# TESTIMONY OF RICHARD P. SERGEL
**President and CEO**
**NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION**

**before the**
**Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology**
**Committee on Homeland Security**
**U.S. House of Representatives**
**on**
**"Implications of Cyber Vulnerabilities on the Resiliency and Security of the Electric Grid"**
**May 21, 2008**

Mr. Chairman and Members of the Subcommittee, the North American Electric Reliability Corporation[1] ("NERC") is pleased to provide this testimony on the progress being made to increase the cybersecurity of the electric grid and to mitigate identified vulnerabilities.

## EXECUTIVE SUMMARY

Cyber security of control systems is an increasing priority for every sector of the U.S. economy. On behalf of the electric power sector, NERC has recognized and responded to this challenge, first through a voluntary cybersecurity standard and now through mandatory Critical Infrastructure Protection ("CIP") Reliability Standards for the bulk power grid. CIP Reliability Standards CIP-002-1 through CIP-009-1 were approved by the Federal Energy Regulatory Commission ("FERC") in January 2008 and become mandatory and enforceable in July. The CIP Reliability standards are intended to assure that the electricity industry will devote the necessary resources to securing control systems and identifying, responding to and reporting security incidents related to critical cyber assets.

The CIP Reliability Standards represent a significant improvement in cyber security for the electricity industry. The new standards will increase the resiliency of control systems and improve the ability of these critical assets to withstand cyber-based attacks. Cyber security requirements will be applied to companies and assets where they have never before been applied, including substations and generating plants. The bulk power system will be more reliable with the CIP Reliability Standards in place.

In approving the CIP Reliability Standards, FERC directed NERC to make certain modifications to the standards, and also to monitor the development and implementation of Recommended Security Controls for Federal Information Systems under development by the National Institute of Standards and Technology ("NIST"). The Commission-required modifications to the CIP Reliability Standards are being addressed through NERC's American National Standards Institute ("ANSI") accredited Reliability Standards development process. That process also provides the mechanism for NERC to monitor developments in the NIST process, and to determine whether any provisions of the NIST standards would better protect bulk power system reliability than the CIP Reliability Standards.

The CIP Reliability Standards will be reviewed, modified and improved on an ongoing basis through the NERC Reliability Standards development process. This will result in ever-increasing cyber security for the bulk power system.

---

[1] NERC is the corporate successor to the North American Electric Reliability Council, also called "NERC," formed to serve as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act ("FPA"), as added by Title XII, Subtitle A of the Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594, 941 (2005).

The CIP Reliability Standards, however, cannot eliminate the threat of a cyber disruption of critical national infrastructure. Because NERC has jurisdiction only to propose reliability standards for the bulk power system, the CIP Reliability Standards cannot address other critical assets – such as telecommunications systems, for example, or electricity distribution systems. Moreover, the open process by which Reliability Standards are developed, while demonstrably successful in producing standards that have significantly enhanced the reliability of the grid, may not be ideally suited to situations where, because of the sensitive subject matter, confidentiality is required.

NERC reviews cybersecurity threats on an ongoing basis. Since 2003, NERC, acting through its Critical Infrastructure Protection Committee ("CIPC"), has compiled an annual list of the highest priority cyber vulnerabilities and their associated mitigation measures.[2] Additionally, NERC serves as the Electricity Sector Information Sharing and Analysis Center ("ES-ISAC"),[3] which is responsible for promptly analyzing and disseminating threat indications, analyses and warnings to assist the electricity industry.

As the Subcommittee is aware, the ES-ISAC issued an Advisory on June 21, 2007, in relation to the vulnerability identified in the Aurora demonstration test. Since that Advisory was issued, important improvements have been made in the notification process. First, NERC now has in place a formal mechanism for issuing alerts to the industry about important matters that come either from NERC's own event analysis efforts or, as was the case with the Aurora demonstration test, from government agencies with specific information about possible threats. Second, NERC has now developed a contact list for every owner, operator and user of the bulk power system. This comprehensive list will assure that future Advisories are directed to those officials responsible for cybersecurity.

## I. BACKGROUND

NERC's mission is to ensure that the bulk power system in North America is reliable. To achieve this objective, NERC develops and enforces reliability standards; monitors the bulk power system; assesses and reports on the adequacy of electricity supplies and transmission; evaluates owners, operators, and users for reliability preparedness; and educates, trains and certifies industry personnel. NERC is a self-regulatory organization that draws upon the collective expertise of the electricity industry. FERC certified NERC as the Electric Reliability Organization ("ERO") in its order issued July 20, 2006.[4]

---

[2] The most recent list is available on the NERC website at: ftp://ftp.nerc.com/pub/sys/all_updl/cip/2007_Top_10_Final_Approved_by_CIPC.pdf.

[3] The ES-ISAC has been operated by NERC since it was formed in 2001. The ES-ISAC was created as a result of action by the U.S. Department of Energy in response to Presidential Decision Directive 63 issued in 1998. The ES-ISAC works with the electricity industry to identify and mitigate cyber vulnerabilities by providing information, recommending mitigation measures, and following up to monitor implementation of recommended measures.

[4] *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006).

Because Reliability Standards are applicable to the entire, interconnected North American bulk power system, NERC is subject to oversight by governmental authorities in both Canada and the United States. In the U.S., with oversight from FERC, since June 18, 2007, NERC has had legal authority to enforce reliability standards applicable to all owners, operators, and users of the bulk power system.

## II. CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

On January 18, 2008, FERC issued Order No. 706, approving eight mandatory Reliability Standards for Critical Infrastructure Protection.[5] NERC views the Commission's approval of the CIP Reliability Standards as another major step forward in ensuring the reliability of the electric grid.

The standards set forth specific requirements that are binding on users, owners and operators of the bulk power system to safeguard critical cyber assets (programmable electronic devices and communication networks including hardware, software, and data). They require identification and documentation of cyber risks and vulnerabilities, establishment of controls to secure critical cyber assets from physical and cyber sabotage, reporting of security incidents, and establishment of plans for recovery in the event of an emergency. The eight approved CIP Reliability Standards are:

- **CIP-002-1 – Cyber Security – Critical Cyber Asset Identification**:
  Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

- **CIP-003-1 – Cyber Security – Security Management Controls**:
  Requires a responsible entity to develop and implement security management controls to protect identified critical cyber assets.

- **CIP-004-1 – Cyber Security – Personnel and Training**:
  Requires verification of identity for personnel with access to critical cyber assets, a criminal background check, and training.

- **CIP-005-1 – Cyber Security – Electronic Security Perimeters**:
  Requires the identification and protection of an electronic security perimeter (which encompass the identified critical cyber assets) and access points.

- **CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets**:
  Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

---

[5] *Mandatory Reliability Standards for Critical Infrastructure Protection,* Order No. 706, 122 FERC ¶ 61,040 (2008), *reh'g denied,* Order No. 706-A, 123 FERC ¶ 61,174 (2008).

- **CIP-007-1 – Cyber Security – Systems Security Management**: Requires a responsible entity 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-008-1 – Cyber Security – Incident Reporting and Response Planning**: Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

- **CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets**: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

The critical infrastructure protection standards approved through Order No. 706 are a sound starting point for the electric industry to address cybersecurity. Order No. 706 is not the end of the process, however. Standards development requires progressive and continuous improvement. Indeed, improvement of the CIP Reliability Standards already is underway, both in response to directions given by FERC in Order No. 706 and as part of NERC's Reliability Standards development process, which requires that each Reliability Standard be reviewed at least every five years.

### A. Implementation of the Approved CIP Reliability Standards

Order No. 706 approved the implementation plan for the CIP Reliability Standards submitted by NERC, which phases in full compliance with all of the requirements over a three-year period (July 2008-December 2010). NERC proposed and FERC approved timelines for achieving compliance that afford a reasonable period of time for grid users, owners and operators to acquire and install the necessary software and equipment and develop new programs and procedures to achieve compliance. Enforcement begins in July for the most urgent requirements, with the implementation of additional requirements continuing through 2010.

NERC has allocated and will continue to devote the resources necessary to administer and enforce the CIP Reliability Standards. NERC's 2008 Business Plan and Budget, as approved by FERC,[6] allocates nearly $8 million (approximately 30% of NERC's overall budget) for compliance enforcement and organization registration and certification activities. To enable NERC to carry out its responsibilities for developing and administering Reliability Standards, NERC's total number of full time equivalent employees will increase by approximately 20% above 2007 levels in 2008.

---

[6] *North American Electric Reliability Corp.*, 121 FERC ¶ 61,057 (2007). The major program elements of NERC's business plan and budget are: 1) Reliability Standards; 2) compliance enforcement and organization registration and certification; 3) reliability readiness audits and improvement; 4) training, education and operator certification; (5) reliability assessment and performance analysis; (6) situational awareness and infrastructure security; and (7) administrative services. P 12. In approving the NERC 2008 Budget and Business Plan, the Commission considered the adequacy of staffing and funding proposed by NERC in finding that the Budget is reasonable. P 22. NERC's funding comes primarily from end users based on net energy for load.

Additionally, FERC has approved the 2008 budgets for the regional Reliability Entities, which share enforcement authority with NERC pursuant to delegation agreements approved by FERC. The Regional Entities are in the process of holding regional seminars on the CIP Reliability Standards.

The Commission in Order No. 706 directed NERC to develop modifications to the CIP Reliability Standards to address specific matters through the Reliability Standards development process. The Commission provided expressly that the development of modifications was not to affect the implementation of the CIP Reliability Standards as approved.[7] NERC originally planned to review the CIP Reliability Standards in 2009, but has advanced this review to address the changes directed by FERC in Order No. 706.

### B. Modifications to Approved CIP Reliability Standards and Additional Directives to NERC

The Commission in Order No. 706 directed NERC to modify the CIP Reliability Standards to remove "reasonable business judgment"[8] and "acceptance of risk"[9] language. The Commission also directed NERC to better define the circumstances under which exceptions to the standards based on technical infeasibility would be allowed.[10] Additional changes pertaining to each of the eight CIP Reliability Standards were ordered by the Commission.

Of particular interest to the Subcommittee, the Commission did not direct NERC to incorporate provisions of NIST Special Publication (SP) 800-53 into the CIP Reliability Standards. Order No. 706, P 232. The Commission did direct NERC to "monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards." Order No. 706, P 233. Any provisions of the NIST standards that are determined to better protect bulk power system reliability are to be addressed in the NERC Reliability Standards development process. *Id.*

FERC further directed NERC to consult with Federal entities required to comply with both the NIST standards and the CIP Reliability Standards on implementation and effectiveness issues. *Id.* This consultation is underway. NERC personnel spoke at the recent Federal Power Marketing Agencies Cyber Security Conference and are working

---

[7] As the Commission explained in Order No. 706 at P 30: "Consistent with section 215 of the FPA, our regulations, and Order No. 693, any modification to a Reliability Standard, including a modification that addresses a Commission directive, must be developed and fully vetted through NERC's Reliability Standard development process. Until the Commission approves NERC's proposed modification to a Reliability Standard, the preexisting Reliability Standard will remain in effect."

[8] Order No. 706 at P 128. "Reasonable business judgment" would have been used as a guide in determining what constituted compliance with the CIP Reliability Standards.

[9] Order No. 706 at P 150. The acceptance of risk language would have permitted entities subject to the CIP Reliability Standards to accept the risk of non-compliance.

[10] Order No. 706 at P 178.

on this issue with representatives from the Bonneville Power Administration and the Tennessee Valley Authority.

Another issue raised in the Subcommittee's comments on the NOPR concerned interdependencies with other critical infrastructure. The Commission addressed this issue in Order No. 706, concluding that Section 215 of the Federal Power Act, which authorizes the establishment of mandatory Reliability Standards, does not extend beyond assets critical to the bulk power system:

> Section 215 of the FPA authorizes the Commission to approve Reliability Standards that "provide for the reliable operation of the bulk-power system," which the statute defines as the facilities and control systems necessary for operation of an interconnected electric energy transmission network and the electric energy needed to maintain transmission system reliability. In addition, section 215(a)(1) specifically excludes from the definition of Bulk-Power System "facilities used in the local distribution of electric energy." Moreover, given the complexities surrounding this issue and the aggressive timeline that will be necessary merely to meet the more modest task of developing and implementing cyber security standards capable of protecting the reliability of the Bulk-Power System, we will follow the approach that we described in the CIP NOPR of approving CIP Reliability Standards designed to safeguard the reliability of the Bulk-Power System.

Order No. 706 at P 340. The Commission identified a need for coordination with stakeholders of other infrastructures and with other government agencies in order to address interdependencies. NERC is pursuing this through the Information Sharing and Analysis Center ("ISAC") Council, which is made up of representatives from critical infrastructure sectors, including telecom, water, oil and natural gas, emergency services, and maritime, in addition to the electricity sector. The ISAC Council routinely shares information about interdependencies. Also, NERC participates in the Partnership for Critical Infrastructure Security ("PCIS") and is actively working through the PCIS Cross Sector Cyber Security Working Group to facilitate information sharing about cyber vulnerabilities and successful mitigation strategies.

### C. CIP Reliability Standards Improvement Is Underway

On March 20, the NERC Standards Committee[11] authorized the posting for comments of a Standard Authorization Request ("SAR") proposing modifications to the CIP Reliability Standards to address the directives from FERC in Order No. 706. The comment period closed on April 19, and the Standards Committee appointed a SAR Drafting Team on April 24 to review and respond to the 30 comments received on the first draft of the SAR.[12] There is active Federal agency input to this process: NIST was

[11] The NERC Standards Committee reports to the NERC Board of Trustees and is responsible for overseeing the development of Reliability Standards.

[12] Detailed information on the proposed modifications is available on the NERC website at: http://www.nerc.com/%7Efilez/standards/Project_2008-06_Cyber_Security.html.

among the entities submitting comments on the SAR, and a representative of the Bureau of Reclamation serves on the SAR Drafting Team.

The SAR, once approved by the Standards Committee, will become the framework upon which the Standard Drafting Team develops the specific revisions to the CIP Reliability Standards. The process of improving the CIP Reliability Standards will likely be structured in multiple phases to address priority items and measures such as removal of the "reasonable business judgment" language first, while recognizing that other improvements will require more time. Application of the NIST standards will be considered during the drafting of the revisions to the CIP Reliability Standards.

Another of the key topics identified in Order No. 706 is for NERC to develop guidance documents to help entities know what is expected to comply with certain aspects of the CIP Reliability Standards. The Standard Drafting Team will work closely with CIPC to develop these guidelines or examples.

In summary, NERC's Reliability Standards development process enables the progressive and continuous improvement of Reliability Standards. Going forward, NERC will address the Commission's directives and continually evaluate how these standards are executed in practice, utilizing this experience as the basis for further improvements. NERC also will monitor key industry and technology developments related to the CIP Reliability Standards, in order to ensure that the bulk power system in North America remains as reliable as possible.

## III. ENHANCED MECHANISMS TO COMMUNICATE EMERGING THREATS AND CYBERSECURITY ISSUES

As noted above, the CIP Reliability Standards in and of themselves cannot eliminate the possibility of a cyber disruption of critical national infrastructure. The limitation on NERC's jurisdiction to propose reliability standards only for the bulk power system means that the CIP Reliability Standards cannot address other critical assets – such as telecommunications systems or electricity distribution systems. Moreover, the Reliability Standards development process is by design a public and transparent one. That public process – while demonstrably successful in producing standards that have significantly enhanced the reliability of the grid – may not be ideally suited to situations where confidentiality is required (such as the response to the Aurora demonstration test).

NERC recognizes the Subcommittee's continuing interest in the response to the Aurora demonstration test. Attachment 1 contains a description of the actions taken by NERC, in its role as the ES-ISAC, to notify the industry of the identified vulnerability, define mitigation measures and assess the industry's implementation of those measures. NERC believes the industry is cooperating in completing the implementation of the recommended mitigation measures contained in the Advisory regarding cybersecurity vulnerabilities issued on June 21, 2007 by the ES-ISAC.

NERC as the ES-ISAC continues to respond to inquiries regarding the measures contained in the June 21 Advisory. Additionally, NERC meets with government agencies as requested to discuss the Aurora demonstration test. On April 25, NERC met with the Department of Defense, the Department of Energy, FERC and other agencies to review DOD installations and determine what additional actions should be taken by DOD to address vulnerabilities resulting from the Aurora demonstration test.

**Lessons Learned:** Among the key lessons learned from the Aurora demonstration test was the need to improve the alert mechanism by which the industry is made aware of significant vulnerabilities and recommended mitigation measures. While ES-ISAC alerts are, by their very nature, advisory only, with careful oversight of the implementation of recommended measures, these alerts can be effective in eliciting responses to identified cyber vulnerabilities that are not addressed by the Reliability Standards.

Additionally, the Aurora demonstration test highlighted the importance of having in place a comprehensive contact list for all users, owners and operators of the bulk power system to facilitate rapid communication of ES-ISAC advisories.

Notwithstanding the limitations on NERC's ability to deal with all aspects of the cybersecurity issue, we are acting to address effectively those aspects of the critical infrastructure cybersecurity challenge that are within our control. If a cyber exploit of an identified vulnerability is imminent, NERC as the ES-ISAC will take the following actions:

- Obtain approval from the Electricity Sector Coordinating Council to escalate the Cyber Threat Alert Level to Red;
- Post the escalated level on the ES-ISAC Web site;
- Issue an industry advisory with recommended mitigation measures/essential actions to respond to the identified vulnerability;
- Send e-mail notifications to the electric industry through distribution lists designed for notification purposes recommending that the industry promptly complete the immediate mitigation measures identified in the ES-ISAC Advisory; and
- Follow-up to monitor progress in implementing the immediate mitigation measures and report to appropriate government agencies.

Since the Aurora demonstration test, this notification system has been significantly enhanced. *First*, NERC now has in place a formal mechanism for issuing alerts to the industry about important matters that come either from NERC's own event analysis efforts or, as was the case with the Aurora demonstration test, from government agencies with specific information about possible threats. The alert system is set out in Rule 810 of NERC's Rules of Procedure[13] and has three levels:

[13] Rule 810, "Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions." *See* ftp://ftp.nerc.com/pub/sys/all_updl/rop/NERC_Rules_of_Procedure_EFFECTIVE_20080321.pdf at pp.

1) "Advisories" are purely informational and are intended to advise certain owners, operators and users of the bulk power system of findings and lessons learned.

2) "Recommendations" are specific actions that NERC is recommending be considered on a particular topic by certain owners, operators, and users of the bulk power system, according to each entity's facts and circumstances.

3) "Essential Actions" are specific actions that NERC has determined are essential to be taken by certain owners, operators, or users of the bulk power system to ensure the reliability of the bulk power system. Essential Actions require NERC board approval before issuance.

"Recommendations" and "Essential Actions" have mandatory reporting requirements on how each entity responds to the alert. This reporting will allow NERC to determine whether further actions may be necessary. FERC requires that NERC provide at least 5 business days' notice to the Commission **before** an alert is issued, with provision for shorter times in the event that faster action is necessary. The Rules of Procedure further provide that a report will be filed with the Commission (and other government agencies, as appropriate) no later than 30 days after the date on which bulk power system owners, users and operators are required to report to NERC on their actions taken in response to the notification.

These alerts are *not* the same as reliability standards – they are not enforceable with financial penalties and other sanctions. NERC believes, however, that the alerts offer an effective and expeditious means of communicating vital information to all owners, operators, and users of the bulk power system who have a need to know. When the NERC Board of Trustees determines that certain actions are essential for owners, operators, and users to take to ensure the reliability of the bulk power system, NERC believes those entities will do what is necessary.

*Second*, NERC has now developed a contact list for every owner, operator and user of the bulk power system. At present, there are over 1800 entities on the list. The list was initially developed as NERC's compliance registry, to identify the entities that are responsible for complying with the mandatory reliability standards. This list is more comprehensive than the ES-ISAC list used to distribute the June 21 Advisory.

NERC is presently using this expanded contact list for alerts, including an alert that relates to cyber security. Each alert is targeted to the types of entities to which it applies (*e.g.*, Reliability Coordinators, Transmission Operators, Generation Owners) and

---

69-70. NERC's Rules of Procedure have been approved by FERC. *See Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, at P 672; *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006); *see also North American Electric Reliability Council, et al.,* 122 FERC ¶ 61,245 (2008).

identifies the types of employees within the entity (*e.g.*, system planners, information technology workers) who need to be informed of the alert. NERC is working with the Regional Reliability Entities and industry trade associations to expand the contact list, so that we have specific contacts for executive officers, cyber security, physical security, and operations within each entity on the list.

## IV. GOVERNMENT'S ABILITY TO SHARE INFORMATION WITH THE PRIVATE SECTOR

As described above, NERC, working with the FERC, has enhanced the formal cybersecurity alerts/communication processes. However, these processes are only as good as the information being distributed. In its roles as the ERO and the ES-ISAC, NERC operates as an information bridge to the electric industry. NERC collects information from users, owners, or operators of the bulk power system, commonly about events on the power system, and shares that information throughout the industry and with government agencies. In addition to this "bottom up" flow of information, NERC also receives information from government agencies in the U.S. and Canada, which is also shared with the industry. The information regarding the Aurora demonstration test addressed in the June 21 ES-ISAC Advisory is an example of this "top down" communication.

Effective communication with the private sector that will trigger an immediate and comprehensive response to an identified vulnerability requires an ability to articulate the seriousness of the threat. NERC understands that the Subcommittee has concerns regarding whether the Department of Homeland Security, in the case of the Aurora demonstration test, shared enough information with the private sector to reveal the magnitude of the agency's concern. Where to draw the line between releasing information that is necessary to inform private action and information that actually expands the vulnerability is a concern for both the public and private sectors.

The formality of the information sharing process now in place has improved the flow of information between the government, NERC and the industry. Under Rule 810.5 of NERC's Rules of Procedure, NERC advises FERC and other applicable governmental authorities of its intent to issue advisories, recommendations and essential actions five days prior to their issuance. The benefits of this notification have already been seen with several alerts. Moreover, NERC will report to FERC on the actions taken by the relevant grid users, owners, and operators in response to an alert and the success of those actions in correcting vulnerabilities or deficiencies.

Another example of formalized information exchange is the memorandum of agreement ("MOA") between the U.S. Nuclear Regulatory Commission ("NRC") and NERC, which describes how the two organizations will communicate and cooperate in sharing of information on grid reliability in general and specifically on the analysis of events that occur on the grid that have the potential to affect nuclear power plants. First executed in 2004, the MOA was updated in 2007. Under the coordination plan for communications and information sharing during or immediately following emergencies,

NERC as the ES-ISAC will contact the NRC Headquarters Operations Officer when NERC becomes aware of a significant grid disturbance or an unusual grid event that has affected or may affect the reliability of offsite power to one or more nuclear power plants. In turn, when the NRC learns through reports from its licensees or other sources about grid events or conditions that have affected or could potentially affect the reliability of offsite power to one or more nuclear power plants, the NRC will contact NERC through the ES-ISAC.

With this structure in place, Federal agencies, including the Department of Energy and the Department of Homeland Security, should have increased confidence in NERC's ability to notify the industry expeditiously about vulnerabilities identified by the government and the appropriate actions to be taken in response.

Beyond these formal processes, CIPC meetings offer one venue for the technical discussion of vulnerabilities between government agencies and the industry. Even within these established mechanisms, however, challenges will still arise when (as in the case of the Aurora demonstration test) the information is classified or there are tight controls on the distribution of the information that needs to be communicated to the industry.

## CONCLUSION

The mandatory and enforceable CIP Reliability Standards represent an important milestone to help ensure grid reliability by improving the resiliency of control system cyber assets and enhancing their ability to withstand cyber-based attacks. The NERC Reliability Standards Development Procedure provides a systematic approach to continuously improving the standards and documenting the basis for those improvements. In addition to providing the mechanism to respond to the directions given by FERC in Order No. 706 to modify the 8 CIP Reliability Standards, this process provides the opportunity to monitor technical and other developments – including the further development of the NIST guidance – and reflect those developments, where appropriate, in the CIP Reliability Standards. NERC will continue to place a high priority on assuring that robust CIP Reliability Standards are adhered to by all responsible entities associated with the bulk power system.

Not all cybersecurity vulnerabilities, however, can be addressed through the CIP Reliability Standards. While NERC's enforcement authority is limited to the measures that are contained in the CIP Reliability Standards, we are committed to analyzing the electric grid to identify vulnerabilities, and working with government agencies and industry through the ES-ISAC and otherwise to support the rapid dissemination of information and mitigation measures for identified vulnerabilities.

# Assessment of the Implementation of the Mitigation Measures Recommended in the June 21, 2007 ES-ISAC Advisory

## Introduction

The June 21, 2007 ES-ISAC Advisory regarding cybersecurity vulnerabilities (ES-ISAC Advisory) was sent to generation owners, generation operators, transmission owners, and transmission operators. It was distributed broadly through the industry trade associations (American Public Power Association; Canadian Electricity Association; Edison Electric Institute (EEI); Electric Power Supply Association; and the National Rural Electric Cooperative Association).

The ES-ISAC Advisory consisted of three parts. The first part contained the recommended short- and mid-range (0–180 days) mitigation measures.[1] Part two was the longer term (greater than 180 days) measures.[2] Part three contained recommendations for immediate measures.[3] The ES-ISAC Advisory recommended the development of plans to implement the immediate measures in the event that a vulnerability is being exploited, but did not recommend that the immediate measures be put into practice.

After the ES-ISAC Advisory was issued, numerous conference calls were held with industry participants to explain the Advisory. Calls were convened by trade associations, reliability regions, and transmission owner and operator forums. ES-ISAC representatives also responded to inquiries from a large number of companies. In general, the industry response was constructive and demonstrated a commitment to mitigating the vulnerability. In communications with the industry, the ES-ISAC acknowledged its lack of authority to require completion of the mitigation measures, and the fact that the Advisory was not part of the NERC Reliability Standards mandatory compliance program. ES-ISAC representatives also discussed the "For Official Use Only" classification on the Advisory, which was established by the Departments of Homeland Security and Energy and the Nuclear Regulatory Commission, and the need for maintenance of the confidentiality of information.

The ES-ISAC conducted both an initial assessment of the implementation of the recommended measures and a formal, written survey to measure industry progress in completing the mitigation measures. The initial assessment was conducted in September and early October 2007 and was performed by gathering information with sector entities in phone conversations and at meetings. No formalized survey instrument was used. In addition, a small number of entities submitted unsolicited reports on their progress to the ES-ISAC.

Based on the information gathered in the discussions, the submitted reports, and expert knowledge of the ownership and geography of the bulk power system, the ES-ISAC concluded that approximately 75% of the transmission grid had received mitigation measures or such measures were in progress.

---

[1] These measures are designated as numbers 1, 2.1, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 3.1 and 3.2 in the ES-ISAC Advisory.
[2] These measures are designated as numbers 4.1, 4.2, 4.2.1, 4.2.2, 4.2.3, 5, 6, 7 and 8 in the ES-ISAC Advisory.
[3] These immediate measures are designated as numbers 1, 2, 3, 4, and 5 in the ES-ISAC Advisory.

The October 19, 2007 survey was sent to a list of 65 contacts representing major entities in the bulk power system developed by the ES-ISAC with assistance from EEI. The written survey focused on the implementation of the short- and mid-range measures only. The survey did not measure progress on the long-term measures. A blank copy of the survey and cover letter is attached.

One hundred thirty-three entities responded to the survey. The respondents ranged from small municipally owned utilities to very large, multistate, investor-owned utilities. More responses were received than surveys were distributed because in some cases, recipients further distributed the survey to affected entities. As an example, surveys were sent to reliability regions and the regions passed the survey on to multiple entities in the region. Responses to the survey were requested by November 2, 2007.

Survey respondents were assured the information submitted would be kept confidential. The following paragraph was included in the survey instrument:

> Information supplied in this response will be kept confidential by the ES-ISAC, and will not be shared in any attributable manner with any other entity or government agency, unless the ES-ISAC first provides notice of its intention to do so. Statistical summary information will be calculated from the results, and that information will be shared with select agencies in the U.S. and Canadian governments to indicate an overall state of completeness.

## General Summary of Responses[4]

The October 19 survey results indicated that 94% of the short- and mid-range mitigation measures recommended in the ES-ISAC Advisory, including the recommendation to establish a plan to implement immediate measures when and if needed, were completed or were in progress. This 94% consisted of 60% completed and 34% in progress. The remaining 6% were not being performed for a variety of reasons (not applicable due to characteristics of equipment; work being done by another entity; the measure could comprise reliability rather than help reliability).

In addition, the information received from the nuclear sector confirmed that the electricity sector worked diligently to complete mitigation measures on the bulk power system near nuclear facilities. The electricity sector took a prioritized approach to completing the mitigation measures, working in the early stages with the nuclear facilities and then continuing to work on other less critical facilities on a prioritized basis. In general, electricity sector entities weighed the risks associated with the vulnerability addressed in the ES-ISAC Advisory against risks associated with other vulnerabilities and worked to balance multiple demands for resources, perform routine maintenance, repair damage caused by weather, build new facilities for a growing economy, and replace obsolete facilities, while mitigating vulnerabilities.

Several key observations regarding the survey responses:

[4] Detailed information on the survey responses was submitted by letter dated December 5, 2007, from David A. Whiteley, Executive Vice President of NERC, to Chairman Langevin.

- The survey results were encouraging and positive and major electricity sector entities representing over 75% of the geography and ownership of the bulk power system were proactive in this mitigation effort.
- A significant portion (25% to 30%) of the sectors' entities did not have the vulnerability due to how they installed their protective systems.
- Respondents were very concerned about the confidentiality of information submitted.
- The results demonstrated a responsible and appropriate response to the ES-ISAC Advisory.

## Summary of Survey Responses by Measure (see Table 1 below)

A total of 105 responses were received on behalf of 133 entities. In certain cases, a single response was provided on behalf of multiple affiliated independent power producers. Of the 105 responses received, 32 entities indicated that none of the vulnerabilities or recommendations contained in the ES-ISAC Advisory was applicable to their facilities. This "non-applicable" response was very common for the independent power producers and a number of the smaller entities that responded their facilities did not have any remotely accessible digital protective control devices (DPCD). The remaining 73 respondents identified at least one of the recommendations in the ES-ISAC Advisory that applied to their facilities, and reported on the implementation of all of the measures that were deemed applicable.

The percentages shown in the grid below are calculated by adding the number of responses that the measure is 'complete' or 'in-progress' and dividing by the total number of responding entities that have the vulnerability. Entities classified as 'not applicable' on Table 1 because they determined that their facilities did not have the vulnerability the measure was meant to address are not included in figuring the percentage. The narrative in the grid is based on the specific survey results as shown in Table 1. Both the grid and the table are keyed to the order in which the recommendations were included in the ES-ISAC Advisory.

| Measure | Response Analysis |
|---|---|
| 1 Plan Immediate Action | Seventy of 71 respondents to which these measures are applicable indicated this is complete or in progress. This 98% (70/71) rate represented a strong effort by the sector to develop the plans to complete the five immediate actions if required. |
| 2.1 Enhance Security Remote Access | This measure is a summary of the four below it. The compliance rate was 97% rate (62/64). |
| 2.1.1 Security | This measure required strengthening the protections to reduce unauthorized remote access. The compliance rate was 98% (63/64). |
| 2.1.2 Training | This measure is to provide security training to employees with access to DPCD. While the overall compliance rate was 98% (63/64), more of the entities reported this as "in progress" (35) rather than "completed" (28). |

| | |
|---|---|
| 2.1.3 Information Protection | Respondents indicated 100% (64/64) took measures to protect DPCD access information, although 28 of 64, almost half, were still in progress. |
| 2.1.4 Seal Unused Ports | This action was more problematic for some respondents due to the virtual impossibility of sealing unused ports in some equipment. Fifty-seven of 62 respondents to which this measure applied were completed or in progress, while five believed sealing unused ports is not possible or is counter productive. |
| 3.1 Control Center Authentication | 55 of 59 respondents considered this configuration that requires an operator in the control center to authenticate a DPCD access. This measure was not feasible in some configurations nor practical if the entity was small and did not have a control room. |
| 3.2 Situation Awareness Process | 47 of 66 respondents reported that they had not performed this measure or that the measure was not applicable. This was an expected response because performance of this measure is the responsibility of Independent System Operators, Regional Transmission Organizations, and reliability coordinators, and thus not the responsibility of many of the recipients of the October 19 survey. |
| 1.1 to 1.5 Specific Immediate Measures | As discussed above, the respondents indicated a high degree of attention to developing the plans necessary to complete these measures if necessary. There was a higher degree of variation in the responses in this category due to different DPCD and equipment configurations. |

# TABLE 1

## SURVEY RESPONSES SHOWING IMPLEMENTATION OF RECOMMENDATIONS FOR SHORT-TERM AND MID-TERM MEASURES AND IMMEDIATE MEASURE PLANNING

| Mitigation Measure | Complete | In Progress | Not Performed | Not Applicable | Total |
|---|---|---|---|---|---|
| **1.** Plan immediate actions | 55 | 15 | 1 | 2 | 73 |
| **2.1** Enhance security-remote access | 38 | 24 | 2 | 9 | 73 |
| 2.1.1 Security | 38 | 25 | 1 | 10 | 74 |
| 2.1.2 Training | 28 | 35 | 1 | 5 | 69 |
| 2.1.3 Information protection | 36 | 28 | 0 | 5 | 69 |
| 2.1.4 Seal unused ports | 33 | 24 | 5 | 8 | 70 |
| **3.1** Control center authentication | 26 | 29 | 4 | 9 | 68 |
| **3.2** Situational awareness process | 7 | 12 | 12 | 35 | 66 |
| **1.1 Attachment A (only) Planning Access** | 47 | 17 | 0 | 7 | 71 |
| **1.2** Disable remote change | 45 | 14 | 5 | 4 | 68 |
| **1.3** Disable auto reclose | 41 | 11 | 2 | 14 | 68 |
| **1.4** Add time delay | 29 | 12 | 5 | 25 | 71 |
| **1.5** Disable remote close | 38 | 10 | 7 | 15 | 70 |
| **Totals** | **461** | **256** | **45** | **148** | |

ES-ISAC
ELECTRICITY SECTOR
INFORMATION SHARING AND ANALYSIS CENTER
OPERATED BY NERC

October 19, 2007

TO: Electric Sector Transmission Owner/Operators
Generation Owner/Operators

## ESISAC Advisory Follow-up Survey

On June 21, 2007, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) issued an advisory regarding a potentially serious vulnerability involving remote access to protective devices found on the electric transmission and distribution systems and in generating stations. The June 21 advisory stated the ES-ISAC would be distributing a follow-up survey to measure the progress made in the electricity sector in implementing the recommended mitigation measures. This letter includes that follow-up survey. The results of the survey will be used to determine whether the ES-ISAC should consider additional actions.

In issuing the advisory, the ES-ISAC acted pursuant to the authority of Rule 808.2.b. of NERC's Rules of Procedure. We acknowledge the terminology has not been consistent. Although the June 21 document was styled an "advisory", the document recommended specific actions to address the potential vulnerability, and therefore it clearly falls within the authority of Rule 808.2.b., "Recommendation". Rule 808 provides, in relevant part, as follows:

**808. Analysis of Off-Normal Events and System Performance**

1. NERC shall analyze system and equipment performance events that do not rise to the level of a major blackout, disturbance, or system emergency, as described in section 807. The purpose of these analyses is to identify the root causes of events that may be precursors of potentially more serious events, to assess past reliability performance for lessons learned, and to develop reliability performance benchmarks and trends.

2. NERC will screen and analyze events for significance, and information from those with generic applicability will be disseminated to the industry in the form of operations or equipment alerts of three possible types:

    a. Advisory — these alerts are purely informational, intended to alert owners, operators, and users of the bulk power system to potential problems;
    b. Recommendation — these alerts are intended to recommend specific action be taken by owners, operators, and users of the bulk power system;
    c. Required Action — these alerts are intended to require specific action by owners, operators, and users of the bulk power system. Such alerts require NERC board approval before issuance.

The survey instrument, with instructions for completion, is attached. Please return the completed survey to Stan Johnson at stan.johnson@nerc.net by November 2, 2007. Please note the survey asks for responses only with respect to Attachment A to the June 21 advisory. No response is

requested at this time for Attachment B. If you have questions or need additional information, please contact Scott Mix at scott.mix@nerc.net or Stan Johnson.

We recommend a coordinated effort be made at each entity to compile a single response rather than multiple responses from the same entity. The ES-ISAC is working with the regional reliability organizations, EEI, and CEA to deliver the survey instrument to the right people in the right entities.

Thank you for your prompt cooperation in this important matter.

Sincerely,

Rick

Richard P. Sergel

Attachment

# Mitigation Status Report

| | |
|---|---|
| Company Name | |
| Contact Name | |
| Contact Phone | |
| Contact Email | |

**Instructions:**

Please enter the status of your mitigation plans and progress in the spreadsheet below. For each identified measure in the advisory, enter an "X" in either "Complete", "In Progress", or "Not Performing".

If you indicate "Complete", then you have completed the indicated mitigation for all locations requiring mitigation.

If you enter "Not Performing", you must provide a brief reason statement in the "Reason" field.

If you indicate "In Progress", you may use the "Reason" field to provide additional information.

Spreadsheet cells requiring a response have been colored cyan.

A response is required for each Mitigation, even if that response is "Not Performing".

For the measures in Attachment A, indicate ONLY the status of your plans for implementation, and indicate the overall status of all measures in Attachment A as the status of Mitigation Measure 1.

No response is requested or required for the Mitigation Measures in Attachment B (long-term).

Do not enter any location or company identifying information in the reason field below. For "In Progress" comments, a percentage of completion or other non-identifying information (e.g., all 230Kv stations complete; working on 135kV stations) should be entered. For "Not Performing", please be as specific as possible without providing any identifying information, to allow the ES-ISAC to understand the rationale for not performing the specific mitigation.

Information supplied in this response will be kept confidential by the ES-ISAC, and will not be shared in any attributable manner with any other entity or government agency, unless the ES-ISAC first provides notice of its intention to do so. Statistical summary information will be calculated from the results, and that information will be shared with select agencies in the US and Canadian governments to indicate an overall state of completeness.

The spreadsheet is designed to print the identifying information and instructions on a separate page than the detailed information so that the analysis can be more readily performed without any identifying information.

| Mitigation | Completion Status | | | |
|---|---|---|---|---|
| | Complete | In Progress | Not Performing | Reason |
| Short Term (0-60 Days) | | | | |
| Measure 1 | | | | |
| Measure 2.1 | | | | |
| Measure 2.1.1 | | | | |
| Measure 2.1.2 | | | | |
| Measure 2.1.3 | | | | |
| Measure 2.1.4 | | | | |
| Mid Term (60-180 days) | | | | |
| Measure 3.1 | | | | |
| Measure 3.2 | | | | |

| | Planning Only | | | |
|---|---|---|---|---|
| | Complete | In Progress | Not Performing | Reason |
| Attachment A: | | | | |
| Immediate (0-60 days) | | | | |
| Measure I.1 | | | | |
| Measure I.2 | | | | |
| Measure I.3 | | | | |
| measure I.4 | | | | |
| Measure I.5 | | | | |