

IT Compliance Magazine  
Spring 07

“Cyber Security under the NERC Reliability Standards”

By

James R. Stanton

Director of NERC Reliability Standards Services for  
ICF International

Historic concerns about corruptions to IT systems have in the past included financial record disruption, compromising sensitive data, and business process disruption. With the increasingly IT intensive nature of the monitoring and control of the nation’s interconnected electrical grids, corruption concerns are now focused on potential devastating outages of electric service to large geographic areas and the accompanying risk to national security.

The Energy Policy Act of 2005 contains provisions to empower the Federal Energy Regulatory Commission (FERC) to enforce mandatory Reliability Standards on the users of the bulk electric system. This empowerment grew largely from concerns over the previous reliability provisions developed by the North American Electric Reliability Council (NERC) which were fairly comprehensive, but were also voluntary. The Northeast Blackout of 2003 drew attention to violations of the voluntary standards, hence the need for broad and significant enforcement.

One set of Standards within the initial set developed by NERC are the Critical Infrastructure Protection (CIP) group. These Standards cover issues from sabotage reporting and identification of critical assets, to securing critical cyber assets against intrusion and physically securing access to such systems.

Too often, ideas about the nature of cyber intrusion incidents lean towards images of disabled file servers, frantic damage control exercises by security personnel, or the loss of critical data. While intrusions can be all these things we must add to our list of consequences the scenes of hundreds of thousands of people stranded within cities, businesses shut down, phone systems down or taxed beyond their limits, and the eerie sight of miles of dark streets stretching between blocks of silent, uninhabitable buildings. This scenario is not hard to imagine as we only have to think back to August 14, 2003.

That outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario. Estimates of the total costs in the United States range between \$4 billion and \$10 billion (U.S. dollars). In Canada, gross domestic product was down 0.7% in August, there was a net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down \$2.3 billion (Canadian dollars).

While the causes of the 2003 blackout were not the result of a cyber attack, similar damages and cascading events could result from coordinated intrusions of the infrastructure that monitors and controls the interconnected electric transmission grids. Obviously, these types of events not only result in high costs and endangerment to the public, but also represent significant breaches in national security.

The timing for implementation of the NERC Cyber Security Standards is still being finalized, but given the significant risks to the electric systems from cyber intrusions, we can safely expect the Standards to be approved for enforcement in late summer or early fall of 2007.

On December 11, 2006, in Docket No. RM06-22-000, FERC Staff issued a Preliminary Assessment of the Critical Infrastructure Protection Standards submitted by NERC. In this assessment, FERC Staff noted, “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.”<sup>1</sup>

Speaking to the highly integrated and interconnected nature of the systems they also said, “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

---

<sup>1</sup> FERC Staff Preliminary Assessment of NERC Reliability Standards pg. 1 Exec. Summary

impact the Bulk-Power System rather than to simply disrupt the operation of some components.”<sup>2</sup>

The key to the Critical Infrastructure Protection Standards lies in CIP-002 which mandates risk based assessments of both physical and cyber assets to determine their criticality to system reliability. While at this writing, NERC has declined to comment on the exact nature of such assessments, FERC staff notes that additional detail around the nature of the assessments is needed. “...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.”<sup>3</sup>

Many Responsible Entities, like unaffiliated Generator Owners and Operators, are looking to their Regional Transmission Organizations or Transmission Providers for assistance in accomplishing the Risk Based Assessment. The NERC *Security Guidelines for The Electricity Sector: Vulnerability and Risk Assessment* document provides the following guidance, “A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.”<sup>4</sup> This type of identification implies a contingency analysis type approach. Unaffiliated Generators do not have access to the transmission data which would allow them to run criticality studies for different scenarios

---

<sup>2</sup> FERC Staff Preliminary Assessment of NERC Reliability Standards pg. 6 Introduction

<sup>3</sup> FERC Staff Preliminary Assessment of NERC Reliability Standards pg. 16

<sup>4</sup> Security Guidelines for The Electricity Sector: Vulnerability and Risk Assessment, pg. 1 Applicability

for their plants. In the event the Generators wish to have a measure of control over the input and methodologies involved in the analysis, some are looking to outside vendors for the studies rather than leaving the fate of their designation up to others.

Commercial issues come into play in the Cyber Security arena in that the proposed Standards contain references to “business judgment” by which Responsible Entities can customize their approach to critical asset protection strategy based on their own business model and equipment. FERC Staff has expressed concern about the nature of business judgment in this forum, “...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.”<sup>5</sup>

Also, in the case of an electric generator meeting the criteria for a critical facility as noted in the Security Guidelines, such identification begs the questions of whether such a designated facility would automatically qualify for a Reliability Must Run (RMR) contract. It would seem at least odd and at worst disingenuous and discriminatory to have one without the other. Herein lies the commercial concern of costs imposed on one Responsible Entity by another. The scope and potential increased costs for entities having such designated equipment, outlined in the CIP-003 through 009 Standards is significant to say the least.

The electric industry, while accomplished at many phases of IT security, will be looking to the IT industry for assistance in securing their systems and complying with the rigorous Standards in place and being developed in the NERC processes. That NERC

---

<sup>5</sup> FERC Staff Preliminary Assessment of NERC Reliability Standards pg. 9

process is an ANSI (American National Standards Institute) certified endeavor that allows and encourages participation by all concerned entities and individuals. Any concerned entity or individual can submit a Standards Authorization Request for a new Standard or to revise an existing one. Also, they can track the development of the Standards on the NERC website ([www.nerc.com](http://www.nerc.com)), nominate themselves or others to serve on Standards drafting teams, and even become a member of NERC at no cost and participate in the ballots for the Standards and revisions that are the heart of the process.

The specter of another large blackout looms constantly over the nation's electrical systems, and the new Cyber Security Standards seek to ensure that if such an occurrence is repeated, it will not be the result of a deliberate, adversarial strike initiated through the highly integrated utility IT systems.

