assets, as well as the non-critical Cyber Assets within an electronic security perimeter. CIP-007-1 contains nine Requirements and nine Measures, with one Measure corresponding to each Requirement.

B. Issues Identified

This system security management standard primarily addresses changes made to the operating control system. In general, any such changes prompt concern that an entity first verify that the change will not inadvertently affect the operating control system. Testing is the usual method to ensure that such adversity does not occur. However, multiple challenges are faced when testing new equipment, security patches or updates to software and hardware. For example, during the testing process, the operating control system is vulnerable for an indeterminate period of time, during which an attacker could potentially use the vulnerability that the new hardware, software, latest security patch or upgrade is supposed to mitigate or eliminate.

Another potential problem with the testing process stems from the contractual agreements entities have with vendors of products they own. Typical service contracts include that the vendor will test patches for their software or hardware before allowing the entity to install it on its operating control system. The language in the contractual agreement with a vendor typically does not allow an entity to install the patch before the vendor verifies the patch, at risk of voiding the warranty. This again gives a window of opportunity for an attacker to exploit the vulnerability that the patch is to eliminate or mitigate because of the time it takes a vendor to test the patch in its own computer laboratory and then allow the customer to install it on its system.

Another challenge associated with testing is that of mirroring the test environment to the operating control system. In order to properly test new equipment, security patches or hardware and software upgrades, the test environment must accurately approximate the operating control system. If it is not accurate, the testing will not represent the operating control system's environment and potential failures of the new product may go undetected. Some entities may face difficulties in conducting proper testing if they do not have the resources to maintain a backup system, let alone a duplicate of their operating control system.

Requirement R1 seeks to ensure that new Cyber Assets and significant changes will not adversely affect the existing cyber security controls. Its primary mechanism is to require the Responsible Entity to create, implement, and maintain cyber security test procedures, when implementing security patches, vendor releases, and upgrades that will minimize adverse effects on the operating control system or its operation. Normally, such testing occurs before deploying the changes or modifications. Testing new hardware and software in this way is a basic security step that is necessary to prevent a degradation of existing security measures. The value of this testing is dependent on the similarities of the testing environment and the operating environment. 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.

Requirement R2 requires the Responsible Entity to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled and all others are disabled. The requirement to "disable other ports and services" is one of the basic building blocks of a cyber security program, and staff commends NERC on establishing this requirement. Assuming a "deny all" stance (i.e., disabling all ports and services first) and then opening the various ports that are needed only for operations, emergency or regular operations is a generally recognized security practice.

However, Requirement R2.3 specifies that, where unused ports and services cannot be disabled due to "technical limitations," the Responsible Entity must either document (1) compensating measures to mitigate exposure or (2) an "acceptance of risk." As discussed previously,[35] the option of "acceptance of risk" raises significant concern. While used in connection with technical limitations, i.e., situations where unused ports and services cannot be disabled and risk can at best be mitigated, acceptance of risk appears to mean acceptance of vulnerabilities without further action. Staff seeks comment on whether this option is appropriate. In any event, if it is appropriate, clear guidance is needed that explains the limited circumstances in which it is appropriate. Without such direction, the "acceptance of risk" option has the potential to become an exemption from compliance that permits the acceptance of unacceptable risks.

Requirement R3 requires the Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-1 (Requirement R6), to establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter. Staff is concerned that this requirement

[35] *See* discussion herein of CIP-003-1, Requirement R3.

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.[36]

Staff notes that Requirement R3.2 provides that the Responsible Entity must document the implementation of security patches and specifies that, in any case where a patch is not installed, the Responsible Entity must document (1) the compensating measures taken to mitigate risk exposure or (2) an acceptance of the risk. 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.

Requirement R4 requires Responsible Entities to use anti-virus and other malicious software prevention tools. The use of such tools is an essential part of any cyber security program, even one for SCADA systems. However, CIP-007-1 does not provide any direction on how to implement this type of protection or where it should be deployed. In addition, an applicable entity must take care in implementing malicious code protection, as some tools may harm the operating control system, and their operation would have to be thoroughly tested before using the protection on the operating control system. Moreover, the Reliability Standard does not suggest the use of a multi-layer, defense in depth strategy through the use of various products from multiple vendors. Such an approach is known to be especially useful to create multiple network layers that must be compromised in order for an attacker to penetrate the electronic security.

Requirement R4 provides that the Responsible Entity shall use anti-virus software and malicious software prevention tools where "technically feasible." As discussed elsewhere, staff is concerned that the use of the phrase "where technically feasible" creates unnecessary discretion for exception to Requirement R4. There would be very limited, if any, legitimate opportunities to not comply with Requirement R4 based on technical infeasibility.

Requirement R4.1 provides that in cases where anti-virus software and malicious software prevention tools are not installed, the Responsible Entity shall document (1)

[36] At the same time, staff recognizes that "compensating measures" may be necessary at times because in many cases the Responsible Entity cannot patch the control system without vendor support. In some cases, the vendor may likely apply the patch in its computer laboratory to assure that the patch does not adversely affect its product. The vendor would then provide the new version of the product to the Responsible Entity.

compensating measures applied to mitigate the risk exposure or (2) an acceptance of the risk. This provision raises the same concerns in connection with the phrase "acceptance of risk" as in Requirement R3.2. 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?

Requirement R6.3 obligates the Responsible Entities to maintain logs of system events related to cyber security to support incident reporting as specified in CIP-008-1. The Requirement, 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.

Requirements R6.3 and R6.4 of CIP-007-1 direct the applicable entity to maintain logs of cyber security-related system events for ninety calendar days to allow time to identify reportable incidents and support incident response as required in CIP-008-1. CIP-008-1 Requirement R2 requires documentation related to reportable incidents be kept for three years. However, the Responsible Entity must only store and maintain logs relating to "non-reportable" incidents for 90 days. 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. Frequent review of logs will facilitate the early detection of reportable incidents and ensure that current data is available for forensics. 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.

While Requirement R6.5 requires logs of system events related to cyber security be reviewed, CIP-007-1 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. The CIP Reliability Standard could be improved by addressing these issues. We seek comment on this perspective.

Requirement R7 requires the Responsible Entity to establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets. Prior to redeployment, the data storage media must be, at a minimum, erased to prevent unauthorized data retrieval. Erasing alone, however, may be inadequate because technology exists today that allows retrieval of "erased" data from storage devices. Effective protection requires that

discarded or redeployed assets undergo high quality degaussing.[37] Staff seeks comments on this issue.

Requirement R8 requires that the entity perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. However, while this is potentially a very powerful Requirement, it provides no direction on what features, functionality, quality, adequacy, appropriateness, capabilities and vulnerabilities upon which the vulnerability assessment process should focus. A poorly chosen vulnerability assessment process could result in a false sense of security. Additionally, 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.

Requirement R9 requires the Responsible Entity to review, update, and maintain all documentation needed to support compliance with the requirements of CIP-007-1. It specifies that documentation should be updated within ninety days, which appears to be an excessively long timeframe. This is especially true when one considers that this Reliability Standard establishes the process and procedures that are a line of defense for protecting Critical Cyber Assets. Under these circumstances, up-to-date documentation is essential in case of an emergency. If an emergency situation were to come about after modifications to the systems or controls and the documentation had not been updated, the personnel in charge of responding to such an emergency would not have the proper documentation to fully implement a response to the emergency.

[37] To degauss is to demagnetize. Degaussing a magnetic storage medium removes all data stored on it.

X. CIP-008-1 – INCIDENT REPORTING AND RESPONSE PLANNING

A. Description

Proposed Reliability Standard CIP-008-1 addresses identification, classification, response to and reporting of cyber security incidents related to Critical Cyber Assets. CIP-008-1 is a companion to CIP-001-0, which addresses the reporting of physical sabotage incidents. CIP-008-1 consists of two Requirements that address: (1) Cyber Security Incident Response Plans (CSIRP); and (2) Cyber Security Incident documentation.

Requirement R1 requires Responsible Entities to develop and maintain a CSIRP. That plan must address the Responsible Entity's proposed reaction to a Cyber Security Incident. It should characterize and classify pertinent events as reportable Cyber Security Incidents, as well as state the response actions. These response actions should document: (1) the roles and responsibilities of incident response teams; (2) procedures for the handling of incidents; and (3) associated communication plans. In addition, there must be a process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ESISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ESISAC either directly or through an intermediary. Changes to the CSIRP are to be documented within ninety days. The CSIRP should be reviewed and tested at least annually. The testing process may range from an actual incident, to a paper drill, to an operational exercise.

Requirement R2 requires the Responsible Entity to retain documentation related to reportable cyber security incidents for a period of three years.

B. Issues Identified

Requirement R1 of CIP-008-1 provides direction on which issues the CSIRP needs to address. The Requirement refers to "reportable" Cyber Security Incidents in a number of places, but it does not provide definition on the characteristics of a "reportable" incident. Does it mean an incident whose reporting is required by a law enforcement agency, a regulator or a guideline? Alternatively, some other descriptive attribute may be required to distinguish a "reportable" incident. Consequently, it is possible that two different entities could experience the same cyber attack on similar assets; one would report it and the other would not, depending upon each entity's interpretation of a "reportable" incident.[38]

[38] Staff recognizes that, in its Frequently Asked Questions document, NERC replied to the question of "what is a reportable incident?" by referencing definitions in ESISAC's, IAW SOP and DOE 417 Report. Since these materials are not incorporated into the proposed Reliability Standard, CIP-008 is

In addition, while CIP-008-1 requires that the ESISAC be notified of any reportable cyber security incident, there is no defined time frame for sending the report. It is important that other Responsible Entities receive timely information regarding a reportable cyber security incident so that they may take precautions against a similar targeted incident. Depending upon the nature of the incident, timelines of incident reporting may be critical. ESISAC procedures provide that a cyber incident report should be filed within one hour of a suspected malicious incident.[39] 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.

Requirement R1.6 requires annual testing of the Cyber Security Incident Response Plan, which could range from a "paper drill" to a full operational exercise. Thus, a Responsible Entity could satisfy this Requirement without actually executing the response plan. The paper drill option, 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.

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 apply them to plan improvement. Nor does it require reassessment of a plan's adequacy in responding to specific issues or implementation of improvements based on lessons learned from paper drills, full operational exercises, or real-world incidents. Staff seeks comment about documentation and implementing "lessons learned."

---

ambiguous in this regard. North American Electric Reliability Council, Frequently Asked Questions (FAQs) Cyber Security Standards CIP-002-1 through CIP-009-1, March 6, 2006, page 27, question 1.

[39] *See* ESISAC, Indications, Analysis and Warnings Program (IAW) - Standard Operating Procedure (SOP), available on ESISAC's Electricity Sector - Investigation Sharing and Analysis Center Web Page – www.esisac.com/IAW.htm.

XI. CIP-009-1 – RECOVERY PLANS FOR CRITICAL CYBER ASSETS

A. Description Proposal

The goal of proposed Reliability Standard CIP-009-1 is to ensure that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. The Reliability Standard requires the development, updating and testing of recovery plans.

B. Issues Identified

CIP-009-1 provides general guidance on issues that recovery plans must address, the performance of required exercises, and on processes and procedures for backups (including testing) and storage of information. However, Requirement R1, which requires the Responsible Entity to create and annually review recovery plan(s) for Critical Cyber Assets does not provide or require a definition of what constitutes a precipitating event or condition that triggers the need to implement the plan. The Requirement merely describes such triggering events as "events or conditions of varying duration and severity that would activate the recovery plan(s)." 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. In addition, there is no directive regarding whether forensics collection should occur prior to, contemporaneously with, or after recovery of the Critical Cyber Assets.

Requirement R2, as in CIP-008-1(Requirement R1.6), does not require a Responsible Entity to conduct full operational exercises. 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.

Requirement R3 requires the Responsible Entity to update the recovery plan(s) to reflect any changes or lessons learned during an exercise or a recovery from an actual event, and to communicate updates to personnel responsible for activating or implementing the recovery plan within 90 days. In order to avoid prolonged exposure and vulnerability of the Critical Cyber Asset, individuals responsible for activation and implementation of process changes in the recovery plan(s) must have the most current information available. We therefore question whether a 90-day time lag is consistent with this objective.

Requirement R4 requires that a recovery plan include processes and procedures for the backup and storage of information necessary to successfully restore Critical Cyber Assets. 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.

Requirement R5 requires annual testing of information stored on backup media to ensure the availability of information essential to system restoration. Testing of media is permitted off site. The availability of information from backup media is critical to the implementation of a recovery plan in the event of a live incident and the recovery from such an incident. There are no specifications as to what actions should be taken in the event of a failure in testing. Such feedback and communication of actions taken are an important part of this process. 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.

XII. NERC SECURITY GUIDELINES

Separate from the CIP Reliability Standards, NERC has developed "Security Guidelines for the Electricity Sector" (Security Guidelines), which NERC describes as a "compendium of best practices for protecting critical facilities against a spectrum of physical and cyber threats."[40] These 19 Security Guidelines address such matters as Communications, Continuity of Business Practices, Business Network Electronic Connectivity, Cyber – Access Controls, Cyber – IT Firewalls, Cyber – Risk Management, and Employment Background Screening. The Security Guidelines describe general approaches, considerations, practices, and planning philosophies to be applied in protecting electric infrastructure systems. According to NERC, the Security Guidelines are meant to be "living" documents that will evolve just as the threats and challenges to the electric infrastructures and the tools used to meet those threats and challenges continue to evolve. The guidelines are not meant to represent any single or "cookbook" approach to electric sector infrastructure protection and are advisory in nature.[41]

Although NERC characterizes the Security Guidelines as "best practices," certain provisions of the guidelines address more basic security needs and may be more appropriate as Requirements. Throughout the preliminary assessment, staff has identified various requirements in the CIP Reliability Standards that would benefit from greater specificity. Often, this additional specificity can be found in the Security Guidelines. Thus, we believe that the Security Guidelines are not only an important complement to the CIP Reliability Standards, but, in certain instances, provide more basic direction than the standards in developing and implementing sound security practices.

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.

---

[40] *See* http://www.nerc.com/cip.html.

[41] *See* NERC Security Guidelines for the Electricity Sector, Overview, Version 1.0 (June 14, 2002).