

## Walking the Line: Getting Ready for NERC Cyber Security Mandates

Kevin T. McDonald, CISSP, CISA, PMP  
ICF International

Following the August 14, 2003 Blackout, the US – Canada Power System Task Force published a report identifying several issues that contributed to its scope and severity<sup>1</sup>. The estimated economic impact was estimated at over \$10 Billion.<sup>2</sup>

### The Aurora Effect:

In early 2007, the DOE Idaho National Lab conducted a demonstration known as the Aurora experiment using cyber attack to destroy a generator. The results of the test were summarized in a 30 second video clip that was widely broadcast on television and the internet. The success of the simulated cyber attack raised the possibility that a real world event could have catastrophic and long lasting effects on the Bulk Power System. This awareness and some of the weaknesses identified within the current proposed standards has turned up the heat on FERC, NERC and the industry to quickly close the gap on Cyber Security.<sup>5</sup>

In the security literature, a cyber attack that is unique when it first appears is termed a zero day attack. It is assumed since it has not occurred before; the effects of the attack will be amplified due to the lack of defense. Aurora represents the real risk that a zero day attack on the electric power grid could cause permanent equipment damage on systems with long lead times for replacement. This is a worst-case scenario, but a successful, widespread Aurora type attack is a serious threat to the grid if enough systems could be tripped offline at once.

The question now is what is the current level of risk? The chances might actually be quite low that an individual system will be successfully attacked in a similar manner. However, as news of the vulnerability spreads, the risk of attack goes up. The fallout from a successful attack will be amplified due to the public knowledge of the vulnerability. This raises the specter that an attack could produce a repeat performance of the 2003 blackout, only this time it could last not just days but weeks or months.

### From Self-Policing to Enforcement:

Prior to the Energy Act of 2005, the industry was self-regulated. Reliability standards were voluntary. Even though several violations of the NERC reliability standards were noted in the 2003 Final Report on the Blackout, there were no fines or sanctions applied because no one had an enforcement capability. The 2005 Act empowered the Federal Energy Regulatory Commission (FERC) to enforce fines up to \$1,000,000 per day per incident and enact sanctions such as banning an organization from market participation.

FERC is required to work with an industry Electric Reliability Organization (ERO) that will develop Reliability Standards for subsequent FERC approval. FERC appointed the North American Electricity Reliability Corp. (NERC) as the ERO for North America in July of 2006. NERC came into being in the sixties as the North American Reliability Council following a similar blackout. Its mission is to maintain and improve the reliability of the Bulk Electric Power Supply in America and Canada.

Since its inception, FERC, NERC and industry representatives have been hammering away at reliability issues. NERC stakeholder committees formulate and vote on standards. NERC's board of trustees review approved standards for submission to FERC.

NERC formulated Cyber Security standards dubbed Critical Infrastructure Protection or CIP standards. The standards were numbered CIP001 through CIP009. CIP001, Sabotage Reporting, was approved by FERC on March 15, 2007. The remaining standards, CIP-002 through CIP-009 were submitted to FERC in June of 2007. FERC has taken these under review and issued a Notice of Proposed Rulemaking (NPR) to solicit comments on the proposed standards. FERC is expected to issue a final rulemaking opinion within a short time.

### Setting the Pace:

Stakeholder Committees drive the standard formulation process. They meet informally every month or so

to consider further drafts of standards. Once a quarter, the committees in the whole meet face to face to vote on finalizing drafts. Since volunteers working part-time run this process, the pace is slower compared to full time entities.

This was touched on by the testimony to the House Committee on Homeland Security by Joseph McClelland, the Director of the Office of Electric Reliability. In his remarks, he provides an excellent overview of the standards making process, the history of NERC and the restrictions presented by Section 215. He acknowledged that FERC and NERC were proceeding according to the guidelines provided under law in the Energy Act of 2005. The downside is that if an urgent vulnerability is discovered, similar to the Aurora experiment, FERC may not have enough regulatory powers to get it corrected quickly. He also indicated if circumstances required it, FERC might pursue help from congress to create fast track rules.<sup>4</sup>

### Comments and Questions:

During the last six months, FERC has gotten several comments regarding the scope of the assets that should be included under the CIP guidelines. To start with, CIP002 requires suppliers to identify the assets and electronic devices 'critical to the bulk power supply' via a self-assessment. From an economic standpoint, this sets up a potential conflict of interest since an asset or device identified as 'Critical' under the standard is then subject to protection that is more rigorous and costly than non-critical assets. Instead of identifying assets based on the number of customers or critical functions served, the assessment only asks if it is critical to the overall bulk power supply. Due to the levels of redundancy within the BPS, it has been argued that no single generation facility is actually critical under this definition.

The compliance function of NERC rests with self-reporting and audits. The eight regional entities throughout the US perform the audit function through spot checks, self-assessment questionnaires and scheduled compliance audits. Since the compliance audits have to be performed by the regional entities, they will likely suffer along with industry if the standards are not clear. Without some metric to guide them, the organizations involved face significant uncertainty. On one hand, the power companies could gamble that they are not in the scope of the standards. On the other, the regional entities could argue they are in the scope. The net result could be confusion, litigation and even more cost to industry and consumers.

### Metrics to the Rescue:

Other models for compliance such as Sarbanes-Oxley stipulated clear metrics such as this applies to public companies with an annual revenue of at least \$75 million. One recent post from the nuclear industry asked that any infrastructure required for black start or orderly shutdown power at nuclear power plant be considered critical. This may seem like taxation without representation to the neighboring power generators. This illustrates how difficult it is to draw a line around a set of interconnected assets like the bulk power system and say this is critical and this is not.

In the Department of Energy's OE-417 reporting requirements, if 500 MW of generation is lost, 200 MW of load is lost, high voltage lines or high voltage substation or any system that could affect

**Now Available Electronically!**

**SUBSCRIBE TODAY TO GET THE LATEST NEWS ABOUT**

**REMOTE**  
Site & Equipment Management



**New Products, Companies, The Industry, Research & Development and Events.**

For a new subscription, or to renew your current subscription go to:

[www.RemoteMagazine.com/r-sub.php](http://www.RemoteMagazine.com/r-sub.php)

and select Print or Electronic Edition

a market fails, the bulk power supplier must quickly report it. Under the CIP002 requirements, these same assets could be designated as non-critical because the organizations have considerable leeway in defining 'critical assets'. Because of these and other inconsistencies, it appears that CIP002 will need further review.

### Into the NIST:

FERC has also received suggestions calling for replacement of the CIP003 through CIP009 standards with the guidelines published under NIST document 800-53, Guidelines for Securing Federal Systems<sup>6</sup> and NIST 800-82 Guidelines for Securing Industrial Control Systems<sup>7</sup>. NIST is a government institute created in 2002 specifically to formulate security standards for federal systems. They have substantial experience drafting security standards. They have a full time staff that eats, drinks and sleeps cyber security. Their analysis of the CIP standards versus NIST 800-53 and NIST 800-82 states that NIST could replace CIP003 through CIP009, but they doubt that the CIP standards are detailed enough to replace all of NIST 800-53 and NIST 800-82.

For example, NIST 800-82 calls for a separation and limited connectivity between control networks and corporate networks. It recommends limited connections with stringent controls. CIP003 to CIP009 does not cover this level of detail. It is possible that the CIP002 standard will even exempt the connection between the control network and corporate network from inspection if it is deemed a communications or data network device. "Exemptions from CIP-002; 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters."<sup>9</sup>

Simply replacing the CIP standards with NIST is not an overnight process. To quote Sir Winston Churchill, "democracy is the worst form of government, except all the others that have been tried." Simply mandating replacing the CIP standards would negate the gains posted by the collaborative efforts of FERC, NERC and the industry thus far. In addition, since the net result of any changes in the standards can translate into huge expenditures, it ignores the risk assessment and cost benefit analysis typically used in security decisions in all other industries.

The House Committee on Homeland Security and the Subcommittees on Emerging Threats echoed this. They summarized the CIP002 critique and referenced the NIST versus CIP debate. They did not call for a mandated replacement but did encourage FERC to look towards the NIST guidelines for best practices.<sup>10</sup> In the Beltway, funding trumps all. As a result, these comments may weigh heavily on FERC's deliberations.

### Guidelines for the Future:

One of the main advantages to implementing the NIST security guidelines is the level of detail provided for the various components of the bulk power system. These guidelines are in fact required for Federal power agencies such as TVA and WPA. It seems a natural extension to require one set of standards for all Bulk Power Suppliers.

Adopting a referential approach to the NIST standards might accomplish three objectives. First, by establishing a referential standard, it would free up NERC and the standing committees to focus on other pressing infrastructure issues such as resource adequacy, real-time grid reporting and demand reduction initiatives. Second, it would provide clear guidance to the regional compliance groups and the power suppliers with detailed guidelines for ensuring their electronic assets are secure. Third, it would allow federal suppliers like TVA and WPA to simplify their compliance requirements.

### Dramatic Improvement:

The impact of the industry concentration on these issues is that the security and reliability posture has dramatically improved. Much of the industry is already implementing the spirit of CIP002 through CIP009. They have identified hundreds of critical assets and cyber assets and vastly increased security and training. This has been a revolutionary result even though the standards remain voluntary at this time.

The debate over adopting more rigorous standards such as NIST is a natural extension of this revolution. The emerging threat environment is what has changed and increasingly sophisticated security is required to counter them. Popular culture such as "24" and the "Diehard" movies trumpet the potential havoc created if we lose the electric power grid. There are definitely entities, both here and abroad, that would seek to exploit these vulnerabilities for any number of reasons, political, cyber-extortion or simply as a target of opportunity.

Against the rising tide of potential threats, knowledge, technology and expertise continue to improve. The electric suppliers, vendors and consultants have made great strides in improving security and reliability working hand in hand with FERC and NERC. This process is still relatively young as the energy act was just passed in 2005. The reliability standards were enacted less than a year later. These address many of the core issues identified in the Blackout report.

The main criticism of the CIP standards are they do not go far enough. However, they have functioned as a guide towards a safer Grid. It is not only regulation that drives innovation and many installations no doubt far exceed the CIP standards. The main difficulty for the electric industry today lies in the interpretation and documentation of their compliance. Since the final rule-making has not been issued, the uncertainty is also slowing implementations; it is always more difficult to walk the line in the dark.

*Kevin T. McDonald, CISSP, CISA, PMP is the Senior NERC Cyber Security Analyst for ICF International, a multi-national consulting firm based in Fairfax, VA. He can be reached at kmcdonald@icfi.com, (479) 422-0146 or www.icfi.com.*

### References:

1. US-Canada Power System Outage Task Force Final Report on the August 14th Blackout in the United States and Canada <https://reports.energy.gov/BlackoutFinal-Web.pdf>
2. The Electricity Consumers Resource Council, "The Economic Impacts of the August 2003 Blackout," February 9, 2004. Cited in Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 5, 2004
3. NERC Reliability Standards - [http://www.nerc.com/~filez/standards/Reliability\\_Standards.html](http://www.nerc.com/~filez/standards/Reliability_Standards.html)
4. Testimony of Director Joseph McClelland, Office of Electric Reliability; The Cyber Threat to Control Systems: Stronger Regulations Are Necessary to Secure the Electric Grid <http://homeland.house.gov/SiteDocuments/20071017164739-39771.pdf>
5. Aurora Test video [www.cnn.com/2007/US/09/26/power.at.risk/index.html](http://www.cnn.com/2007/US/09/26/power.at.risk/index.html)
6. Guide to Industrial Control Systems Security, K. Stouffer, J. Falco, K. Scarfone NIST 800-82, 2007 <http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf>
7. Recommended Security Controls for Federal Systems Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, Annabelle Lee <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>
8. Rulemaking Comment by NIST under RM06-22. <http://elibrary.ferc.gov/idmws/nvcommon/NVViewer.asp?Doc=11249992:0>
9. NERC CIP002 Cyber Security - Critical Cyber Asset Identification, page 2 [ftp://www.nerc.com/pub/sys/all\\_updl/standards/rs/CIP-002-1.pdf](ftp://www.nerc.com/pub/sys/all_updl/standards/rs/CIP-002-1.pdf)
10. Rulemaking Comment of Members of House of Representatives, Committee on Homeland Security (Thompson, King, Langevin, McCaul, Jackson-Lee, and Lungren) under RM06-22. <http://elibrary.ferc.gov/idmws/nvcommon/NVViewer.asp?Doc=11471251:0>
11. CIP-001 to CIP-009 implementation timeline [http://www.nerc.com/~filez/standards/Reliability\\_Standards.html](http://www.nerc.com/~filez/standards/Reliability_Standards.html)

# Remote 2008

## CONFERENCE AND EXPO

SCADA, Device Networking, M2M, Wireless Technology, Onsite Power, And Security for Remote Sites and Equipment

No other industry conference brings together technology users that manage remote sites like the Remote 2008 Conference and Expo. Over 50 conference sessions will provide cutting-edge technology direction and application strategies from the companies and users driving the growth in SCADA, M2M, device networking, data communications, system & site security, emerging wireless technology, remote monitoring and automated control, and onsite powering of distributed equipment, networks and facilities.

[www.RemoteExpo.com](http://www.RemoteExpo.com)

NOVEMBER 5-6, 2008 - ATLANTA, GA.