



***Preparing for New Cyber Security Reliability Standards
in the Electric Power Industry
The Energy Policy Act of 2005***

President Bush signed the Energy Policy Act of 2005 into law on August 8, 2005. The changes to the bulk electric power industry envisioned by this law do not take place immediately, however significant changes are already occurring and many more significant changes will occur within the next year. Securicon Analysts work extensively within the Electric Power Industry and closely track the changes in the regulatory environment of its clients. This document will be updated periodically over the next 18 months to reflect the most current status of the new Cyber Security Requirements that will result from the Energy Policy Act of 2005.

Author: Mike Chaney
Mike.Chaney@Securicon.com
www.Securicon.com

SECURICON

Abstract

The Energy Policy Act of 2005 (the Act) addresses many goals to improve the strategic posture of the United States in Energy sectors such as Natural Gas and Hydropower. The focus of this paper is a review of the new regulatory compliance infrastructure being created within the Electric Power industry and, specifically, the cyber security standards being introduced and enforced to support the goals of Electric Power reliability.

Introduction

The electric power grid is a unique critical infrastructure, inherently complex, sensitive to disruption, and composed of many high-risk components (such as electricity itself). The power grid is an extremely valuable resource to every government, business, and individual citizen and represents a fundamental component of the economy and national defense. There is an expectation of constant availability of stable electrical power. Meeting this expectation requires world-class engineering, constant monitoring, and a great deal of effort. Fortunately, people intuitively understand the importance of reliable electrical power. The entities responsible for designing, operating, and managing the power grid have worked well together and have delivered a quality infrastructure without significant disruption for decades at a time. However, on August 14, 2003, the Eastern United States and Canada experienced a massive electric power blackout affecting an estimated 50 million customers that lasted up to two days in some parts of the US and even longer in some parts of Ontario.¹ The August 2003 blackout delivered a massive economic impact, but more significantly, an overall loss of confidence in the integrity and reliability of the electric power grid's infrastructure.

Recommendations derived from the investigation and analysis of the August 2003 blackout followed a primary theme: All stakeholders must move towards adherence to high reliability standards within the framework of a proper balance between regulatory and market factors. Investigators identified cyber security standards as a significant part of the new required reliability standards. The Act seeks to address these recommendations and will result in widespread changes in the regulatory environment including requirements for all players in the bulk electric power grid to adhere to new cyber security standards. Within the bulk electric power system, any entity that sells, purchases, or transmits electric power directly will be affected under the new law.

The regulation of critical infrastructure such as the electric power grid must be tailored to some degree. In the financial services or transportation industries a regulator may take action that temporarily or permanently takes a member of that industry out of operation and may even force it out of business. However, this type of action is often not realistic and even counter productive within the electric power grid. A regulator's goal would rarely include taking a portion of the infrastructure out of operation. The goal must always be to ensure the reliability of the infrastructure.

¹ *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*; U.S.-Canada Power System Outage Task Force; April 2004.

SECURICON

Enforceable Reliability Standards

The new reliability standards are intended to provide for reliable operation of the bulk electric power system, including cyber security protection. To date, the North American Energy Reliability Council (NERC) has created 91 reliability standards. The standards identify the entities responsible for performing the functions necessary to meet each requirement. So far, none of the approved standards have related to cyber security.

However, NERC is currently developing cyber security standards, known as CIP-002 to CIP-009. The new cyber security standards cover areas ranging from the security of critical cyber assets to personnel screening and training requirements. An example subsection of a draft standard would be: “The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).”²

Development of the draft cyber security standards into approved, enforceable standards that will be enforceable is moving forward more rapidly within the bulk electric power industry since the President’s signature of the Act. The new cyber security reliability standards are expected to apply to:

- Distribution providers
- Load-serving entities
- Generation owners
- Generation operators

These cyber security standards have been in development for the past two years and can be found at this link: <http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

The fourth revision of the cyber security standards was posted for a 30-day pre-ballot review on January 16, 2006. The cyber security standards are expected to be approved and enforceable by the summer of 2006.

The Act provides the flexibility to allow regional entities to propose standards in order for the development process to effectively address variations in regional implementations of the bulk electric power grid. The parties drafting the new reliability standards take these proposals into account and strive to create new reliability standards that are flexible enough to address any regional variances while adhering to a reasonable risk model. Once standards are in place, no Regional Reliability Organization (RRO) or bulk electric power system owner, operator, or user shall be allowed an exemption to an Electric Reliability Organization (ERO) reliability standard without approval of such a variance through the applicable procedure.

New Roles and Responsibilities

With the implementation of the Act, several organizations will undergo significant changes in their roles and responsibilities. The Federal Energy Regulatory Commission (FERC) regulates and oversees all U.S. energy industries. The Act provides FERC with new responsibilities in all energy industry sectors including Gas, Electric, and Hydropower. Specifically, in accordance with the new law, FERC is authorized to approve

² NERC Standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s); Paragraph R2.3; ftp://www.nerc.com/pub/sys/all_updl/standards/sar/CIP-002-009-1_30-day_Pre-ballot_Comment.pdf; January 17, 2006.

SECURICON

mandatory reliability standards for the bulk electric power system and ensure that they are properly enforced. The new law provides FERC with jurisdiction over the reliability of bulk electric power system in the U.S. For purposes of reliability only, FERC has jurisdiction over:

- Owners, operators, users of the bulk electric power system, including state and municipal entities
- Rural electric cooperatives

Under provisions of the new law, FERC is currently engaged in developing a framework of rules to implement the provisions of the Act and to meet its new responsibilities. A final rule implementing the new reliability provisions are due to be issued by February 2006.

The Act provides for FERC to certify one ERO to develop and enforce reliability standards. The newly created ERO must be independent of owners, operators, and users of the bulk electric power system. FERC will supervise within the United States; within Canada, the Provinces will supervise the efforts of the ERO. In accordance with the new law, the existing NERC will transition and become the new ERO. NERC is currently funded by 10 regional reliability councils, which adapt NERC rules to meet the needs of their regions. As a result of the Act, NERC will transition and change its name to the North American Electric Reliability *Corporation* signifying a change from a “council” of regions to an independent (government sponsored) corporation. This change will allow the new NERC/ERO to serve as an international government sponsored entity and will allow it to retain the acronym ‘NERC’ as it takes on the role of the ERO. In its new role, the ERO must equitably allocate reasonable dues, fees, and other charges among end-users for its activities.

On December 16, 2005, NERC submitted an application for certification as the Electric Reliability Organization for public review and comment.³ The transition plan for NERC to take on the role of the ERO envisions the ERO being certified by the FERC in the summer of 2006. As the ERO, NERC will continue to serve as the Electricity Sector Information Sharing and Analysis Center (ESISAC).

Once new rules and reliability standards are in place, the ERO will be able to impose a penalty (which may include limitations on activities, functions, or operations, or other appropriate sanctions) on an owner, operator, or user of the bulk electric power system if, after notice and an opportunity for a hearing, the ERO finds that the owner, operator, or user violated a reliability standard. FERC will play an oversight role and may affirm, modify, or set aside penalties.

FERC may also order compliance with a reliability standard and impose a penalty on an owner, operator, or user of the bulk electric power system if it finds that the owner, operator, or user has engaged in, or is about to engage in, activity that violates a reliability standard. FERC may also take action against the ERO or a regional entity with

³ ftp://www.nerc.com/pub/sys/all_updl/ero/application/ERO-Package-12-16-05.pdf; January 12, 2006

SECURICON

delegated enforcement authority to ensure compliance with a reliability standard or any FERC order regarding the ERO or the regional entity.

The Act allows for the ERO to make agreements with regional entities that will allow the ERO to delegate enforcement authority in a particular area to a regional entity. The ERO, through the regions, will certify entities performing certain critical reliability functions such as balancing authorities, transmission operators, and reliability coordinators. The ERO shall set the requirements for and maintain control over the registration and certification program for organizations within the power grid. The ERO will be the certifying entity for regional entities. The ERO, through the regions, will maintain a list of entities that meet the definition of bulk electric power system owner, operator, or user and are therefore responsible for complying with the reliability standards. The list will identify the functional responsibilities of each registered entity as follows:

- Reliability coordinators
- Balancing authorities
- Transmission operators
- Transmission owners
- Transmission service providers
- Planning authorities
- Transmission planners
- Resource planners
- Generator operators
- Generator owners
- Load-serving entities
- Distribution providers
- Market operators⁴

The list will be filed with regulatory authorities (FERC within the United States) and maintained current.

Readiness Audit Program

NERC established the Readiness Audit Program following the 2003 blackout to ensure that operators of the bulk electric power system can meet their reliability responsibilities and perform under emergency conditions. NERC began the Readiness Audit Program in 2004 and will complete the first three-year cycle in 2006. This program should not be confused with the Compliance Program described below. The Readiness Audit Program is intended to act as an assistance program and an opportunity for the industry to develop more realistic and effective best practices and reliability standards. The program will incorporate assessments of cyber security controls as they are finalized and approved.

In 2004 and 2005, the first two years of the program, NERC completed audits that covered 72% of the total load in North America — 77% in the Eastern Interconnection, 43% in the Western Interconnection, and 100% in the Electric Reliability Council of

⁴ Draft ERO Application, Page 9, NERC; ftp://www.nerc.com/pub/sys/all_updl/ero/application/ERO-Package-12-16-05.pdf; December 29, 2005

SECURICON

Texas. NERC plans to conduct about 75 audits of registered reliability entities and about 10 audits of local control centers in 2006.⁵

The readiness audit program evaluates the readiness of reliability coordinators, balancing authorities, and transmission operators, as well as other operational entities that may be designated by FERC, that are responsible for the reliable operation of the bulk electric power system. The audits are intended to identify areas of excellence in operations and areas in need of improvement. The readiness audit program is managed and implemented by the NERC/ERO with active involvement and support from the regions. Currently, the NERC/ERO is planning for each organization falling within the regulatory framework to undergo a Readiness Audit at least once every three years.

Compliance Enforcement Program (CEP)

NERC began collecting and reporting specific violations of standards in 2004. Because of their sensitive nature, NERC does not release the names of entities with confirmed violations that involve critical infrastructure issues. The NERC Enforcement Program currently provides for only simulated sanctions. However, NERC and the regions track the mitigation plans for these entities. With the certification of the NERC as the ERO in accordance with the provisions of the Act (expected to occur in the summer of 2006), NERC/ERO Reliability Standards shall be in force and enforceable. From that point forward, entities subject to the reliability standards enforced under the Act may face actual sanctions.

Many of the current processes used by NERC and the regions rely on participation by industry members and experts who exert peer pressure. The previous emphasis on independence and the current goal of consistency of the ERO CEP means that some regional processes will need to be changed to meet these goals. NERC and the regions will be updating procedures in the second quarter of 2006. At that point, FERC rules will be in force and NERC will be finalizing efforts to achieve certification as the ERO. These changes should be finalized by the end of 2006.

Within the Compliance Program, reporting must be verified through audits, investigations of system events, reports of non-compliance and spot checks of self-reporting. Evidence of possible noncompliance with an ERO standard shall be reported to the ERO for resolution through the compliance enforcement program. If the issue is judged to be an immediate threat to reliability, the notification to the ERO shall be made within 24 hours of discovery. Enforcement action will involve monetary penalties, with possible escalation of penalties based upon increasing risk to reliability, the degree at which the standard is violated, and continuing poor compliance performance.

Investigations will be conducted to evaluate compliance with reliability standards when certain system events occur, or when other owners, operators, or users of the bulk electric power system file valid complaints. Investigations can be initiated at the discretion of the regional compliance staff, the senior regional officer, ERO compliance staff, or the ERO president.

⁵ <http://www.nerc.com/~filez/nercnews/news-0106c.html> ; January 12, 2006.

SECURICON

Risks of Non-Compliance

The NERC CEP currently uses a multi-faceted approach to penalize non-compliance, which addresses severity of non-compliance and failure to address identified violations. Penalties range from Letters of Non-Compliance, for less severe non-compliance, to simulated monetary fines that can total as much as \$10,000 or \$10 per Megawatt (whichever is higher) in case of continuous, significant non-compliance. However, once FERC issues a final rule implementing the new reliability provisions, the severity and applicability of these penalties may change. In addition, the degree of public disclosure for cases of non-compliance may also be affected.

Reliability Assessment of the Interconnect

In accordance with the Act, the ERO shall conduct and report the results of an independent assessment of the overall reliability, adequacy, and associated risks of the interconnected North American bulk electric power systems, both as existing and as planned. Regional entities and applicable bulk electric power system owners, operators, and users will be required to provide ERO-requested data necessary to complete the reliability assessments. This assessment may provide findings that lead to additional future reliability standards including cyber security standards.

Upcoming Developments

As the NERC transitions to the ERO over the next year, it will engage in many transition-related activities such as drafting new budgets, hiring of staff, developing tools to track compliance with reliability standards, and completion of agreements with Regional Reliability Organizations. The regional delegation agreements will likely be signed after FERC certifies NERC as the ERO, forecast for June 2006. While the FERC is scheduled to have rules in place by February 2006, the ERO is not required to be certified until August of 2006. The transition plan provides for the new ERO program being implemented including enforcement activity effective January 1, 2007.

SECURICON

Recommended Actions

2006 will be a watershed year for members of the electric industry. Many industry members have already begun to make significant changes to their infrastructure and operations in order to meet the new requirements of existing and soon-to-be-approved cyber security reliability standards. Cyber security standards have never before been mandatory for members of the industry. Therefore, affected organizations are encouraged to take the following actions:

- Monitor developments in FERC's rulemaking process and NERC's new standards.
- Create a list of physical and cyber assets that will be subject to audit.
- Initiate steps towards compliance by conducting a comparative gap analysis of the latest version of NERC cyber security standards with the current state of the organization's critical cyber assets (seek guidance from 3rd party service providers with expertise in this area).
- Craft budgets that address the new requirements.
- Maintain situational awareness of any changes to your organizations categorization within the NERC CEP. NERC may make additional entities register as responsible entities within the CEP and comply with additional reliability standards.
- Monitor NERC's quarterly *Examples of Excellence Bulletin*, which highlights industry practices for the reliability of the interconnected bulk electric power system.
- Provide qualified volunteers to participate in NERC/ERO readiness audits. The audits provide volunteers the opportunity to witness examples of excellence and learn lessons to improve reliable operations within their own organizations. Information about the Readiness Audit Program is available at <http://www.nerc.com/~rap/>