IMPLICATIONS OF CYBER VULNERABILITIES ON THE RESILIENCE AND SECURITY OF THE ELECTRIC GRID

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

MAY 21, 2008

Serial No. 110–117

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

43–177 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

JAMES R. LANGEVIN, Rhode Island, *Chairman*

ZOE LOFGREN, California
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
AL GREEN, Texas
BILL PASCRELL, JR., New Jersey
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MICHAEL T. MCCAUL, Texas
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
PAUL C. BROUN, Georgia
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Director and Counsel*
DR. CHRIS BECK, *Senior Advisor for Science and Technology*
CARLA ZAMUDIO-DOLAN, *Clerk*
KEVIN GRONBERG, *Minority Professional Staff Member*

CONTENTS

Page

STATEMENTS

The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island, and Chairman, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology:
Oral Statement 1
Prepared Statement 3
The Honorable Ginny Brown-Waite, a Representative in Congress From the State of Florida 4

WITNESSES

The Honorable Joseph T. Kelliher, Chairman, Federal Energy Regulatory Commission (FERC), Accompanied by Joseph McClelland, Director, Office of Electric Reliability, FERC:
Oral Statement 6
Prepared Statement 7
Mr. Richard Sergel, President and Chief Executive Officer, North American Electric Reliability Corporation (NERC):
Oral Statement 13
Prepared Statement 14
Mr. Greg Wilshusen, Director, Information Security Issues, Government Accountability Office (GAO), Accompanied by Naba Barkakati, Senior Level Technologist, GAO:
Oral Statement 25
Prepared Statement 26
Mr. William R. McCollum, Jr., Chief Operating Officer, Tennessee Valley Authority (TVA), Accompanied by John Long, Chief Administrative Officer, TVA:
Oral Statement 32
Prepared Statement 34

FOR THE RECORD

Mr. Bill Pascrell, Jr., a Representative in Congress From the State of New Jersey:
Exhibit A: ES–ISAC Advisory Follow-up Survey 45
Exhibit B: Letters 47

APPENDIX

Questions From Chairman James R. Langevin 81

IMPLICATIONS OF CYBER VULNERABILITIES ON THE RESILIENCE AND SECURITY OF THE ELECTRIC GRID

Wednesday, May 21, 2008

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:13 p.m., in Room 311, Cannon House Office Building, Hon. James R. Langevin [chairman of the subcommittee], presiding.

Present: Representatives Langevin, Lofgren, Etheridge, Green, Pascrell, McCaul, and Brown-Waite.

Also present: Representative Jackson Lee.

Mr. LANGEVIN. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on Implications of Cyber Vulnerabilities on the Resiliency and Security of the Electric Grid.

I will begin by recognizing myself for an open statement.

Good afternoon. I would like to thank our witnesses for testifying today.

Over the last year, this subcommittee has spent a lot of time and energy on improving Federal network security. Today's issue, the security of our critical infrastructure networks, is one that demands equal attention. The effective functioning of our critical infrastructure, from dams and water systems to factories and the electric grid, is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions.

Once largely proprietary closed systems, control systems are becoming increasingly connected to open networks such as corporate intranets and the Internet itself. This connectivity places these infrastructures at increased risk of intentional or unintentional control system failures which can have a significant and potentially devastating impact on the economy, public health and national security of the United States.

There can be no doubt that America's critical infrastructure networks are under constant threat. Pervasive vulnerabilities of hardware and software and the connectivity of these machines to the Internet make our multi-layered lines of defense, meaning anti-virus, firewall and intrusion detection, relatively ineffective in addressing the problem.

To compound matters, many organizations prefer to focus on the deployment of new technology without regard for the security or integrity of their systems or information. This often means that information security officers are simultaneously facing increased responsibility and shrinking budgets.

These are overwhelming challenges without clear solutions. The Federal Government and the private sector must act with a sense of urgency to address these issues; and yet, as I read today's testimony, I still do not get the sense that we are addressing cybersecurity with the seriousness that it deserves.

Today's hearing will focus on two primary issues.

First, we will receive an update from the Federal Energy Regulatory Commission, FERC, and the North American Electric Reliability Corporation, NERC, about electric industry efforts to mitigate a cyber vulnerability known as Aurora. I think we could search far and wide and not find a more disorganized, ineffective response to an issue of national security of this import. Everything about the way this vulnerability was handled, from press leaks, to DHS's failure to provide more technical details to support the results of its test, to NERC's dismissive attitude to the industry's halfhearted approach toward mitigation, leaves me with little confidence that we are ready or willing to deal with the cybersecurity threat.

As time passes, I grow particularly concerned by NERC, the self-regulating organization responsible for ensuring the reliability of the bulk power system. Not only do they propose cybersecurity standards that, according to the GAO and NIST, are inadequate for protecting critical national infrastructure, but throughout the committee's investigation they continued to provide misleading statements about their oversight of industry efforts to mitigate the Aurora vulnerability.

If NERC doesn't start getting serious about national security, it may be time to find a new electric reliability organization. NERC can begin demonstrating its commitment by incorporating more of the NIST security controls in the next iteration of its reliability standards.

Now I am thankful today that Chairman Kelliher and his staff at FERC are taking cybersecurity seriously. In earlier correspondence, Chairman Thompson and I voiced our concern that the Commission not only lacked authority to regulate potentially vulnerable cybersecurity assets, but they are not covered in the NERC standards, but also the authority to issue orders to owners and operators in the event of an imminent exploitation of an asset on the grid.

The chairman and I fully support FERC's request for additional legal authorities to adequately protect the bulk power system, and we certainly look forward to working with you and the appropriate committees in the future.

Our second issue of discussion today involves the GAO investigation that this committee commissioned last year. We asked GAO to provide insight into the cybersecurity controls of the Nation's largest public power utility, the Tennessee Valley Authority, TVA. The TVA's service area covers 80,000 square miles in the southeastern United States, with a total population before 8.7 million people.

Unfortunately, the GAO found that the TVA security posture was seriously lacking. According to the report, TVA has not implemented appropriate security practices to secure the control systems and networks used to operate its critical infrastructures. Until TVA addresses these weaknesses, it risks a disruption of its operations as a result of a cyber incident which could impact its customers.

Now I am pleased to hear that TVA has taken significant steps toward implementing higher levels of security.

But these problems are not unique to TVA. I believe they are typical of security practices across the industry; and given what we have seen with the Aurora mitigation, I have little confidence that the industry is taking appropriate actions.

Now, in closing, I would like to challenge each of you here and everyone in the industry to, among other things, prove to our committee that you are serious about cybersecurity. Show us you are willing to adopt better standards because it will make the entire grid more secure. Leverage the critical infrastructure community to push control system vendors to build more secure products and commit the manpower and the money to mitigating your vulnerabilities.

I can say this, that we will continue our oversight in this area. It will be robust. In the next subcommittee hearing, though, I certainly look forward to talking about all the progress the industry has made in meeting our challenges.

[The statement of Chairman Langevin follows:]

PREPARED STATEMENT OF CHAIRMAN JAMES R. LANGEVIN

MAY 21, 2008

Good afternoon. I'd like to thank our witnesses for testifying today. Over the last year, this subcommittee has spent a lot of time and energy on improving Federal network security. Today's issue—the security of our critical infrastructure networks—is one that demands equal attention.

The effective functioning of our critical infrastructure—from dams and water systems, to factories and the electric grid—is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. This connectivity places these infrastructures at increased risk of intentional or unintentional control system failures, which can have a significant and potentially devastating impact on the economy, public health, and national security of the United States.

There can be no doubt that America's critical infrastructure networks are under constant threat. Pervasive vulnerabilities in hardware and software, and the connectivity of these machines to the Internet make our multilayered lines of defense—anti-virus, firewall, and intrusion detection—relatively ineffective in addressing the problem. To compound matters, many organizations prefer to focus on the deployment of new technology without regard for the security or integrity of their systems or information. This often means that information security officers are simultaneously facing increased responsibilities and shrinking budgets.

These are overwhelming challenges without clear solutions. The Federal Government and the private sector must act with a sense of urgency to address these issues, and yet, as I read today's testimony, I still do not get the sense that we are addressing cybersecurity with the seriousness it deserves.

Today's hearing will focus on two primary issues. First, we will receive an update from the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) about electric industry efforts to mitigate a cyber vulnerability known as Aurora. I think we could search far and wide and not find a more disorganized, ineffective response to an issue of national security. Everything about the way this vulnerability was handled—from press leaks, to DHS's failure to provide more technical details to support the results of its test, to NERC's

dismissive attitude, to the industry's half-hearted approach toward mitigation—leaves me with little confidence that we are ready or willing to deal with the cybersecurity threat.

As time passes, I grow particularly concerned by NERC, the self-regulating organization responsible for ensuring the reliability of the bulk power system. Not only did they propose cybersecurity standards that—according to the GAO and NIST—are inadequate for protecting critical national infrastructure, but throughout the committee's investigation they continued to provide misleading statements about their oversight of industry efforts to mitigate the Aurora vulnerability. If NERC doesn't start getting serious about national security, it may be time to find a new electric reliability organization. NERC can begin demonstrating its commitment by incorporating more of the NIST security controls in the next iteration of its reliability standards.

I am thankful that Chairman Kelliher and his staff at FERC are taking cybersecurity seriously. In earlier correspondence, Chairman Thompson and I voiced our concern that the Commission not only lacked authority to regulate potentially vulnerable cybersecurity assets that are not covered in the NERC standards, but also the authority to issue orders to owners and operators in the event of an imminent exploitation of an asset on the grid. The Chairman and I fully support FERC's request for additional legal authorities to adequately protect the bulk power system, and we look forward to working with you and the appropriate committees in the future.

Our second issue of discussion today involves a GAO investigation that this committee commissioned last year. We asked GAO to provide insight into the cybersecurity controls of the Nation's largest public power company, the Tennessee Valley Authority (TVA). The TVA's service area covers 80,000 square miles in the southeastern United States, with a total population of about 8.7 million people. Unfortunately, GAO found that TVA's security posture was seriously lacking. According to the report, TVA has not fully implemented appropriate security practices to secure the control systems and networks used to operate its critical infrastructures. Until TVA addresses these weaknesses, it risks a disruption of its operations as a result of a cyber incident, which could impact its customers.

I am pleased to hear that TVA has taken significant steps toward implementing higher levels of security. But these problems are not unique to TVA. I believe they are typical of security practices across the industry. And, given what we've seen with the Aurora mitigation, I have little confidence that the industry is taking the appropriate actions.

In closing, I'd like to challenge each of you here, and everyone in the industry. Prove to our committee that you are serious about cybersecurity. Show us you're willing to adopt better standards because it will make the entire grid more secure. Leverage the critical infrastructure community to push control system vendors to build more secure products. And commit the manpower and the money to mitigating your vulnerabilities.

We will continue our oversight in this area. At the next subcommittee hearing, I look forward to talking about all the progress the industry has made in meeting our challenges.

Mr. LANGEVIN. With that, the Chair now recognizes the ranking member of the subcommittee, standing in for Mr. McCaul from Texas. The gentlelady from Florida, Ms. Ginny Brown-Waite, is recognized 5 minutes.

Ms. BROWN-WAITE. Thank you, Mr. Chairman.

I look forward to hearing from Chairman Kelliher today as he provides us with an update on FERC's progress in implementing critical infrastructure protection standards that were issued earlier this year.

While I understand the new regulations are not perfect, I believe that they are a positive step toward ensuring that the electric grid remains available to provide reliable energy despite emerging threats. Clearly, though, more can be done to secure the assets critical to generating, transmitting and delivering power, but I am pleased by efforts that are already under way to increase the focus on security.

Regarding TVA's inadequate security posture a lack of regulation does not seem to be the issue. There are already Federal network security regulations in place, regulations that it clearly appears that TVA just has not lived up to. Regardless of whether harmful incidents arise from malicious attacks or operator error, the effect would be the same, serious damage to the critical infrastructure and limited ability of TVA to provide power to its customers.

I understand that TVA actually has agreed with the majority of GAO's recommendations and has a plan in place to mitigate the vulnerabilities that GAO identified. Certainly this is good news. But I urge the TVA management to make every possible effort to secure their computer systems quickly and to fortify their critical assets. The increasing interconnectivity of computer systems and dire economic consequences of a successful network-based attack warrant very careful oversight of computer security efforts.

I look forward to hearing from the witnesses today, and I thank you all very much for being here.

With that, I yield back.

Mr. LANGEVIN. I thank the gentlelady.

Other members of the subcommittee at some point are reminded of the committee rules that opening statements may be submitted for the record.

I now welcome our distinguished panel of witnesses.

Our first witness, Mr. Joseph Kelliher, is the chairman of the Federal Energy Regulatory Commission. Chairman Kelliher was nominated by President George W. Bush and was sworn in on November 20, 2003, for a first term and on December 21, 2007, for his second term. He was designated chairman of the Commission by President Bush effective July 9, 2005. Before becoming a Commissioner, Mr. Kelliher was a senior policy adviser to Secretary of Energy, Spencer Abraham. In that capacity, he advised the Secretary in a wide range of energy policy matters; and I thank you for being here, Mr. Chairman.

Our second witness, Mr. Richard Sergel, has been President and Chief Executive Officer of the North American Electric Reliability Corporation since September 12, 2005. Until 2004, Mr. Sergel served as President and Chief Executive Officer for the National Grid USA and was National Grid Group PLC Executive Director for North America on the completion of the National Grid New England electric system merger in March, 2000.

Our third witness is Mr. Greg Wilshusen, Director for Information Security Issues at GAO, where he reads information security related studies and audits the Federal Government. Mr. Wilshusen has testified before the subcommittee on a number of occasions, and we certainly welcome you back today.

Our fourth witness is Mr. William McCollum, the Chief Operating Officer of the Tennessee Valley Authority. He has held that position since April, 2007. He is responsible for the management of TVA power's production, transmission, power trading and resources management programs.

Welcome to you, Mr. McCollum.

Without objection, the witnesses' full statements will be inserted into the record; and I now ask each witness to summarize their statement for 5 minutes, beginning with Chairman Kelliher.

STATEMENT OF THE HONORABLE JOSEPH T. KELLIHER, CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION (FERC), ACCOMPANIED BY JOSEPH MC CLELLAND, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FERC

Mr. KELLIHER. Thank you, Mr. Chairman; and I want to commend you and the subcommittee for its interest in these important issues.

I am accompanied today by Joseph McClelland, who is the Director of the FERC Office of Electric Reliability, who testified before the subcommittee last fall; and I appreciate the opportunity to discuss the need to improve cybersecurity and to protect the reliability of the power grid against cyber attacks.

Congress made FERC responsible for overseeing reliability of the power grid, guarding the grid against reliability attacks, including cyber threats, by establishing and enforcing mandatory reliability standards; and that duty was established by the Energy Policy Act of 2005.

Since then, much progress has been made on grid reliability. We have certified the Electric Reliability Organization, established mandatory reliability standards. We are working to improve those standards over time and are establishing an enforcement regime. But today I would like to focus my remarks on the cyber threat to the grid and the need for effective defense.

In my letter to the subcommittee of November 7 of last year, I stated my view that an effective defense of the power grid from cyber attack has three necessary elements: No. 1, timely and effective identification of cyber vulnerabilities; No. 2, an ability to adopt mandatory reliability standards that mitigate the vulnerability on a timely basis; and, No. 3, an ability to maintain the confidentiality of information regarding cyber vulnerability during the standards development process, during Commission review, and during compliance monitoring and development.

In my view, current law is inadequate to mount such a defense and that FERC needs additional legal authority to effectively guard the power grid from national security threats such as cyber attacks.

With respect to the first element of an effective defense, FERC is not a national security or an intelligence agency; and we are not in the best position to identify cyber threats. U.S. Government, though, does have the ability to identify cyber threats in a timely and effective manner. FERC cooperates with agencies that are in a better position to assess these vulnerabilities.

With respect to the second element of an effective defense, currently there is not an adequate means to establish mandatory reliability standards in a timely manner. Currently, there are two basic means to protect the grid against cyber threats: No. 1, the process in the Energy Policy Act, section 215 of the Federal Power Act; or, No. 2, NERC advisories. In my view, neither means is adequate. The 215 process produces reliability standards that are mandatory but untimely, given the nature of cyber threats, while NERC advisories are timely but voluntary.

With respect to the 215 process, FERC is using and will continue to use the process established by section 215 to set reliability standards including cyber standards. Just last January, we ap-

proved eight critical infrastructure protection standards, with 160 requirements designed to improve cybersecurity; and I think those standards will improve cybersecurity.

But the principal flaw of the 215 process is it simply takes too long. It does not allow for protection of critical information. Under the 215 process, it can take years to develop new and modified reliability standards, including cyber standards.

If you ask why is there a need for timely action in this area, I think it is because the cyber threat is fundamentally different from other reliability threats. The section 215 of the Federal Power Act was to designed to address different reliability challenges.

Most regional blackouts in the past have been caused in part by poor vegetation management near power lines, trees. The section 215 process was designed in response to western blackouts in the summer of 1996 that involved tree contact. It was not designed with a cyber threat in mind, and I think the reliability threat posed by poor vegetation management and trees is a fundamentally different threat than the cyber threat. The cyber threat is a national security threat that may be posed by foreign governments or organized groups, and the process designed to guard against poor vegetation management is not well-suited to meet national security threats.

The second means of protecting the power grid from cyber threats, the alternative to the mandatory reliability standard under 215, is the NERC advisory; and the principal virtue of the advisory is dispatch. Its fundamental flaw is that compliance is voluntary.

In the advisory issued last year in response to NERC, I want to commend NERC for acting quickly in response to that threat. As detailed in our testimony, FERC has been reviewing the industry response to the advisory. Significant progress has been made, but the results have been inconsistent. I think that is, frankly, the predictable result of voluntary advisory, but those inconsistencies can weaken the grid because the grid is interconnected.

The third element is confidentiality. The third element of an effective defense is confidentiality. The standards development process established under 215 typically imposes few or no restrictions on dissemination of information. In the case of cyber vulnerability, public release of information related to cybersecurity can be very harmful.

For those reasons, we have concluded that legislation is necessary to address the cyber threat and be able to mount an effective defense; and we look forward to working with the committee and the committee of jurisdiction, the Energy and Commerce Committee, to give FERC the authority it needs to be able to effectively defend the power grid against cyber threats.

With that, I just want to thank the subcommittee for its interest.

[The statement of Mr. Kelliher follows:]

PREPARED STATEMENT OF JOSEPH T. KELLIHER

MAY 21, 2008

Mr. Chairman and Members of the subcommittee, thank you for the opportunity to speak with you today about the cyber vulnerabilities of the Nation's bulk power system. I appreciate the subcommittee's attention to this critically important issue.

The Energy Policy Act of 2005 (EPAct 2005) made the Federal Energy Regulatory Commission (FERC or Commission) responsible for overseeing the reliability of the bulk power system. EPAct 2005 authorized the Commission to approve and enforce mandatory reliability standards, including cyber security standards, to protect and improve the reliability of the Nation's bulk power system. Under the new statutory framework, reliability standards are proposed by the Electric Reliability Organization (ERO) (the North American Electric Reliability Corporation or NERC) to the Commission for its review. The Commission must either approve the proposed standards or remand them to NERC. The Commission and NERC are well underway in implementing the new law, including now having in place an initial set of mandatory cyber security standards with varying effective dates. Much progress has been made in the past 3 years. However, more work needs to be done, both with respect to improving those cyber security standards and possibly adding new ones. In addition, the Commission has made substantial progress in examining whether industry has in place adequate mitigation to address the cyber security vulnerability, known as Aurora, which was raised at the subcommittee's last hearing on cyber security threats to the transmission grid.

Protecting the interstate bulk power system against cyber security threats is critical to the welfare of our Nation's citizens. It is therefore appropriate to examine whether sufficient Federal authority exists to take timely and effective action to protect against such threats, particularly in emergency circumstances. In my view, FERC currently does not have sufficient authority to adequately guard against cyber security threats to reliability of the bulk power system.

BACKGROUND

In EPAct 2005, the Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability standards for the Nation's bulk power system (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. Section 215 requires the Commission to select an ERO that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory only after Commission approval. The ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission review and approval. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

The Commission may approve proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification on a specific matter. The Commission also may initiate enforcement on its own motion.

The Commission has implemented section 215 diligently. In anticipation of reliability legislation being passed, it established a reliability group at the agency even before the passage of EPAct 2005. Within 180 days of enactment, the Commission adopted rules governing the reliability program. In the summer of 2006, it approved NERC as the ERO. In March 2007, the Commission approved the first set of national mandatory and enforceable reliability standards. In April 2007, it approved eight regional delegation agreements to provide for development of new or modified standards and enforcement of approved standards by Regional Entities. The Commission has since approved eight additional reliability standards.

In exercising its new authority, the Commission has interacted extensively with NERC and the industry. The Commission also has coordinated with other Federal agencies, such as the Department of Homeland Security, the Department of Energy, the Nuclear Regulatory Commission, and the Department of Defense. Also, the Commission has established regular communications with regulators from Canada and Mexico regarding reliability, since the North American bulk power system is an interconnected continental system subject to the laws of three nations.

CYBER SECURITY STANDARDS APPROVED UNDER SECTION 215

Section 215 defines "reliability standard[s]" as including requirements for the "reliable operation" of the bulk power system including "cybersecurity protection." Section 215 defines reliable operation to mean operating the elements of the bulk power system within certain limits so instability, uncontrolled separation, or cascading

failures will not occur "as a result of a sudden disturbance, including a cybersecurity incident." Section 215 also defines a "cybersecurity incident" as a "malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."

In August 2006, NERC submitted eight new cyber security standards, known as the Critical Infrastructure Protection (CIP) standards, to the Commission for approval under section 215. NERC proposed an implementation plan under which certain requirements would be "auditably compliant" beginning by mid-2009 and the others would be so by the end of 2010.

On January 18, 2008, the Commission issued a Final Rule approving the CIP Reliability Standards and concurrently directed NERC to develop modifications addressing specific concerns.

The eight CIP standards contain over 160 requirements and sub-requirements. Generally, the CIP standards will require the following actions when fully implemented at the end of 2010:

- *Critical Cyber Asset Identification*.—Requires the identification of an entity's critical assets and critical cyber assets using a risk-based assessment methodology.
- *Security Management Controls*.—Requires an entity to develop and implement security management controls to protect critical cyber assets.
- *Personnel and Training*.—Requires personnel with access to critical cyber assets to go through identity verification, criminal background checks and employee training.
- *Electronic Security Perimeters*.—Requires the identification and protection of electronic security perimeters and access points. The security perimeters are to encompass the critical cyber assets.
- *Physical Security of Critical Cyber Assets*.—Requires the creation and maintenance of a physical security plan that ensures all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.
- *Systems Security Management*.—Requires an 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 the perimeter.
- *Incident Reporting and Response Planning*.—Requires the identification, classification and reporting of cyber security incidents related to critical cyber assets.
- *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.

In the Final Rule, the Commission stated its concern with the breadth of discretion left to utilities by the standards. For example, the standards state that utilities "should interpret and apply the reliability standard[s] using reasonable business judgment." Similarly, the standards at times require certain steps "where technically feasible," but this is defined as not requiring the utility "to replace any equipment in order to achieve compliance." Also, the standards would allow a utility at times not to take certain action if the utility documents its "acceptance of risk." To address this, the Final Rule directed NERC to, among other things:

- Develop modifications to the CIP reliability standards to remove the "reasonable business judgment" language.
- Develop modifications to remove "acceptance of risk" exceptions from the CIP reliability standards.
- Develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception. This allows flexibility and customization of implementation of the CIP reliability standards in a controlled manner that includes external oversight and audit.
- Provide additional guidance regarding the development of a risk-based assessment methodology for the identification of critical assets.

For certain other requirements in the CIP standards, the Commission addressed its concern about discretion by requiring external oversight of utility decisions, such as critical assets lists. This oversight could be provided by industry entities with a "wide-area view," such as reliability coordinators or the Regional Entities, subject to the review of the Commission.

CURRENT PROCESS TO PROTECT CYBER SECURITY OF BULK POWER SYSTEM

In my view, section 215 is an adequate statutory foundation to protect the bulk power system against most reliability threats. However, the cyber security threat is different. It is a national security threat that may be posed by foreign nations,

or others intent on undermining the United States through its electric grid. The nature of the threat stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and relay maintenance. Given the national security dimension to the cyber security threat, there may be a need to act quickly to protect the bulk power system, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure. Our legal authority is inadequate for such action.

Section 215 Process

As an initial matter, it is important to recognize how mandatory reliability standards are established under section 215. Under section 215, reliability standards are developed by the ERO through an open and public process. The Commission can direct NERC to develop a reliability standard to address a particular reliability vulnerability, including cyber security threats. However, the NERC process can take years to develop standards for the Commission's review. In fact, the cyber security standards approved by the agency last January took the industry approximately 3 years to develop.

Section 215 relies on the ERO to develop and submit proposed reliability standards. NERC's procedures for doing so allow extensive opportunity for industry comment, are open, and are generally based on the procedures of the American National Standards Institute (ANSI). The NERC process is intended to develop consensus on both the need for the standard and on the substance of the proposed standard. Although inclusive, the process is not nimble.

Key steps in the NERC process include: nomination of a proposed standard using a Standard Authorization Request (SAR); public posting of the SAR for comment; review of the comments by industry volunteers; drafting or redrafting of the standard by a team of industry volunteers; public posting of the draft standard; field testing of the draft standard, if appropriate; formal balloting of the draft standard, with approval based on 75 percent of total votes and two-thirds of weighted industry sector votes; re-balloting, if negative votes are supported by specific comments; voting by NERC's board of trustees; and an appeals mechanism to resolve any complaints about the standards process. NERC-approved standards are then submitted to the Commission for its review.

For the first set of reliability standards proposed by NERC and for the CIP standards, the Commission began its process by issuing a staff assessment of the proposed standards and allowing public comment on the assessment. Based on its consideration of those comments, the Commission then issued a Notice of Proposed Rulemaking identifying the Commission's proposed actions and allowing additional opportunities for public comment. After considering these additional comments, the Commission issued a Final Rule approving the proposed standards and requiring NERC to prospectively modify them using its standards development process, thereby engaging industry.

Generally, the procedures used by NERC are appropriate for developing and approving reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process is a strength of the process as it relates to most reliability standards. However, it can be a weakness in the development of cyber security standards, given the nature of the threat.

The procedures used under section 215 for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber security risks to the bulk power system, particularly in emergency situations. Certain circumstances, such as those involving national security, may require immediate action. If a significant vulnerability in the bulk power system is identified, procedures used so far for adoption of reliability standards take too long to implement effective corrective steps.

FERC rules governing review and establishment of reliability standards allow the agency to direct the ERO to develop and propose reliability standards under an expedited schedule. For example, FERC could order the ERO to submit a reliability standard to address an identified reliability vulnerability within 60 days. NERC's rules of procedure include a provision for approval of urgent action standards that can be completed within 60 days and which may be further expedited by a written finding by the NERC board of trustees that an extraordinary and immediate threat exists to bulk power system reliability or National security.

However, even a reliability standard developed under the urgent action provisions would likely be too slow in certain circumstances. Faced with a cyber security or other national security threat to reliability, FERC may need to act decisively in hours or days, rather than months or years. That would not be feasible under the

urgent action process. In the meantime, the bulk power system would be left vulnerable to a known cyber security threat. Moreover, existing procedures, including the urgent action procedure, would widely publicize the vulnerability and the possible solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, the proposed standard submitted to the Commission may not be sufficient to address the vulnerability. As noted above, when a proposed reliability standard is submitted to FERC for its review, whether submitted under the urgent action provisions or the usual process, the agency cannot modify such standard and must either approve or remand it. Since the Commission may not modify a proposed reliability standard under section 215, we would have the choice of approving an inadequate standard and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. Under either approach, the bulk power system could remain vulnerable for a prolonged period.

NERC Advisories

Currently, the alternative to a mandatory reliability standard is for NERC to issue an advisory encouraging utilities and others to take action to guard against cyber vulnerabilities. That approach provides for quicker action, but any such advisory is voluntary, and should be expected to produce inconsistent responses. That was our experience with the response to an advisory issued last year by NERC regarding an identified cyber security threat. Since the grid is interconnected, those inconsistencies can retard cyber security measures. Reliance on voluntary measures to assure cyber security is fundamentally inconsistent with the conclusion Congress reached during enactment of the Energy Policy Act, namely that voluntary standards cannot assure reliability of the bulk power system.

In response to the risk of cyber attack identified last year as Aurora, this subcommittee convened a hearing on October 17, 2007. Mr. Joseph H. McClelland, the Director of the Commission's Office of Electric Reliability, testified at that hearing. NERC reported that it issued an advisory to generator owners, generator operators, transmission owners, and transmission operators. According to NERC, this advisory identified a number of short-term measures, mid-term measures and long-term measures designed to mitigate the cyber vulnerability. NERC asked the recipients to voluntarily implement the measures. NERC also sent a data request to industry members to determine compliance with the advisory. That data request was limited in scope, however, asking only that industry members indicate if their mitigation plans are "complete," "in progress," or "not performing."

The Commission determined that the information sought by NERC in the above data request was not sufficient for the Commission to discharge its duties under section 215 because it did not provide sufficient details about individual mitigation efforts for the Commission to be certain that the threat had been addressed. For example, it did not provide information such as what facilities were the subject of the mitigation plans, what steps to mitigate the cyber vulnerability were being taken, and when those steps were planned to be taken—and, if certain actions were not being taken, why not. Therefore, on October 23, 2007, the Commission provided notice to the Office of Management and Budget (OMB) that it intended to immediately issue a directive requiring all generator owners, generator operators, transmission owners, and transmission operators that are registered by NERC and located in the United States to provide to NERC certain information related to actions they have taken or intend to take to protect against the cyber vulnerability; this would allow the Commission to review the mitigation plans at a central location to be certain that the vulnerability had been addressed. The Commission requested emergency processing of this proposed information collection. After receiving clearance from OMB, the Commission issued a Notice of Proposed Information Collection and Request for Comments (Notice). Comments were due on January 14, 2008.

The Commission received seven sets of comments in response to the Notice, including joint comments filed by four industry trade associations: American Public Power Association, Edison Electric Institute, National Rural Electric Cooperative Association, and the Electric Power Supply Association. These trade associations represented the majority of entities that would be required to respond to the proposed information collection. A common concern among the commenters was the need to ensure the confidentiality of sensitive information that would be provided in response to the proposed information collection. Commenters urged that the Commission implement additional security measures to safeguard the collected information. Commission staff met with trade association representatives to discuss these concerns and how they might be addressed. Rather than experience further delays by answering these objections to the proposed mandatory information collection, it was determined that staff would first work with industry groups to develop a plan

to informally gather information, on a voluntary basis, regarding the status of compliance with NERC's Aurora advisory. In February, Commission staff began performing interviews with a stratified sampling of electric utilities concerning their compliance with the Aurora advisory. These interviews are continuing as of this date.

Commission staff has conducted over 20 detailed interviews with a variety of electric utilities geographically dispersed across the contiguous 48 States, to assess the state of the industry's protection against remote access cyber vulnerabilities, including the Aurora vulnerability. The utilities were selected to encompass both large and small companies, and a mixture of generating companies, transmission companies, and mixed-asset companies. The sample of companies included both investor-owned utilities and cooperative organizations. Interviews with publicly owned utilities and municipal organizations are planned in the near future. Each interview typically lasted 6 to 8 hours and utilities voluntarily participated. The utilities were well prepared with documents to explain their actions, and were very cooperative in responding to staff questions.

Topics discussed included the use of passwords and other forms of access controls, means of authenticating users, physical security of cyber assets, means of communicating, vendor access, access revocation, the use of firewalls and intrusion detection/prevention devices, vulnerability assessments, the ways in which communications devices are utilized, as well as the prevalence and functionality of digital control devices. Staff found a wide range of equipment, configurations and security features implemented by the utilities interviewed. While staff intends to perform more interviews, there are several observations that can be made based on the interviews to date.

All of the companies selected by the Commission fully cooperated in the interviews. We learned that no company we interviewed ignored the Aurora advisory, although we did find there was a broad range of compliance based on individual interpretations of the threat and the application of the recommended mitigation measures. In fact, all of the utilities interviewed by the Commission requested additional information to help understand the technical implications of the attack and the specific strategies to mitigate the identified vulnerabilities. Through these selected interviews, FERC staff has determined that although progress has been made by every entity it interviewed, much work remains to be done.

While NERC can issue an alert, as it did in response to the Aurora vulnerability, compliance with these alerts is voluntary. Further, as Commission staff has found with the Aurora alert, such alerts can cause uncertainty about the specific strategies needed to mitigate the identified vulnerabilities.

CONCLUSION

The Congress made FERC responsible for overseeing the reliability of the bulk power system, but it provided specific restrictions on the procedures to be used to develop and put into effect mandatory reliability standards. Section 215 is an adequate basis to protect the bulk power system against most reliability threats, and for that reason I do not believe there is a need to amend section 215. However, I believe a different statutory mechanism is needed to protect the grid against cyber security threats, given the nature of these threats. One approach would allow the Commission to directly establish interim reliability standards that are mandatory and enforceable upon a finding by a national security or intelligence agency that there is a national security threat to the bulk power system. This narrowly tailored approach would ensure that reliability of the bulk power system can be protected until the ERO reliability standards development process can create a permanent reliability standard. It also would provide that the authority be used rarely, in instances when other appropriate agencies determine that a threat is real and the Commission determines existing standards to be inadequate. It also may be necessary to authorize the Commission to protect certain information from disclosure, if its release could have significant adverse effect on the health and safety of the public or the common defense or national security.

The full range of cyber security risks to the bulk power system are not known, and new risks will continue to arise. I believe we should not allow the Nation's bulk power system to be vulnerable to a known national security threat while waiting months or years for a reliability standard to be developed and submitted to the Commission for review. At the same time, reliance on a voluntary alert issued by NERC similarly does not provide adequate assurance that steps will be taken in sufficient time to address a known vulnerability. Given the national security dimension to the cyber security threat, there may be a need to act quickly to protect the bulk power system, to act in a manner where action is mandatory rather than voluntary,

and to protect certain information from public disclosure. Our legal authority is inadequate for such action.

The Commission has taken, and will continue to take, action to protect the bulk power system from cyber vulnerabilities. We continue to work with national security agencies to understand the nature of the threats facing the bulk power grid. We have established mandatory cyber security standards under the section 215 process and have directed improvements in approved standards over time. We also continue to review the industry response to the NERC advisory on the Aurora threat, and may review the response to any future such advisories. But I do not want to leave you under the impression that these steps adequately protect the bulk power system against cyber attacks.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

Mr. LANGEVIN. Mr. Kelliher, thank you very much for your testimony.

I now recognize Mr. Sergel to summarize his statement for 5 minutes.

STATEMENT OF RICHARD SERGEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC)

Mr. SERGEL. Good afternoon, Mr. Chairman and members of the subcommittee. I am president and chief executive officer of the North American Electric Reliability Corporation, better known as NERC, and appreciate the opportunity to appear here today to regain—to begin to regain your trust in NERC and to discuss the progress being made to increase the cybersecurity of the electric grid and to mitigate identified vulnerabilities; and I am going to focus on the two things that we have done since the last time we were here.

The first is—my testimony will address two major points. First, the cybersecurity standards for the bulk power system, mandatory and enforceable this July, represent a significant improvement in cybersecurity for the electricity industry. Second, NERC has enhanced the process for warning the electric industry of cybersecurity threats and implementing mitigation measures to address identified vulnerabilities.

Now cybersecurity of control systems is an increasing priority for every sector of the U.S. economy. NERC and the electricity sector have recognized and responded to this challenge first through the voluntary standards but now through mandatory critical infrastructure standards. The standards are intended to ensure that the electric industry will devote the necessary resources to securing control systems and related cyber assets. The Commission approved those standards in January 2008.

Now the standards development requires progressive and continuous improvement. You have mentioned that in your statement, and the improvement of those standards already is under way through NERC's standards development process. In improving the standards, FERC directed NERC to make certain modifications. Those will be made.

FERC also directed us to monitor the development and implementation of the NIST standards; and if provisions of the NIST standards that would better protect the system are identified, they will be addressed in the standards development process. NERC originally planned to review the standards in 2009 but has ad-

vanced this review to address the changes directed by the Commission.

Now while our protections for the grid are stronger with the standards in place, those standards cannot eliminate the threat of a cyber disruption. Vigilance is required. More is required.

NERC serves as the Electricity Sector Information Sharing and Analysis Center, ES–ISAC, which is responsible for promptly analyzing and disseminating threat indications, analyses and warnings to assist the electric industry; and, as the subcommittee is aware, the ES–ISAC issued an advisory on June 21, 2007, in relation to the vulnerability identified in the demonstration test. Now, since that advisory was issued, important improvements have been made in the cybersecurity alert system.

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 or, as was the case with the Aurora demonstration test, from government agencies with specific information about possible threats.

Second, NERC now has developed a contact list for all 1,800 owners, operators, and users of the bulk power system. It did not have that at the time.

Third, coordination with the Commission on these important communications is now a requirement of the rules of procedure.

None of those were in place. They are in place now. We believe we have substantially addressed many of the concerns expressed by the Chair and the committee, and we look forward to addressing the others in the months ahead.

In closing, the mandatory and enforceable standards now in place represent a important milestone to strengthen grid reliability; and NERC has strengthened the existing alert system to advise the industry when a cyber threat is identified.

We look forward to answering your questions. Thank you very much.

[The statement of Mr. Sergel follows:]

PREPARED STATEMENT OF RICHARD SERGEL

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 re-

[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).

sources 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.

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 indus-

[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.

try. FERC certified NERC as the Electric Reliability Organization ("ERO") in its order issued July 20, 2006.[4]

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 United States, 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.
- *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 5 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 3-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.

---

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

[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).

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 percent 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 percent above 2007 levels in 2008.

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 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:

---

[6] *North American Electric Reliability Corp.,* 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.

[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.

> 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 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

[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 Web site at: *http://www.nerc.com/%7Efilez/standards/Project__2008-06__Cyber__Security.html.*

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:

- (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.

---

[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. 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).

"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 1,800 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 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 United States 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 5 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 fol-

lowing 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.

ATTACHMENT 1.—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

[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.

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 percent of the transmission grid had received mitigation measures or such measures were in progress.

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 percent 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 percent consisted of 60 percent completed and 34 percent in progress. The remaining 6 percent 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:

- The survey results were encouraging and positive and major electricity sector entities representing over 75 percent of the geography and ownership of the bulk power system were proactive in this mitigation effort.

[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.

- A significant portion (25 percent to 30 percent) 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 percent (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 percent rate (62/64).
2.1.1	Security	This measure required strengthening the protections to reduce unauthorized remote access. The compliance rate was 98 percent (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 percent (63/64), more of the entities reported this as "in progress" (35) rather than "completed" (28).
2.1.3	Information Protection	Respondents indicated 100 percent (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.

Measure		Response Analysis
3.1	Control Center Authentication	Fifty-five 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	Forty-seven 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	.....

Mr. LANGEVIN. I thank you for your testimony.

I will now recognize Mr. Wilshusen to summarize his statement for 5 minutes.

Welcome, Mr. Wilshusen.

STATEMENT OF GREG WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE (GAO), ACCOMPANIED BY NABA BARKAKATI, SENIOR LEVEL TECHNOLOGIST, GAO

Mr. WILSHUSEN. Thank you. Mr. Chairman and members of the subcommittee, thank you for the opportunity to participate in today's hearing to discuss control systems security.

I am accompanied today by Naba Barkakati, GAO's acting technologist.

As you know, we have previously reported and testified before this subcommittee that critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities and the serious potential impact of attacks, as demonstrated by several reported incidents. If control systems are not adequately secured, their vulnerabilities could be exploited and our critical infrastructures could be disrupted or disabled, possibly resulting in loss of life, physical damage or economic losses.

Mr. Chairman, at your request, GAO examined the information security controls for the control systems and networks used to operate TVA's critical infrastructure. In reports being issued today on the results of our examination, we determined that TVA had not fully implemented appropriate security controls to properly protect its networks and control systems.

On TVA's corporate network, for example, many of the work stations and servers that we examined lacked key security patches or were insecurely configured. In addition, certain network protocols and devices provided limited protections; and TVA's ability to monitor its network using its intrusion detection system was limited. On certain control systems and networks, passwords or other equivalent documented controls were not effectively implemented, user activity was not logged, software patches were not current, and viruses protection software was not consistently implemented.

The interconnectivity between the corporate network and control systems networks at certain facilities provided opportunities for weaknesses on one network to potentially affect systems on other networks. Physical security weaknesses also introduced risk to control systems at certain facilities. For example, live network jacks connected to TVA's internal network were publicly accessible.

An underlying reason for these weaknesses is that TVA had not fully implemented its information security program. Although TVA had implemented program activities related to contingency planning and incident response, it had not consistently conducted key activities related to, among other things, developing an inventory of systems, assessing risks, completing appropriate training for individuals with significant security responsibilities, testing and monitoring the effectiveness of security controls and identifying and tracking remedial actions to mitigate known uncontrolled weaknesses. As a result, systems and networks that operate TVA's critical infrastructures were at increased risk of unauthorized modification or disruption by both internal and external threats.

Accordingly, opportunities exist for TVA to enhance the security of its control systems networks. In reports being issued today, we are making a total of 92 recommendations to strengthen security controls and implement an effective information security program

that can provide TVA with a solid foundation for ensuring sufficient protection of its control systems. TVA has concurred with most of our recommendations.

In summary, TVA's power generation and transmission critical infrastructures are important to the economy of the southeastern United States and the safety, security and welfare of millions of people. However, multiple weaknesses in both the agency's corporate network and control systems networks place these infrastructures at increased risk. If TVA does not take sufficient steps to secure its control systems and fully implement its security program, it risks not being able to prevent or respond properly to a disruption caused by either malicious or unintended cyber incident.

Mr. Chairman, this concludes our statement. We would be happy to answer questions at this time.

[The statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

MAY 21, 2008

INFORMATION SECURITY: TVA NEEDS TO ENHANCE SECURITY OF CRITICAL INFRASTRUCTURE CONTROL SYSTEMS AND NETWORKS

GAO HIGHLIGHTS: HIGHLIGHTS OF GAO–08–775T, A TESTIMONY BEFORE THE SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY, COMMITTEE ON HOMELAND SECURITY, HOUSE OF REPRESENTATIVES

Why GAO Did This Study

The control systems that regulate the Nation's critical infrastructures face risks of cyber threats, system vulnerabilities, and potential attacks. Securing these systems is therefore vital to ensuring national security, economic well-being, and public health and safety. While most critical infrastructures are privately owned, the Tennessee Valley Authority (TVA), a Federal corporation and the Nation's largest public power company, provides power and other services to a large swath of the American Southeast.

GAO was asked to testify on its public report being released today on the security controls in place over TVA's critical infrastructure control systems. In doing this work, GAO examined the security practices in place at TVA facilities; analyzed the agency's information security policies, plans, and procedures in light of Federal law and guidance; and interviewed agency officials responsible for overseeing TVA's control systems and their security.

What GAO Recommends

In public and limited distribution reports being issued today, GAO is recommending that TVA take steps to improve implementation of the agency's information security program and to correct specific security weaknesses identified at TVA facilities.

In comments on drafts of GAO's reports, TVA provided information on steps it is taking to implement these recommendations.

What GAO Found

TVA had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures at facilities GAO reviewed. Multiple weaknesses within the TVA corporate network left it vulnerable to potential compromise of the confidentiality, integrity, and availability of network devices and the information transmitted by the network. For example, almost all of the workstations and servers that GAO examined on the corporate network lacked key security patches or had inadequate security settings. Furthermore, TVA did not adequately secure its control system networks and devices on these networks, leaving the control systems vulnerable to disruption by unauthorized individuals. Network interconnections provided opportunities for weaknesses on one network to potentially affect systems on other networks. For example, weaknesses in the separation of network segments could allow an individual who gained access to a computing device connected to a less secure portion of the network to compromise systems in a more secure portion of the network, such as the control systems. In addition, phys-

ical security at multiple locations that GAO reviewed did not sufficiently protect the control systems. For example, live network jacks connected to TVA's internal network at certain facilities GAO reviewed had not been adequately secured from unauthorized access. As a result, TVA's control systems were at increased risk of unauthorized modification or disruption by both internal and external threats.

An underlying reason for these weaknesses was that TVA had not consistently implemented significant elements of its information security program. For example, the agency lacked a complete and accurate inventory of its control systems and had not categorized all of its control systems according to risk, limiting assurance that these systems are adequately protected. In addition, TVA's patch management process lacked a mechanism to effectively prioritize vulnerabilities. As a result, patches that were identified as critical, meaning they should be applied immediately to vulnerable systems, were not applied in a timely manner.

Numerous opportunities exist for TVA to improve the security of its control systems. For example, TVA can strengthen logical access controls, improve physical security, and fully implement its information security program. If TVA does not take sufficient steps to secure its control systems and fully implement an information security program, it risks not being able to respond properly to a major disruption that is the result of an intended or unintended cyber incident.

Mr. Chairman and Members of the subcommittee, thank you for the opportunity to participate in today's hearing to discuss control systems security. We have previously reported and testified before this subcommittee that critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents.[1] If control systems are not adequately secured, their vulnerabilities could be exploited, and our critical infrastructures could be disrupted or disabled, possibly resulting in loss of life, physical damage, or economic losses.

The majority of our Nation's critical infrastructures are owned by the private sector; however, the Federal Government owns and operates critical infrastructure facilities including ones used for energy, water treatment and distribution, and transportation. One such entity, the Tennessee Valley Authority (TVA)—a Federal corporation and the Nation's largest public power company—generates electricity using its 52 fossil, hydro, and nuclear facilities, all of which use control systems. As a wholly owned government corporation, TVA is to comply with the Federal Information Security Management Act of 2002[2] (FISMA) by developing a risk-based information security program and implementing appropriate information security controls for its computer systems.

In our testimony today, we will summarize the results of our review of the security controls over TVA's critical infrastructure control systems. We are issuing two reports today, one publicly available and one with limited distribution, which provide additional details on the results of our review.[3] Our objective was to determine whether TVA has effectively implemented appropriate information security practices for its control systems. In preparing for this testimony, we relied on our work supporting these reports, which discuss the details of our scope and methodology. The information in this testimony is specifically based on our public report, which has been reviewed for sensitivity by TVA.

Our testimony is based on the work done for our reports from March 2007 to May 2008. The work on which this testimony is based was conducted in accordance with generally accepted government auditing standards, which require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS IN BRIEF

TVA had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures at facilities we reviewed. Specifically, network interconnections provided opportunities for weaknesses on one network to potentially affect systems on other networks. For example, weaknesses

[1] GAO, *Critical Infrastructure Protection: Federal Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO–07–1036 (Washington, D.C.: September 2007) and GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain.* GAO–08–119T (Washington, D.C.: October 2007).

[2] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107–347 (Dec.17, 2002).

[3] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks,* GAO–08–459SU and GAO–08–526 (Washington, D.C.: May 2008).

in the separation of network segments could allow an individual who gained access to a computing device connected to a less secure portion of the network to compromise systems in a more secure portion of the network, such as the control systems. In addition, physical security at multiple locations that we reviewed did not sufficiently protect the control systems. As a result, TVA's control systems were at increased risk of unauthorized modification or disruption by both internal and external threats.

An underlying reason for these weaknesses was that TVA had not consistently implemented significant elements of its information security program. For example, the agency lacked a complete and accurate inventory of its control systems and it had not categorized all of its control systems according to risk, limiting assurance that these systems were adequately protected. In addition, TVA's patch management process lacked a mechanism to effectively prioritize vulnerabilities. Until TVA fully and consistently implements its information security program, it risks a disruption of its operations, which could impact both TVA and its customers.

In the reports being issued today,[4] we are making 19 recommendations to the Chief Executive Officer of TVA to improve the implementation of its agencywide information security program and 73 recommendations to correct specific information security weaknesses.

In its comments on our reports, TVA concurred with all of our recommendations regarding its information security program and the majority of our recommendations regarding specific information security weaknesses and provided information on steps the agency was taking to implement our GAO recommendations.

BACKGROUND

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. Of particular importance is the security of information and systems supporting critical infrastructures—physical or virtual systems and assets so vital to the Nation that their incapacitation or destruction would have a debilitating impact on national and economic security and on public health and safety. Although the majority of our Nation's critical infrastructures are owned by the private sector, the Federal Government owns and operates key facilities that use control systems, including oil, gas, water, electricity, and nuclear facilities. In the electric power industry, control systems can be used to manage and control the generation, transmission, and distribution of electric power. For example, control systems can open and close circuit breakers and set thresholds for preventive shutdowns.

Critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the potential impact of attacks as demonstrated by reported incidents.[5] Control systems are more vulnerable to cyber threats and unintended incidents now than in the past for several reasons, including their increasing standardization and connectivity to other systems and the Internet. For example, in August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant operated by TVA failed, forcing the unit to be shut down manually. The failure of the pumps was traced to an unintended incident involving excessive traffic on the control system's network.

To address this increasing threat to control systems governing critical infrastructures, both Federal and private organizations have begun efforts to develop requirements, guidance, and best practices for securing those systems. For example, FISMA outlines a comprehensive risk-based approach to securing Federal information systems, which include control systems. Federal organizations, including the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), and the Nuclear Regulatory Commission (NRC), have used a risk-based approach to develop guidance and standards to secure control systems. NIST guidance has been developed that currently applies to Federal agencies; however, much of the guidance and standards developed by FERC and NRC has not yet been finalized. Once implemented, FERC and NRC standards will apply to both public and private organizations that operate covered critical infrastructures.

TVA Provides Power to the Southeastern United States

The TVA is a Federal corporation and the Nation's largest public power company. TVA's power service area includes almost all of Tennessee and parts of Mississippi, Kentucky, Alabama, Georgia, North Carolina, and Virginia. It operates 11 coal-fired fossil plants, 8 combustion turbine plants, 3 nuclear plants, and a hydroelectric sys-

[4] GAO–08–526 and GAO–08–459SU.

[5] See GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,* GAO–07–1036 (Washington, D.C.: Sept. 10, 2007).

tem that includes 29 hydroelectric dams and one pumped storage facility.[6] TVA also owns and operates one of the largest transmission systems in North America.

Control systems are essential to TVA's operation because it uses them to both generate and deliver power. To generate power, control systems are used within power plants to open and close valves, control equipment, monitor sensors, and ensure the safe and efficient operation of a generating unit. Many control systems networks connect with other agency networks to transmit system status information. To deliver power, TVA monitors the status of its own and surrounding transmission facilities from two operations centers.

TVA HAD NOT FULLY IMPLEMENTED APPROPRIATE CONTROLS TO PROTECT CONTROL SYSTEMS FROM UNAUTHORIZED ACCESS

TVA had not fully implemented appropriate security practices to secure the networks on which its control systems rely. Specifically, the interconnected corporate and control systems networks at certain facilities that we reviewed did not have sufficient information security safeguards in place to adequately protect control systems. In addition, TVA did not always implement controls adequate to restrict physical access to control system areas and to protect these systems—and their operators—from fire damage or other hazards. As a result TVA, control systems were at increased risk of unauthorized modification or disruption by both internal and external threats.

Weaknesses in TVA's Corporate Network Controls Placed Network Devices at Risk

Multiple weaknesses within the TVA corporate network left it vulnerable to potential compromise of the confidentiality, integrity, and availability of network devices and the information transmitted by the network. For example:

- Almost all of the workstations and servers that we examined on the corporate network lacked key security patches or had inadequate security settings.
- TVA had not effectively configured host firewall controls on laptop computers we reviewed, and one remote access system that we reviewed had not been securely configured.
- Network services had been configured across lower- and higher-security network segments, which could allow a malicious user to gain access to sensitive systems or modify or disrupt network traffic.
- TVA's ability to use its intrusion detection system[7] to effectively monitor its network was limited.

Weaknesses in TVA Control Systems Networks Jeopardized the Security of its Control Systems

The access controls implemented by TVA did not adequately secure its control systems networks and devices, leaving the control systems vulnerable to disruption by unauthorized individuals. For example:

- TVA had implemented firewalls to segment control systems networks from the corporate network. However, the configuration of certain firewalls limited their effectiveness.
- The agency did not have effective passwords or other equivalent documented controls to restrict access to the control systems we reviewed. According to agency officials, passwords were not always technologically possible to implement, but in the cases we reviewed there were no documented compensating controls.
- TVA had not installed current versions of patches for key applications on computers on control systems networks. In addition, the agencywide policy for patch management did not apply to individual plant-level control systems.
- Although TVA had implemented antivirus software on its transmission control systems network, it had not consistently implemented antivirus software on other control systems we reviewed.

Physical Security Did Not Sufficiently Protect Sensitive Control Systems

TVA had not consistently implemented physical security controls at several facilities that we reviewed. For example:

---

[6] A pumped-storage plant uses two reservoirs, with one located at a much higher elevation than the other. During periods of low demand for electricity, such as nights and weekends, energy is stored by reversing the turbines and pumping water from the lower to the upper reservoir. The stored water can later be released to turn the turbines and generate electricity as it flows back into the lower reservoir.

[7] An intrusion detection system detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, availability, or integrity of a protected network and its computer systems.

- Live network jacks connected to TVA's internal network at certain facilities we reviewed had not been adequately secured from unauthorized access.
- At one facility, sufficient emergency lighting was not available, a server room had no smoke detectors, and a control room contained a kitchen (a potential fire and water hazard).
- The agency had not always ensured that access to sensitive computing and industrial control systems resources had been granted to only those who needed it to perform their jobs. At one facility, about 75 percent of facility badgeholders had access to a plant computer room, although the vast majority of these individuals did not need access. Officials stated that all of those with access had been through the required background investigation and training process. Nevertheless, an underlying principle for secure computer systems and data is that users should be granted only those access rights and permissions needed to perform their official duties.

INFORMATION SECURITY MANAGEMENT PROGRAM WAS NOT CONSISTENTLY IMPLEMENTED ACROSS TVA'S CRITICAL INFRASTRUCTURE

An underlying reason for TVA's information security control weaknesses was that it had not consistently implemented significant elements of its information security program, such as: documenting a complete inventory of systems; assessing risk of all systems identified; developing, documenting, and implementing information security policies and procedures; and documenting plans for security of control systems as well as for remedial actions to mitigate known vulnerabilities. As a result of not fully developing and implementing these elements of its information security program, TVA had limited assurance that its control systems were adequately protected from disruption or compromise from intentional attack or unintentional incident.

TVA's Inventory of Systems Did Not Include Many Control Systems

TVA's inventory of systems did not include all of its control systems as required by agency policy. In its fiscal year 2007 FISMA submission, TVA included the transmission and the hydro automation control systems in its inventory. However, the plant control systems at its nuclear and fossil facilities had not been included in the inventory. At the conclusion of our review, agency officials stated they planned to develop a more complete and accurate system inventory by September 2008.

TVA Had Not Assessed Risks to Its Control Systems

TVA had not completed categorizing risk levels or assessing the risks to its control systems. FISMA mandates that agencies assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure disruption, modification, or destruction of their information and information systems. However, while the agency had categorized the transmission and hydro automation control systems as high-impact systems,[8] its nuclear division and fossil business unit, which includes its coal and combustion turbine facilities, had not assigned risk levels to its control systems. TVA had also not completed risk assessments for the control systems at its hydroelectric, nuclear, coal, and combustion turbine facilities. According to TVA officials, the agency plans to complete the hydroelectric and nuclear control systems risk assessments by June 2008 and they plan to complete the security categorization of remaining control systems throughout TVA by September 2008, except for fossil systems, for which no date has been set.

Inconsistent Application of TVA's Policies and Procedures Contributed to Program Weaknesses

Several shortfalls in the development, documentation, and implementation of TVA's information security policies contributed to many of the inadequacies in TVA's security practices. For example:

- TVA had not consistently applied agencywide information security policies to its control systems, and TVA business unit security policies were not always consistent with agencywide information security policies.
- Cyber security responsibilities for interfaces between TVA's transmission control system and its hydroelectric and fossil generation units had not been documented.
- Physical security standards for control system sites had not been finalized or were in draft form.

[8] Federal Information Processing Standard 199 provides criteria for categorizing risk to systems as high, moderate, or low.

Patch Management Weaknesses Left TVA's Control Systems Vulnerable

Weaknesses in TVA's patch management process hampered the efforts of TVA personnel to identify, prioritize, and install critical software security patches to TVA systems in a timely manner. For a 15-month period, TVA documented its analysis of 351 reported vulnerabilities, while NIST's National Vulnerability Data base[9] reported about 2,000 vulnerabilities rated as high or medium risk for the types of systems in operation at TVA for the same time period. In addition, upon release of a patch by the software vendor, the agency had difficulty in determining the patch's applicability to the software applications in use at the agency because it did not have a mechanism in place to provide timely access to software version and configuration information for the applications. Furthermore, TVA's written guidance on patch management provided only limited guidance on how to prioritize vulnerabilities. The guidance did not refer to the criticality of IT resources or specify situations in which it was acceptable to upgrade or downgrade a vulnerability's priority from that given by its vendors or third-party patch tracking services. For example, agency staff had reduced the priority of three vulnerabilities identified as critical or important by the vendor or a patch tracking service and did not provide sufficient documentation of the basis for this decision. As a result, patches that were identified as critical were not applied in a timely manner; in some cases, a patch was applied more than 6 months past TVA deadlines for installation.

TVA Had Not Developed System Security and Remedial Action Plans for All Control Systems

TVA had not developed system security or remedial action plans for all control systems as required under Federal law and guidance. Security plans document the system environment and the security controls selected by the agency to adequately protect the system. Remedial action plans document and track activities to implement missing controls such as missing system security plans and other corrective actions necessary to mitigate vulnerabilities in the system. Although TVA had developed system security and remedial action plans for its transmission control system, it had not done so for control systems at the hydroelectric, nuclear, or fossil facilities. According to agency officials, TVA plans to develop a system security plan for its hydroelectric automation and nuclear control systems by June 2008, but no timeframe has been set to complete development of a security plan for control systems at fossil facilities. Until the agency documents security plans and implements a remediation process for all control systems, it will not have assurance that the proper controls will be applied to secure control systems or that known vulnerabilities will be properly mitigated.

OPPORTUNITIES EXIST TO IMPROVE SECURITY OF TVA'S CONTROL SYSTEMS

Numerous opportunities exist for TVA to improve the security of its control systems. Specifically, strengthening logical access controls over agency networks can better protect the confidentiality, integrity, and availability of control systems from compromise by unauthorized individuals. In addition, fortifying physical access controls at its facilities can limit entry to TVA restricted areas to only authorized personnel, and enhancing environmental safeguards can mitigate losses due to fire or other hazards. Further, establishing an effective information security program can provide TVA with a solid foundation for ensuring the adequate protection of its control systems.

Because of the interconnectivity between TVA's corporate network and certain control systems networks, we recommend that TVA implement effective patch management practices, securely configure its remote access system, and appropriately segregate specific network services. We also recommend that the agency take steps to improve the security of its control systems networks, such as implementing strong passwords or equivalent authentication mechanisms, implementing antivirus software, restricting firewall configuration settings, and implementing equivalent compensating controls when such steps cannot be taken.

To prevent unauthorized physical access to restricted areas surrounding TVA's control systems, we recommend that the agency take steps to toughen barriers at points of entry to these facilities. In addition, to protect TVA's control systems operators and equipment from fire damage or other hazards, we also recommend that the agency improve environmental controls by enhancing fire suppression capabilities and physically separating cooking areas from system equipment areas.

[9] The National Vulnerability Data base is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.

Finally, to improve the ability of TVA's information security program to effectively secure its control systems, we are recommending that the agency improve its configuration management process and enhance its patch management policy. We also recommend that TVA complete a comprehensive system inventory that identifies all control systems, perform risk assessments and security risk categorization of these systems, and document system security and remedial action plans for these systems. Further, we recommend improvements to agency information security policies.

In commenting on drafts of our reports, TVA concurred with all of our recommendations regarding its information security program and the majority of our recommendations regarding specific information security weaknesses. The agency agreed on the importance of protecting critical infrastructures and stated that it has taken several actions to strengthen information security for control systems, such as centralizing responsibility for cyber security within the agency. It also provided information on steps the agency was taking to implement certain GAO recommendations.

In summary, TVA's power generation and transmission critical infrastructures are important to the economy of the southeastern United States and the safety, security, and welfare of millions of people. Control systems are essential to the operation of these infrastructures; however, multiple information security weaknesses exist in both the agency's corporate network and individual control systems networks and devices. An underlying cause for these weaknesses is that the agency had not consistently implemented its information security program throughout the agency. If TVA does not take sufficient steps to secure its control systems and implement an information security program, it risks not being able to respond properly to a major disruption that is the result of an intended or unintended cyber incident.

Mr. Chairman, this concludes our statement. We would be happy to answer questions at this time.

Mr. LANGEVIN. Thank you, Mr. Wilshusen.

The Chair now recognizes Mr. McCollum to summarize your statement for 5 minutes. Welcome.

STATEMENT OF WILLIAM R. McCOLLUM, JR., CHIEF OPERATING OFFICER, TENNESSEE VALLEY AUTHORITY (TVA), ACCOMPANIED BY JOHN LONG, CHIEF ADMINISTRATIVE OFFICER, TVA

Mr. MCCOLLUM. Good afternoon, Chairman Langevin, Ranking Member Ms. Brown-Waite and members of the subcommittee.

I am Bill McCollum, Chief Operating Officer of the Tennessee Valley Authority. I am accompanied today by TVA's Chief Administrative Officer, John Long.

I appreciate this opportunity to appear before you to discuss the Government Accountability Office report on the security of the computer networks and control system used in TVA's operations.

As TVA's Chief Operating Officer, I am responsible for the safe and reliable operation of the TVA power system which generates and distributes electricity for a region of the southeast which covers the State of Tennessee and adjacent parts of six neighboring States. All of our operations are financed by revenues from the sale of electricity. TVA does not receive any annual congressional appropriations.

I am also pleased to note that earlier this week we observed the 75th anniversary of the TVA. As we have for 75 years, we remain focused on carrying out our three-part mission in energy, economic development and environmental stewardship. Each part of this mission has contributed significantly to the progress of our 80,000-square-mile service region.

In performing our mission, the safety of our employees and the public is paramount in all of our operations, including specialized

security requirements to protect the computerized control systems involved in the generation and transmission of electricity.

On behalf of TVA, we appreciate the substantial time and resources that the GAO allotted to examining and evaluating our computer security. As you know, the report made public today listed 19 recommendations for improving the security of our computer systems. We concur with all of these recommendations, and we have either completed or are aggressively moving to implement remedial actions for all 19.

It is important to note that TVA was already in the process of addressing 17 of the 19 recommendation areas when GAO's field work began at TVA last October. We also initiated several actions to address other aspects of our security while the field team was conducting its evaluation. These actions were the result of ongoing assessments by TVA staff and the independent TVA office of the Inspector General, which had initiated planning for an audit of our information technology security by Science Applications International Corporation. GAO's work has been very helpful in affirming and focusing the need for these and other measures that we are taking.

Some of the security issues identified by the GAO report involved instances that have been addressed by the centralization of our cybersecurity policy, its administration and its oversight activities into a corporate-level organization. The centralization of this responsibility was completed in February, which now gives TVA a uniform security set of procedures to be followed by all its organizations and covers all control systems.

In conjunction with our implementation of additional measures to strengthen our defense-in-depth security posture, we commissioned a third-party consultant to perform penetration testing of our infrastructure to identify any immediate weaknesses. Testing involved both informed and uninformed circumstances in which the third party made attempts to penetrate our networks. We are pleased to note that the consultant's team was unable to gain access to any of the targeted process control networks in either type of test. While the test failed to penetrate our control network security, the process identified several opportunities to further insulate and protect our security systems. We are now implementing those additional measures.

In closing, the TVA fully understands that it has a solemn responsibility to ensure the safety and security of the systems that are vital to our Nation's critical infrastructure, our region and the Nation's economy and the health and safety of the public. One of my responsibilities is ensuring that we embrace safety as a value in all aspects of our operations to protect the health and well-being of our work force and the public. We are moving as quickly as possible to complete remedial measures for all 19 of the GAO's recommendations, along with other steps that have been identified to elevate every level of our security and computer network security.

As a Federal entity, we are cognizant of our special responsibility to provide leadership in this important aspect of our electric system operations. We assure the subcommittee and the public at large that TVA is committed to ensuring that the infrastructure en-

trusted to our responsibility meets or exceeds the best accepted practices in government and in the electric utility industry.

Thank you for this opportunity to provide our perspectives and experiences as you continue this subcommittee's important work in assessing the adequacy of security measures within the Nation's critical electric power infrastructure.

[The statement of Mr. McCollum follows:]

PREPARED STATEMENT OF WILLIAM R. MCCOLLUM, JR.

MAY 21, 2008

Good afternoon Chairman Langevin, Ranking Member McCaul, and Members of the subcommittee. I am Bill McCollum, Chief Operating Officer of the Tennessee Valley Authority (TVA). I am accompanied today by TVA's Chief Administrative Officer, John Long.

I appreciate this opportunity to appear before you to discuss the Government Accountability Office (GAO) report on the security of the computer networks and control systems used in TVA's operations.

As TVA's Chief Operating Officer, I am responsible for the safe and reliable operation of the TVA power system, which generates and distributes electricity for a region of the Southeast which covers Tennessee and adjacent parts of six neighboring States. All of our operations—the generation and distribution of electricity and our stewardship of the Nation's fifth largest river system and economic development work—are financed by revenue from the sale of electricity. TVA does not receive any annual congressional appropriations.

I am pleased to note that earlier this week we observed the 75th Anniversary of TVA in Muscle Shoals, Alabama. As we have for 75 years, we remain focused carrying out our historic three-part mission in energy, economic development and environmental stewardship. Each part of our mission has contributed significantly to the progress of our 80,000-square-mile service region, which is centered on the watershed of the Tennessee River.

In performing our mission, the safety of our employees and the public is paramount in all of our operations, including the specialized security requirements to protect the computerized control systems involved in the generation and transmission of electricity.

On behalf of TVA, we appreciate the substantial time and resources that the GAO allotted to examining and evaluating our computer security. As you know, the report made public today by the GAO listed 19 recommendations for improving the security of our computer systems. We concur with all of those recommendations, and we have either completed or are aggressively moving to implement remedial actions for all 19.

It is important to note that TVA was already in the process of addressing 17 of the 19 recommendation areas when GAO's field work began at TVA last October. We also initiated several actions to address other aspects of our security while the field team was conducting its evaluation. These actions were the result of on-going assessments by TVA staff and the independent TVA Office of Inspector General, which had initiated planning for an audit of our Information Technology Security by Science Applications International Corporation. GAO's work has been very helpful in affirming and focusing the need for these and other measures that we are taking.

Some of the security issues identified by the GAO report involved instances that have been addressed by the centralization of our cyber security policy, its administration and its oversight activities into a corporate-level organization. The centralization of this responsibility was completed in February, which now gives TVA uniform security procedures to be followed by all of its organizations and covers all control systems.

In conjunction with our implementation of additional measures to strengthen our defense-in-depth security posture, we commissioned a third-party consultant to perform penetration testing of our infrastructure to identify any immediate weaknesses. The testing involved both "informed" and "uninformed" circumstances in which this third party made attempts to penetrate our networks. We are pleased to note that the consultant's team was unable to gain access to any of the targeted Process Control Networks in either type of test. While the tests failed to penetrate our control network security, the process identified several opportunities to further

insulate and protect the security of our systems. We are now implementing those additional measures.

In closing, TVA fully understands that it has a solemn responsibility to ensure the safety and security of systems that are vital to the Nation's critical infrastructure, our region and Nation's economy, and the health and safety of the public. As the Chief Operating Officer, one of my responsibilities is ensuring that we embrace safety as a value in all aspects of our operations to protect the health and well-being of our work force and the public. We are moving as quickly as possible to complete remedial measures for all 19 of GAO's recommendations, along with other steps we have identified, to elevate every level of our computer and network security.

As a Federal entity, we are cognizant of our special responsibility to provide leadership in this important aspect of electric system operations. We assure the subcommittee and the public at-large that TVA is committed to assuring that the infrastructure entrusted to our responsibility meets or exceeds the best accepted practices in government and in the electric utility industry.

Thank you for this opportunity to provide our perspectives and experiences as you continue the subcommittee's important work in assessing the adequacy of security measures within the Nation's critical electric power infrastructure.

Mr. LANGEVIN. Thank you, Mr. McCollum.

I want to thank the witnesses for their testimony.

I remind each member that he or she will have 5 minutes to question the panel, and I now recognize myself for questions.

Last October, this committee was told that 75 percent of the transmission grid has either taken appropriate actions or is in the process of implementing those actions for Aurora. In NERC's testimony today, they suggest 94 percent of the short midrange mitigation measures have been completed or in progress. Yet, on the other hand, Chairman Kelliher is telling us in testimony that there is a broad range—there is a broad range of compliance based only on individual interpretations of the threat and the application of the recommended mitigation measures.

My question for the panel is, who is right? What are we—what do these varying assessments tell us about the industry's readiness or ability to comply with the reliability standards?

Mr. KELLIHER. I think both answers might be true and that we are actually asking different questions. So we are coming to somewhat different answers. We are conducting a subjective review of some of the utility plans in response to the advisory, whereas NERC is really asking a different question. So I think, actually, both can be true at the same time.

Mr. SERGEL. Chairman, there are three different sources for that information. The first would have been done immediately after our advisory last year. It involved going out and doing interviews and gathering information with respect to the status. We did that at that time because we did not have in place a data base to get the entirety of the users and owners and operators, and I know that was some source of confusion. For that we apologize. The responsibility, to be clear, is ours and ours entirely; and we will do better the next time.

The second data that you refer to, the 94 percent, is from a written survey that we sent out. It is the data that came back from it. But I will tell you that we recognized and the Commission recognized and took action that that type of survey was limited, and we provided it to you with that knowledge.

I think the third that has been done and is ongoing is being done by the Commission. It is both the most recent, it is the most com-

prehensive, and it is the one that is the best information at this point in time.

Mr. LANGEVIN. I am surely troubled by the last time that NERC appeared before us; and, you know, at best, the answers that were given were confusing. At worst, it was highly misleading. I am glad to hear that you have worked to clarify some of that today, but I hope never to hear that kind of testimony or lead us to be misled ever in the future.

I mentioned in my opening statement that I have real doubts about NERC's ability to regulate these new reliability standards. From where I sit, I would say that NERC seems either not to take their authority as the electric reliability office seriously—for instance, NERC was responsible for following up with industry to see how they implemented the Aurora mitigation, but, according to FERC, the NERC survey was much too limited in scope to make a real determination about how far the industry had come in mitigating the Aurora vulnerability. It is hard to understand why the regulatory body responsible for the security and the safety of the bulk power system would take such a laissez faire approach to this critical issue.

Chairman Kelliher, based on your findings, do you think that NERC will, in fact, be able to carry out its duty as the ERO and how are you working with them to fix the shortcomings?

Mr. Sergel, given this first halfhearted effort to oversee the industry, how does your organization plan on fulfilling its enforcement authority role and what specific lessons have you learned and what structures are in place to address my concerns?

Chairman Kelliher, please.

Mr. KELLIHER. I think NERC is doing a job under a law that is very imperfect, particularly with regard to this kind of threat. As I already said, there are two means to address to defend the grid against cyber attacks. The only quick means is an advisory. It is purely voluntary. I think a voluntary by its nature is always going to produce inconsistent results.

That is what led Congress to legislate on reliability 2½ years ago. The industry historically has relied on voluntary compliance with unenforceable standards. Congress ultimately concluded—correctly, in my judgment—that that was fundamentally flawed, that you needed to have mandatory standards.

Now, we can develop mandatory standards on cybersecurity, but it takes time. It can take years. That is the dilemma that we have right now. We have a threat just by whose nature requires quick action and mandatory action, mandatory compliance with that action. We actually have to choose one or the other right now. We can choose quick action, where compliance is purely voluntary, or we can go down the path of mandatory standards that can take years.

I think NERC realized there was a need for quick action in response to Aurora and took the only course that it had available, an advisory. The results haven't been consistent, but I actually think that is predictable and perhaps unavoidable.

Mr. SERGEL. Mr. Chairman, again, the responsibility for being clear is entirely ours, and our failure to do that is noted, and we intend to do better going forward.

With respect to lessons learned, talk about two things. The first is that we have put in a formal system of advising the industry. That system has been approved by the Commission. It comes in levels. We have—the first level is simply an advisory. Then we have a second level, which is a recommendation; and the third is an essential action. Each of those we notify the Commission in advance and coordinate with them before we issue it. We would coordinate with any other appropriate government agency if it was on a topic relative to them.

We now have in place the list of 1,800 users, owners and operators to communicate with. They understand the system. They have been notified in advance. They understand what an advisory is and a recommendation. We didn't have that before. So we are in a much better position going forward to communicate better and be more effective within the limited authority that we have. It is limited.

Then, with respect to enforcement of these standards, we now have a standard. We will enforce it. We have been very active in the last few months. We have put out a guidance on what it means, the fact that it is effective beginning in July for those for whom the voluntary standards were in place, and they understood those. We will enforce the standard up to the parameters included in the law.

Mr. LANGEVIN. In our last hearing, we discussed the standards problem. NIST standards which apply to Federal entities are much more robust than the NERC standards which apply to private entities. Unfortunately, publicly and privately owned infrastructure on the grid are so interconnected weak security controls in one utility can pose a harm to another utility that shares a connection.

My question is, Mr. McCollum, you are required to implement NIST, yet you are connected to folks who implement NERC; and are you concerned that a weakness on a NERC-compliant infrastructure can affect your network?

Mr. MCCOLLUM. We are moving aggressively to be in compliance and remain in compliance or exceed the requirements of all of those standards in terms of the security of our critical infrastructure and networks. This is going to be an increasing challenge going forward. As you noted in your opening testimony, the deployment of technology has resulted in increased interconnectivity; and we are moving aggressively to stay ahead of this issue and skate to where the puck is going to be in the future in terms of implementing sufficient controls.

I believe that through a defense-in-depth posture and compliance with all of these controls and protocols which meet or exceed these standards, we will provide adequate protection for all of the critical infrastructure.

Mr. LANGEVIN. Finally, Mr. Sergel, could you please tell us what steps are being taken to transition the NERC reliability standards toward NIST and why should the scope of CIP–002 be changed to include all equipment that is electronically connected?

Mr. SERGEL. Let me deal with the second part of that first, which is that standard two requires that the users, owners and operators identify the critical assets that they have on the system and then those become the ones that are then accountable to the remaining standards.

The identification of critical assets is a requirement, and I want to begin with that. It is often you hear that, well, that means someone can just not identify any and they are in compliance. Doesn't meet my test of what it means to identify your critical assets. So the identification of critical assets is one in which we expect the list to be inclusive of all those that are, in fact, critical.

So going to the question of, well, why then didn't we just start with all assets, I think the answer to that is there are so many in the industry at this point in time, the challenge is so great, that we believe that the priority is to start with those that are critical, identify those, and move forward. We will continuously evaluate the standard and continuously evaluate whether more is required; and if it is, we will do that. But it is a matter of prioritization.

Mr. LANGEVIN. But specifically to NIST, do you see that as the—do you recognize that, as most of us do, as being the gold standard of standards and are you—tell me about your transition efforts.

Mr. SERGEL. Well, we have a process in place—it has been done already—to review and propose new standards that will incorporate any of the NIST requirements that are appropriate to real-time power system operating systems.

We have been directed to do that by the Commission, and we will do that. We have begun that work. We, in fact, have accelerated it by a year. So what you are looking for is now part of our work plan, but, beyond that, it has been directed to us that we it be done by the Commission.

Mr. LANGEVIN. Thank you, and as far as I am concerned the sooner the better.

With that, at this time I would yield to the ranking member, but he has asked me to yield to the gentlelady from Florida, first, Ms. Ginny Brown-Waite, which I will do at this time, to pose some questions.

Ms. BROWN-WAITE. Thank you very much, Mr. Chairman.

Actually, I am following up on the questions of the chairman.

There was an article in today's Washington Post. Now everyone up here knows and we regularly tell our constituents don't believe everything you read in the paper, but let me just kind of summarize something that should be of concern.

It says, security experts, however, contend that existing NERC standards contain loopholes and don't adequately protect critical power systems. For example, telecommunication equipment is excluded, even though there are documented cases of computer worms shutting off service from control systems to substations.

It goes on to say, you have got a whole bunch of utilities who claim they have no critical cyber assets, which means they don't have to do anything else to secure their current cyber system.

The person also went on to say, we have some very big electric utilities who claim they just have 10 cyber assets, when most companies have more critical relays like that in a single substation.

Mr. Sergel, if you could respond to that, and perhaps Mr. Kelliher.

Mr. SERGEL. That is a specific statement on the issue I just mentioned before, and it is an interpretation of the standard which requires that they identify their critical assets, and it implies that

someone can merely say I don't have any and now they don't have to comply with the standards, all of the other standards.

As of July 1, for the most important parts of that industry and all those that have been subject to the voluntary standards in the past, they will have a requirement to have identified the critical assets. I can assure you if they have critical assets and put down zero that we will begin to evaluate whether they are in compliance with that standard, and their audit would identify that.

So I believe that there is not a weakness in these standards with respect to the notion that the identification of critical assets simply leaves it to them to decide they don't have any. I just disagree with that.

The second issue is that we at NERC by statute are limited to the bulk power system. Now to the extent that those telecommunications providers are part of the protection mechanisms that they are relying on to meet the standards, then we have some reach for those. But I can't understand why someone would say you have not gone far enough. There are telecommunications issues you should direct.

Those are beyond the scope of the law that we have. We are restricted to the users, owners and operators of the bulk power system. We do not have any jurisdiction to require a telecommunications company to make a change, for example, or to set a standard for them.

Ms. BROWN-WAITE. Mr. Kelliher, do you think that telecommunications should be included?

Mr. KELLIHER. The SCADA systems are so interrelated that it is hard to draw a line if you were to—FERC only has the authority that the Congress gave us. We have the authority to oversee reliability of the bulk power system. That is a defined term, and it typically does not extend into the telecom industry.

I do, though, with respect to the issue about critical facilities, I think the industry is doing a faithful job implementing and respecting reliability standards. I don't see widespread noncompliance in that kind of approach. But we don't necessarily accept the representation of a company. If the company were to come in and say we have zero critical facilities, we don't have to accept that representation.

Ms. BROWN-WAITE. I have one more question for Mr. Sergel; and that is, could you share with the committee some examples of when an expedited process has been used in an urgent situation?

Mr. SERGEL. Probably the best example is the original establishment of the cyber standards. Now this is before my time as the CEO, so it is difficult for me to answer that. But the cyber ones were put in under a process of moving, of expediting the schedule.

We have three levels of speed at which we operate. The first is the normal speed, and typically in that category we are operating in an environment in which all of the information is well-known, and it is a significant process of bringing together the technical talent to evaluate the standards so there is no horizons of time. We can expedite it, which means it is important enough that we ought to do it more quickly; and there are rules, procedure that do that. Then we can also establish it in an emergency period of time. So we can speed up the time that we can create a standard.

But what we can't do is we can't speed it up and not have it be a public process; and that is why the chairman is here asking for additional authority, I believe, more fundamentally than the time. Because we can act quickly, but we can't act quickly and confidentially. Everything we do has to be posted in an opportunity for notice and evaluation and comment. We can ask people to do that very quickly, right, but we can't do that quickly and confidentially simultaneously, and therefore I see that as a significant reason why they are asking for additional authority.

Ms. BROWN-WAITE. Thank you very much; and, with that, I yield back the balance of my time.

Mr. LANGEVIN. I thank the gentlelady for her very insightful questions. I think that it raises a lot of questions in my mind and poses some challenges, given the fact of how interrelated SCADA—it really is and how do we, in fact, tie in the regulation of telecom in this area. It is going to pose a challenge for us.

With that, the Chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. Wilshusen, is that correct?

Mr. WILSHUSEN. Yes.

Mr. GREEN. You mentioned a total, I believe, of 92 recommendations that were made to TVA, is that correct?

Mr. WILSHUSEN. That's correct.

Mr. GREEN. And the representative from TVA, I think you responded to 19 of the 92.

Mr. WILSHUSEN. Yes. The difference is because we are issuing two reports to them, one that is publicly available, and that report has 19 recommendations in it. We are also issuing a limited official-use-only report which contains more details and specifics about the individual findings that we identified, and in that report we are making 73 recommendations.

Mr. GREEN. My assumption is that you believe that all 92 of them should be addressed.

Mr. WILSHUSEN. Yes, sir.

Mr. GREEN. Okay, so let me go over to Mr. McCollum. Is that correct, sir?

Mr. MCCOLLUM. That's correct.

Mr. GREEN. Mr. McCollum, if there is something about this that you can't say publicly, I understand, but you addressed only 19 of the 92?

Mr. MCCOLLUM. In my opening statement, I referred to the 19 recommendations in the public report. However, we have responded to and are addressing or have already addressed all of the recommendations in both of those reports that were just referred to.

Mr. GREEN. Could you kindly define "addressed", please? "Addressed" could simply mean that you looked at it and you decided that it was something that you will get around to, or it could mean that you completely corrected the situation. There are 73 recommendations concerning specific information security weaknesses that should be corrected. So how do you address them?

Mr. MCCOLLUM. We have an action plan in place. A number of those recommendation actions have already been closed on those to complete the actions necessary to remediate those recommenda-

tions. We have others in progress that will be complete shortly. By the end of this fiscal year and calendar year, we will have completed a majority of the actions.

Some of the recommendations address items in the standards that relate to longer-term assessments and documentation and other actions that will take a little longer. But we have an action plan in place to address and remediate all of those recommendations on a priority basis, as noted in some of the earlier testimony in responses to questions. It is important that we address those most important——

Mr. GREEN. If I may, let me go back to Mr. Wilshusen.

Sir, have you had an opportunity to see the proposed action plan?

Mr. WILSHUSEN. Not the specific action plans. We have received responses from TVA that they made in response to our report, which is included in our reports. But as a matter of GAO policies and, of course, the government auditing standards we will go back later to verify the corrective actions that TVA has taken or will take on these actions on our recommendations.

Mr. GREEN. Are these actions that should be taken with the next 10 years?

Mr. WILSHUSEN. I would hope so. I think many of them should be taken immediately. As Mr. McCollum indicated some already have been taken and they have been completed actions on some of them already.

Mr. GREEN. Should they all be finished within the next 10 years?

Mr. WILSHUSEN. I would think so, yes.

Mr. GREEN. Should they be finished within the next 5 years? Within the next 3 years?

Mr. WILSHUSEN. Probably so, the recommendations we are making.

Mr. GREEN. Will you, in continuing your audit, provide information as to how the action plan is progressing? Is that information that we can receive?

Mr. WILSHUSEN. We can certainly work with your staff to provide that information, yes.

Mr. GREEN. Those things that should be done immediately, I assume will make them priority No. 1. I assume that they are priority No. 1 for a reason. Are you finding that any of these priority No. 1 items are not being addressed what we will call timely?

Mr. WILSHUSEN. At this point, we have not gone back to verify the actions taken by TVA on our recommendations. So I can't comment as to whether or not the actions have been completed. All we have at this point are assertions by TVA that they have taken action or plan to take actions.

Mr. GREEN. I have about 8 seconds. How long do you think it will take you to verify what has been indicated has been done currently?

Mr. WILSHUSEN. It would not take us too long if we were to go out and conduct our tests.

Mr. GREEN. It is not too long, 2 weeks; or is it 2 months?

Mr. WILSHUSEN. It could be 2 weeks to do the work, but we would not necessarily be able to go out in 2 weeks to do that, given our other workload and activities and commitments that we have.

Mr. GREEN. Thank you.

I yield back, Mr. Chairman.

Mr. LANGEVIN. I thank the gentleman.

The chairman now recognizes the ranking member, the gentleman from Texas, Mr. McCaul, for 5 minutes.

Mr. MCCAUL. I thank the chairman.

This is really kind of a follow-up hearing to the hearing that we had after the story of Aurora broke on national television on CNN. We had had closed briefings on that, and it raised kind of a specter of what could happen if we had a cyber attack on our power grids. It revealed a major vulnerability in this Nation to our security, the idea that the power grid could be shut down by the use of intrusions through computer networks. Of course, everything is tied to computer networks. This raises a broader specter.

I think the Commission that Chairman Langevin and I formed to study this issue hopefully will provide good recommendations for the next administration.

But I have just a couple of questions. One is, in your dealings—and this is directed to Mr. Kelliher and Mr. Sergel. In your dealings with the private sector, how serious do you think they are really taking this threat, which so many of us in Congress believe is a serious threat to the not only economic viability but security of this Nation?

Mr. KELLIHER. I think they are taking it very seriously.

Mr. MCCAUL. Mr. Sergel.

Mr. SERGEL. I believe they are taking it very seriously as well.

I do believe that understanding the complexity of the threat, you described one part of it, which is that somebody could attack the grid itself. I think many of us are increasingly concerned that the attack would come from the grid to a private facility, to a critical facility, which is an entirely different issue. I think for that reason, as we wrestle with the complexity of it, we often find that folks say, well, I have taken care of it, and then learn that they haven't. It is not they aren't working at it hard and taking it seriously, but, rather, it is because, as we dig deeper, we find more. It doesn't make our concern go away. It makes our concern go up.

Mr. MCCAUL. I appreciate that response.

Mr. Sergel, do you believe that you have enough authority to adequately address this issue in the private sector?

Mr. SERGEL. So, at NERC, we are a not-for-profit. We are designated by the Federal Energy Regulatory Commission as the ERO, subject to our application and subject to their continuing jurisdiction. As such, we are limited to the bulk power system. We do not have authority over distribution, so there is a limitation there. We do not have authority over telecommunications. There is a limitation there. The structure of the law and because we are not a government agency suggests that we do everything publicly. We post for comment, and we evaluate it and then take action. So all of those are limitations on what we can do.

What I can assure you is that we have a great challenge in this area, but we will continue to do everything we can within the jurisdiction that we do have, and that includes within the standards. We will push as far as we can to get as much done on the telecommunications side within the standard, and we will push as

hard as we can to get as much of the bulk power system covered and protected.

Mr. MCCAUL. Thank you.

My understanding is you have jurisdiction over the bulk power system, as you said.

With respect to telecom and oil and gas and banking and all of the other sectors in the private sector, that would be within the jurisdiction of the Department of Homeland Security?

Mr. KELLIHER. And other agencies, yes.

Mr. MCCAUL. And other agencies.

What is your relationship with DHS? Do you have a good working relationship with them?

Mr. KELLIHER. Yes, it is a very cooperative relationship, in part because we realize we are not in the best position to assess the nature of a cyber threat, particularly if it is a threat posed by a foreign country or an organized group. That is really the province of the national security or intelligence agency. So we think they are the ones best suited to identify the threat, and we might be the best suited to actually act upon that threat.

Mr. MCCAUL. So they are in the best position to deal with the nature of this type of threat.

Is the coordination positive and productive?

Mr. KELLIHER. Yes, it has been very positive and productive. I am tempted to say "seamless," but there are probably always some seams between government agencies.

Mr. MCCAUL. Mr. Sergel, do you have a response?

Mr. SERGEL. We also have a very positive relationship with both the Department of Homeland Services and the Department of Energy.

Mr. MCCAUL. Okay.

I yield back. Thank you.

Mr. LANGEVIN. I thank the ranking member.

I wanted to clarify something. You know, we are talking about not the entire telecommunications industry; we are talking about telecommunications equipment on the bulk power system. I think that that is an important distinction to be made, and there has got to be a mechanism to allow for some oversight or regulation in that area with respect to FERC and NERC, and we are going to explore those avenues with you. If it requires involvement of other committees and jurisdictions, we will involve them as well.

With that, Ms. Jackson Lee, a member of the full committee, has asked to participate in the hearing. I ask unanimous consent that she be allowed to participate.

Hearing none, Ms. Jackson Lee will be recognized for questions after the members of the subcommittee are recognized.

We welcome you here to the participation, and we appreciate the work that you are doing on your subcommittee with respect to infrastructure protection.

With that, the Chair now recognizes the gentleman from New Jersey for 5 minutes, Mr. Pascrell.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Chairman, this is an issue of compliance. We had the same pushback from the chemical industry when we were deciding in a bipartisan fashion how we can protect the chemical industry and,

hence, protect our families because that is what it comes down to, homeland security. Knowing what the mission of this committee—this subcommittee—is, its having been formed from two previous committees, our mission is pretty clear, Mr. Chairman, as far as I am concerned. We are not the enemy, this committee. The enemy are those who wish to attack America and to put our families in jeopardy.

So, Mr. Sergel, I have some questions to ask of you. I have to clarify something for the record. We are trying to figure out who has mitigated the Aurora vulnerability. We have gone through all of the nomenclature—CIP, NERC, FERC, BPS, ERO. I am frustrated because your organization has provided this committee with so many conflicting and inaccurate statements that I have to question how seriously NERC takes its responsibility as the electric liability organization.

I was here on October 17 last year when your colleague David Whiteley testified before the subcommittee. The Chairman asked Mr. Whiteley to describe the survey that your organization claimed to have sent to the owners and the operators of the grid. Mr. Whiteley stated for the record that approximately 75 percent of the transmission grid either took or was in the process of implementing mitigation. When asked if these were anecdotal numbers, Mr. Whiteley told us that these were hard numbers. After the hearing, we asked you to provide us a copy of the survey.

Mr. Chairman, this is exhibit A, electric sector transmission owner-operators, generation owner-operators.

This is what you submitted on October 19, 2007.

I want to enter this into the record with your permission, Mr. Chairman.

Mr. LANGEVIN. Without objection.

[The information referred to follows:]

Exhibit A

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

ESISAC Advisory Follow-up Survey
Page 2

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

Mr. PASCRELL. That is what we got back. So I have a copy of this survey, and it is dated October 19. It was 2 days, I think, after the hearing. So you misled this committee back in October by claiming that you sent a survey out and received hard numbers back. That did not happen.

Unfortunately, this was not the last time, Mr. Chairman, that this committee was misled.

When we got a copy of the survey back, we asked the staff how you could have hard numbers at the hearing when you had not sent the survey out yet. I think that is a pretty reasonable question. The story changed. We were told that NERC received detailed information about the industry's efforts during a meeting in St. Louis back in September. Having been misled once, the committee requested information from all of the participants at that meeting. This is exhibit B.

Exhibit B, which I have in my hand, Mr. Chairman, has almost 20 response letters from the attendees at that meeting. Each one of them was asked to provide a narrative of the conversation they had with NERC, the North American Energy Reliability Corporation, the organization which has the job of endorsing the regulations. None of them claim to have discussed these mitigation efforts with you. None of them.

Mr. Chairman, I ask unanimous consent to enter these letters into the record as well as exhibit B.

Mr. LANGEVIN. Without objection.

[The information referred to follows:]

Exhibit B

hydro one

EMERGENCY PREPAREDNESS DEPARTMENT
483 BAY STREET • 14TH FLOOR • TORONTO ON • M5G 2P5

January 18, 2008

Bennie G. Thompson and James R. Langevin, Chairmen
Committee on Homeland Security
House of Representatives
Congress of the United States
Washington, DC 20515-6480

02-25-08x11:46 RCVD

Dear Messrs. Thompson and Langevin:

In response to your January 8, 2008, letter requesting me to provide details of discussions I had with NERC staff while attending the September 27-28, 2007, Critical Infrastructure Protection Committee meeting in St. Louis. I need to clarify matters stated in your letter.

I did not meet individually with NERC staff during this meeting to discuss Hydro One Networks Inc.'s implementation efforts. I also did not answer questions regarding the clarity of the recommendations contained in the NERC Advisory, and I did not discuss or otherwise advise NERC staff at this meeting of my company's efforts to mitigate the Aurora vulnerability or the existence of my company's cyber security training program for employees.

However, I did complete, on behalf of Hydro One Networks Inc., a questionnaire provided to me by NERC, and it is my understanding that NERC has provided you with a copy of the completed questionnaire.

Yours very truly,

Dave Baumken
Manager, Emergency Preparedness and
Business Continuity Planning
Hydro One Networks Inc.
Cell 416-564-3394
Office 416-345-4009
david.baumken@HydroOne.com

EMERGENCY PREPAREDNESS DEPARTMENT
483 BAY STREET • 14TH FLOOR • TORONTO ON • M5G 2P5

hydro one

January 18, 2008

Bennie G. Thompson and James R. Langevin, Chairmen
Committee on Homeland Security
House of Representatives
Congress of the United States
Washington, DC 20515-6480

02-25-08 RCVD

Dear Messrs. Thompson and Langevin:

In response to your January 8, 2008, letter requesting me to provide details of discussions I had with NERC staff while attending the September 27-28, 2007, Critical Infrastructure Protection Committee meeting in St. Louis. I need to clarify matters stated in your letter.

I did not meet individually with NERC staff during this meeting to discuss Hydro One Networks Inc.'s implementation efforts. I also did not answer questions regarding the clarity of the recommendations contained in the NERC Advisory, and I did not discuss or otherwise advise NERC staff at this meeting of my company's efforts to mitigate the Aurora vulnerability or the existence of my company's cyber security training program for employees.

However, I did complete, on behalf of Hydro One Networks Inc., a questionnaire provided to me by NERC, and it is my understanding that NERC has provided you with a copy of the completed questionnaire.

Yours very truly,

Dave Baumken

Dave Baumken
Manager, Emergency Preparedness and
Business Continuity Planning
Hydro One Networks Inc.
Cell 416-564-3394
Office 416-345-4009
david.baumken@HydroOne.com

My first mailing of this letter was returned to me.
Hopefully my letter meets your needs, it has been an experience getting this to you.
Best Regards
Dave

Consumers Energy

A CMS Energy Company

January 22, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, Science and Technology
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Thompson and Chairman Langevin:

Thank you for your letter of January 8, 2008 (copy attached). As indicated in your letter, I attended the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Committee meeting in September, 2007 in St. Louis, MO. I was a participant at the meeting, but I did not speak in any panel discussions. More importantly, at this meeting I did not engage in any individual discussions with NERC staff, nor did I answer any questions regarding the matters specified in your letter. Since no such discussion took place, I am unable to provide you with the narrative you request.

I hope this information sufficiently responds to your request. Should you need more information or have any questions, please do not hesitate to contact me.

Sincerely,

L. Michael Ketchens/pm

L. Michael Ketchens,
Consumers Energy Company

One Energy Plaza . Jackson, MI 49201 . www.consumersenergy.com

Alliant Energy Corporate Services, Inc.
Corporate Headquarters
4902 North Biltmore Lane
P.O. Box 77007
Madison, WI 53707-1007

Office: 1.800.862.6222
www.alliantenergy.com

January 23, 2008

01-23-08P06:52 RCVD

The Honorable Bernie G. Thompson, Chairman
The Honorable James R. Langevin, Chairman
U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Emerging Threats, Cyber Security, Science and Technology
Washington, D.C. 20515

Dear Gentlemen:

Thank you for your January 8, 2008, inquiry regarding the "Aurora" vulnerability as disclosed in the June 21, 2007, NERC ES-ISAC Advisory, and associated communications. Let me assure you Alliant Energy Corporate Services, Inc. takes this issue very seriously and respects the concerns you have expressed. The following are answers to the questions that were sent by your office in the January 8, 2008 communiqué.

On September 27-28, 2007, I attended the NERC Critical Infrastructure Protection Committee in St. Louis Missouri.

Although I participated in the public meeting, I did not meet separately, privately, or individually with NERC staff to discuss my company's implementation efforts.

During the course of the public meeting, the topic of the "Aurora" vulnerability as disclosed in the June 21, 2007 NERC ES-ISAC Advisory was discussed. This discussion was held in a round-table forum context, where any attendee could offer their opinions, suggestions, or input.

During this discussion, I was not asked to disclose, nor did I disclose specific steps that Alliant Energy Corporate Services, Inc. performed as part of a response to the "Aurora" vulnerability.

To the best of my recollection, I expressed concern regarding certain mitigation measures that were published in the advisory. I stated that it may be counter productive to permanently damage or disable components of system protection equipment as mentioned in the June 21, 2007 NERC ES-ISAC Advisory Mitigation Measure 2.1.4.

Sincerely,

David Batz
Cyber Security Risk Manager

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

3

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

January 8, 2008

Mr. John Lim
Consolidated Edison Co. of New York
4 Irving Place, Room 349-S
New York, New York 10003

Dear Mr. Lim:

The Committee on Homeland Security is conducting a review of the electric industry's efforts to mitigate the "Aurora" vulnerability. The Committee recently requested and received documentation from the North American Electric Reliability Corporation (NERC) to help determine the extent of the sector's efforts to implement the security recommendations contained in the June 21, 2007 NERC Advisory. According to these documents, NERC staff met with you individually at the NERC Critical Infrastructure Protection Committee meeting, held from September 27-28 in St. Louis, Missouri, to discuss your company's implementation efforts.

During this meeting with NERC staff, you answered questions regarding the clarity of the recommendations contained in the NERC Advisory, the extent of your company's efforts to mitigate the Aurora vulnerability, and existence of your company's cybersecurity training program for employees. Please provide the Committee with a detailed narrative explaining this discussion with NERC.

Pursuant to Rule X (3) (g) and Rule XI of the Rules of the House of Representatives, we request a response in writing by not later than January 25, 2008. If you have any questions, please contact, Cherri L. Branson, Chief Oversight Counsel, Committee on Homeland Security at (202) 226-2616.

Sincerely,

Bennie G. Thompson
Chairman

James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, Science and Technology

01/22/2008 12:40 FAX 501 570 2480 IT DIVISION 002

Arkansas Electric Cooperative Corporation

Your Touchstone Energy Cooperative

8000 Scott Hamilton Drive
P.O. Box 194208
Little Rock, Arkansas 72219-4208
(501) 570-2200

January 22, 2008

01-22-08P01:47 RCVD

U.S. House of Representatives
Committee on Homeland Security
176 Ford House Office Building
Washington, DC 20515

Dear Sirs/Madams,

I am writing in response to a letter from the Committee, dated January 8, 2008 and sent to my attention, regarding my involvement in a meeting of the Critical Infrastructure Protection Committee (CIPC) of the North American Electric Reliability Corporation (NERC) on September 27-28, 2007 in St, Louis, MO. That letter suggested that I had discussions with NERC Staff while at that meeting and asked that I provide detailed information regarding those discussions.

Though I am a Member of the NERC CIPC and attended the meeting in question, I did not:

a) have individual meetings with NERC Staff regarding Arkansas Electric Cooperative Corporation's (AECC) implementation efforts related to the NERC Advisory issued June 21, 2007;
b) answer questions regarding the clarity of the recommendations contained in the NERC Advisory;
c) answer questions regarding the extent of AECC's efforts to mitigate the Aurora vulnerability; or
d) answer questions related to the existence of AECC's cyber security training program for employees.

Since I did not participate in any of those activities, I am unable to provide the detailed narrative requested by the Committee.

Sincerely,

Robert H. McClanahan
Vice President, Information Technology
Arkansas Electric Cooperative Corporation
Member, NERC CIPC

Xc: Robert M. Lyford, AECC

Sent via fax transmission on 01/22/2008
The Electric Cooperatives of Arkansas
We're here for you.

American Electric Power
Service Corporation
1 Riverside Plaza
Columbus, OH 43215
614 223 1000

AEP
AMERICAN ELECTRIC POWER

January 23, 2008

The Honorable Bennie G. Thompson
Chair, Committee on Homeland Security

The Honorable James R. Langevin
Chair, Subcommittee on Emerging Threats,
Cybersecurity, Science and Technology

U.S. House of Representatives
H2-176 Ford House Office Building
Washington DC 20515

Dear Chairman Thompson and Chairman Langevin:

Thank you for your letter of January 8, 2008, concerning the electric industries efforts to mitigate the "Aurora" vulnerability. You noted that I talked with staff of the North American Electric Reliability Corporation (NERC) during the September NERC Critical Infrastructure Protection Committee meeting. You requested details of my discussions with NERC staff concerning my company's efforts to implement the security recommendations contained in the June 21, 2007, NERC Advisory.

I attended the NERC Critical Infrastructure Protection Committee and had only brief conversations with NERC Staff on my company's implementation activities. I assured NERC staff that my company's efforts were timely and successful.

If you would like to discuss this matter, or have any questions, please contact Joe Hartsoe, 202.383.3435 in our Washington Office or me.

Sincerely,

Gerald Freese
Director, IT Security Engineering

Northeast Utilities

107 Selden Street, Berlin, CT 06037

Northeast Utilities
P. O. Box 270
Hartford, CT 06141-0270
Phone: (860) 665-5000

January 24, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, and Science and Technology
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairmen:

Thank-you for your letter of January 8, 2008, regarding the Committee on Homeland Security's review of the electric industry's efforts to mitigate the cyber vulnerability identified in the "Aurora" demonstration. Northeast Utilities ("NU") shares your desire that all appropriate steps should be taken to protect against actions that could potentially damage the nation's electric infrastructure and cause significant impacts to our economy, public health and national security.

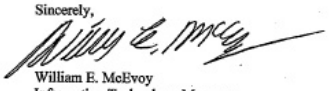
Your letter states that I met individually with the North American Electric Reliability Corporation ("NERC") staff at the September 27-28, 2007 Critical Infrastructure Protection Committee meeting in St. Louis, Missouri to discuss NU's implementation of the Electric Sector Information Sharing and Analysis Center's ("ES-ISAC") June 21, 2007 advisory on security measures to address the "Aurora" cyber vulnerability. While I attended this meeting, I did not have any discussions with or answer any questions from the NERC staff regarding the clarity of the ES-ISAC recommendations or their implementation by NU. Since the discussions described in your letter did not occur, I am unable to provide the detailed narrative you have requested.

Nevertheless, I want to assure you that NU is taking appropriate action to protect its electrical system critical infrastructure from cyber threats under the bulk power system reliability measures required by section 215 of the Federal Power Act. NU has folded its response to the ES-ISAC advisory into its compliance program for all NERC standards, including the Critical Infrastructure Protection Standards

("CIPS") that were approved last week by the Federal Energy Regulatory Commission ("FERC") in Order No. 706. In that order, the FERC approved the eight proposed CIP Reliability Standards with directives to NERC to address specific concerns with the individual standards and to reduce the permitted exceptions to full compliance with the standards. NU expects to be fully compliant with the approved CIPS requirements by the 2010 implementation deadline. Further, NU will incorporate any of the FERC's suggested revisions to the CIPS adopted by NERC, plus any other enhancements NERC deems necessary to ensure cyber-security. In sum, NU is working diligently to ensure that timely and effective measures are in place to guard against the cyber vulnerability of our critical electrical system assets.

If I can be of further assistance to the Committee or Subcommittee in this matter, please do not hesitate to let me know.

Sincerely,



William E. McEvoy
Information Technology Manager
mcevowe@nu.com
860-665-2465

Entered Attch to 01/08 Ltr.

conEdison
a conEdison, Inc. company

Consolidated Edison Company
of New York, Inc.
4 Irving Place
New York NY 10003
www.conEd.com

01-28-08P03:15 RCVD

January 24, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S House of Representatives
Washington, DC 20515

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, Science and Technology
Committee on Homeland Security
U.S House of Representatives
Washington, DC 20515

Dear Messrs Thompson and Langevin:

I am responding to the request in your letter dated January 8, 2008 regarding electric industry mitigation of the "Aurora" vulnerability.

I attended the NERC Critical Infrastructure Protection Committee meeting held on September 27-28, 2007 in St. Louis, Missouri as a representative of the Northeast Power Coordinating Council. The NERC ES-ISAC June 21, 2007 Advisory (NERC Advisory) was on the committee's agenda. NERC staff member Stan Johnson led a group discussion around the format and distribution method of a proposed survey as a follow-up to the NERC Advisory, lessons learned from the advisory process, and the CNN report.

During a meeting break, I had a sidebar conversation with two NERC staff members who were former fellow team members of the NERC Cyber Security Standards Drafting Team and briefly and generally discussed the Aurora vulnerability and the CNN report without any specific reference to Con Edison.

I did not have any further discussion on the Aurora vulnerability with any NERC staff member at the meeting.

Sincerely,

John Lim
Department Manager
Consolidated Edison Co. of New York, Inc.
4 Irving Place, Rm 349-S
New York, NY 10003

Southern Company Services, Inc.
30 Ivan Allen Jr. Boulevard NW
Atlanta, Georgia 30308

January 23, 2008

SOUTHERN COMPANY
Energy to Serve Your World

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cyber Security, and Science and Technology
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairmen:

I am writing in response to your letter of January 8, 2008 regarding North American Electric Reliability Corporation (NERC) meetings in St. Louis and the "Aurora" Advisory. Your letter requested information about individual meetings I may have had with NERC staff about the Southern Company response to this advisory. This letter is to respond to your request and inform you that I did not have any such meetings with NERC staff as described in the January 8 letter.

I hope that this information satisfies your request. Please let me know if you have any questions or if there is anything further that I need to do.

Sincerely,

RD Canada

R.D. Canada
Business Assurance Principal

PRIVILEGED AND CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION

Add. to 01/08 letter.

Southern Company Services, Inc.
30 Ivan Allen Jr. Boulevard NW
Atlanta, Georgia 30308

January 23, 2008

SOUTHERN COMPANY
Energy to Serve Your World™

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

01-28-08 10:29 PCVC

The Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cyber Security, and Science and Technology
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairmen:

I am writing in response to your letter of January 8, 2008 regarding North American Electric Reliability Corporation (NERC) meetings in St. Louis and the "Aurora" Advisory. Your letter requested information about individual meetings I may have had with NERC staff about the Southern Company response to this advisory. This letter is to respond to your request and inform you that I did not have any such meetings with NERC staff as described in the January 8 letter.

I hope that this information satisfies your request. Please let me know if you have any questions or if there is anything further that I need to do.

Sincerely,

Jay S. Cribb
Information Security Analyst

PRIVILEGED AND CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION

Kansas City Power & Light®

January 15, 2008

01-30-08P02:23 RCVD

Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington DC 20515

Dear Chairman Thompson

On Friday January 11, 2008 I received a request; copy enclosed, from you to provide a narrative explaining discussions with the staff of the North American Electric Reliability Corporation, NERC. I can provide the following information regarding your request.

First, the letter was addressed to Robert Dolci. My name is Lawrence Dolci but since I did attend the September 27-28 meeting in St. Louis referred to in the letter I assume the letter was meant for me.

Second, I had no individual meeting with NERC staff at the St. Louis meeting. I had no discussion with the NERC staff regarding my Company's "implementation efforts". I did not answer questions from the NERC staff "regarding the clarity of the recommendations contained in the NERC Advisory, the extent of your company's efforts to mitigate the Aurora vulnerability, and existence of your company's cybersecurity training program for employees."

Since the discussions you reference did not take place I cannot provide you with the narrative you requested.

Sincerely yours,

Lawrence H. Dolci
Director Resource Protection

cc Honorable James R. Langevin
Chairman
Subcommittee on Emerging Threats
Cybersecurity, Science and Technology

1201 Walnut Street | Post Office Box 418679 | Kansas City, Mo. 64141-9679 | tel. 816.556.2200 | www.kcpl.com

Exelon.

Corporate Security Department
10 South Dearborn
50th Floor
Chicago, IL 60603

www.exeloncorp.com

January 23, 2008

Hon. Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

02-06-08A10:24 RCVD

Reference: January 8, 2008 Request for Information
Relating to NERC Mitigation Discussions

Dear Mr. Chairman:

I am writing you in response to your January 8th letter requesting information about discussions at the September 27th – 28th NERC Critical Infrastructure Protection Committee meeting in St. Louis.

I attended the EEI Conference held in St. Louis the week of September 24th, including the NERC Critical Infrastructure Protection Committee meeting held September 27-28, 2007.

I did not, however, meet with the NERC Staff to discuss the NERC Advisory, the extent of my company's efforts to mitigate the Aurora vulnerability, the existence of my company's cybersecurity training program, or indeed any other subject.

I hope this satisfies your request. If you have any further questions, please do not hesitate to contact me.

Thank you,

Eliasa Rhee-Lee
Vice President, Corporate Security

cc: James R. Langevin

Entergy

Entergy Services, Inc.
639 Loyola Avenue 70113
P.O. Box 61000 70161
New Orleans, LA
Tel 504 529 5262

6 February, 2008

02-07-08 11:11 RCVD

Mr. Bennie Thompson
Mr. Jim Langevin
Congress of the United States
Committee on Homeland Security
Subcommittee on Emerging Threats, Cyber Security, Science and Technology

Dear Mr. Thompson and Mr. Langevin:

I am writing in response to your letter dated 8 January, 2008. Your letter stated that documents which the Committee received from NERC indicated that NERC staff met with me individually to discuss my company's efforts to implement security recommendations contained in the NERC security advisory of June 21, 2007. Your letter specifies the NERC Critical Infrastructure Protection Committee [CIPC] meeting, held from September 27-28, 2007 in St. Louis, Missouri, Conference, as the site of the meeting.

I attended the CIPC Conference, but I do not have any recollection of a meeting or conversation with a NERC representative on this topic. I have checked my calendar and other records from the Conference and they also do not reflect any meetings or discussions with NERC. Accordingly, I cannot provide the detailed narrative requested in your letter.

I welcome the opportunity to be of further assistance.

Sincerely,

David L. Norton, CISSP
Program Manager – Transmission IT Security
Entergy Services, Inc.
639 Loyola Avenue / L-ENT-17B
New Orleans, LA 70113

AMERICAN TRANSMISSION COMPANY®

MAILING ADDRESS: P.O. BOX 47 • WAUKESHA, WI 53187-0047
STREET ADDRESS: N19 W23993 RIDGEVIEW PARKWAY WEST• WAUKESHA, WI 53188-1000
262.506.6700• Toll Free: 866.899.3204 • FAX: 262.632.6710 • www.atcllc.com

Council
Add to 01/08 Cal.

February 7, 2008

02-11-08P03:20 RCVD

U.S. House of Representatives
Committee on Homeland Security
Washington, D.C. 20515

Attention: Chairman Bennie G. Thompson and Chairman James R. Langevin, Subcommittee on Emerging Threats, Cyber security, Science and Technology

Dear Chairman Thompson and Chairman Langevin:

Per your letter dated January 8, 2008, which requests information regarding any discussions I held with NERC staff at the NERC Critical Infrastructure Protection Committee meeting held on September 27-28, 2007, in St. Louis, Missouri, I submit the below response to your inquiry.

While I did attend the NERC Critical Infrastructure Protection Committee meeting referenced above and in your letter, and did represent American Transmission Company LLC ("ATC") at such meeting, I did not have the opportunity to meet individually with NERC staff, at that time, to discuss ATC's implementation of the NERC advisory relating to the "Aurora" vulnerability. Due to the fact that I did not meet individually with NERC staff, I did not then answer any questions regarding the clarity of the recommendations contained in the noted NERC Advisory.

I acknowledge that I had previously received the NERC "Aurora" Advisory and thereafter ensured that the appropriate ATC personnel were made aware of the contents of that advisory. While I did not discuss our compliance efforts with the NERC staff present at the Critical Infrastructure Protection Committee meeting held in September, I can assure you that ATC has fully complied with the NERC Advisory and successfully mitigated any previous exposure, if any, that ATC may have had to an intrusion similar to that demonstrated in the Idaho National Laboratory's "Aurora" experiment.

I will also note that while there was some discussion at the September NERC committee meeting of a proposed technical conference addressing the particulars of the Aurora vulnerability, I did not offer any suggestions relating to such proposal. Further, the September meeting also included an update on the potential for NERC and/or others within the industry to conduct a "How" workshop addressing the Critical Infrastructure Protection standards.

If you have any further questions, please contact me at 262.506.6746.

Sincerely,

Eric Solberg

Attach to cyber ltr.

PACIFIC NORTHWEST
SECURITY COORDINATOR
TO-DITT1-NWSC
5411 NE Highway 99
Vancouver, Washington 98663-1302

Phone: (360) 418-2956
Fax: (360) 993-2204
Email: jack@pnsc-center.com

02-11-08P01:25 RCVD

"COST-EFFECTIVE OVERSIGHT FOR STABLE, SECURE GRID OPERATIONS"

January 23, 2008

Congressman Bennie G Thompson
Chairman, Committee on Homeland Security
US House of Representatives
Washington, DC 20515

SUBJECT: **Request for Narrative of September 27-28, 2007 Discussion with NERC Staff Regarding the "Aurora" Vulnerability**

Dear Congressman Thompson:

I did not receive your January 8, 2008 letter until yesterday, so this is necessarily brief.

I do not recall the individual meeting with NERC staff referenced in your letter.

The Pacific Northwest Security Coordinator, Inc (PNSC) is a nonprofit corporation registered in the State of Washington for the specific purpose of providing Reliability Coordination services to the electric industry entities in our area of responsibility.

We are not an electricity sector owner or operator. Therefore we do not own or operate any equipment for which the "Aurora" vulnerability applies.

We accomplish our oversight tasks by monitoring and analyzing system conditions and directing the appropriate entities to take mitigating actions when necessary. We do not have any direct control over any equipment. Our ability to influence the posture of the electric grid rests primarily with voice communications.

We operate by agreement from a facility owned by the US Department of Energy's (DOE) Bonneville Power Administration. All members of our staff participate in the DOE's security training programs, including its cyber security training.

Sincerely,

D. J. (Jack) Bernhardsen
President

2008/JAN/23/WED 01:25 PM Corp.SecEnerg.Prep. FAX No. 6263027881 P. 002

SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

Robert L. Sypult
Director
Corporate Security

02-08-08 05:29 RCVD

Ms. Cherri L. Branson
Chief Oversight Counsel
Committee on Homeland Security
U.S. House of Representatives
176 Ford Bldg.
Washington, D.C. 20151

Re: Letter dated January 8, 2008

Dear Ms. Branson:

Thank you for clarifying the Homeland Security Committee's request for information regarding my attendance at a meeting of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Council (CIPC) in St. Louis, Mo on September 27, 2007.

As we briefly discussed, I attended one-day of the meeting as a representative of the Western Electric Coordinating Council (WECC), leaving mid-afternoon on the 27th. During the meeting, there was open/general discussion about the ES-ISAC advisory sent out by NERC in June 2007, the distribution process, and action-items needed to improve the process in the future. It was agreed that one of the action-items would be a survey sent out by NERC staff to ascertain the progress of utilities in mitigating against the "Aurora" vulnerability outlined in the June advisory. All of this was documented in the meeting minutes, which are publicly available at NERC's website:

http://www.nerc.com/~filez/cipmin.html

At no time during the meeting did I meet individually with the NERC staff on this issue, nor do I recall any vote being taken regarding any of the follow-up activity, so to clarify the questions in the referenced letter, I did not answer any questions at the meeting, but merely participated as a WECC representative, along with about 100 other attendees.

That, to the best of my recollection, was my involvement in the referenced CIPC meeting. If there are any additional questions, I can be contacted through SCE at the address you have on file, or at 626-302-7875. Thank you.

Sincerely,

Robert L. Sypult
Director, Corporate Security &
Emergency Preparedness (Retired)

Cc: M. Mackness
R. Furman
J. Monroe
xc: Young Gault, NOC

8631 Rush Street
Rosemead, CA 91770
626-302-7910/FAX 27910
Fax 626-302-7881
Robert.Sypult@sce.com

ONCOR

William E. Muston
Manager
Research & Technology Development

Oncor Electric Delivery
1601 Bryan Street
Dallas, TX 75201

Tel 214 486 3015
bill.muston@oncor.com

January 24, 2008

02-11-08P01:25 RCVD

Hon. Bennie G. Thompson
Chairman, Homeland Security Committee

Hon. James R. Langevin
Chairman, Subcommittee on Emerging Threats, Cybersecurity, Science and Technology

U.S. House of Representatives
Committee on Homeland Security
Washington, D.C. 20515

Dear Chairman Thompson and Chairman Langevin,

This is a response to your letter to me dated January 8, 2008, regarding the "Aurora" vulnerability and discussions at a meeting of the Critical Infrastructure Protection Committee (CIPC) of the North American Electric Reliability Corporation (NERC) in St. Louis on September 27 – 28. I will address your questions about that meeting and will discuss cyber security within a somewhat larger context.

By way of background, NERC CIPC has been engaged in the development of information and guidelines on cyber security for control systems and in the development of industry standards for cyber security for control systems for several years. Most notably, the NERC CIP Standards were approved by the FERC last week. With the FERC action, the industry now has specific requirements and a schedule to put in place a comprehensive management approach to cyber security. As you undoubtedly are aware, technical aspects of cyber security and related threat vectors are continuously changing, and a comprehensive approach to cyber security is necessary.

Oncor is very attuned to cyber security with respect to controls for the electric transmission grid. Oncor is also very supportive of NERC and the NERC CIPC, and looks forward to continuing to cooperate with NERC and complying with the NERC CIP standards and in mitigating threats and vulnerabilities. Oncor has been actively engaged in meeting the requirements and schedule of the NERC CIP Standards since June 2006.

As a general matter, risk management is an important management element of Oncor's business. Oncor's risk management considers a wide variety of risks and utilizes judgment of threat capabilities, likelihood, and impact, in assigning resources toward the various business and operational risks the company faces. To date, Oncor has not received any intelligence on threat capabilities that might be actively seeking to exploit this vulnerability, even though Oncor has chosen to take mitigating action.

Cyber security for transmission control systems is not new to Oncor. Oncor first began considering cyber security vulnerabilities in 1997 when it came into contact with a program operated through DOE's national laboratories that was examining cyber security. Oncor agreed to enter into "red teaming" studies with the national laboratories, and a kickoff meeting was held in November of 1998.

DTE Energy Company
2000 2nd Ave., Detroit, MI 48226-1279

DTE Energy

January 24, 2008

01-24-08P03:38 RCVD

Hon. Bennie G. Thompson, Chairman
U.S House of Representatives
Committee on Homeland Security
2432 Rayburn House Office Building
Washington, DC 20515

Hon. James R. Langevin, Chairman
Subcommittee on Emerging Threats, Cybersecurity,
Science and Technology
U.S House of Representatives
Committee on Homeland Security
109 Cannon House Office Building
Washington, DC 20515

Re: NERC Meeting

Gentlemen:

I am responding to your letter dated January 8, 2008 in which you requested information regarding a North American Electric Reliability Corporation (NERC) meeting held in St. Louis on September 27-28, 2007.

I did attend the NERC Critical Infrastructure Protection Committee meeting held on those dates in St. Louis and while I do recall a discussion of the Aurora vulnerability, I do not recall answering any questions concerning either the clarity of NERC's recommendations contained in its Advisory, or The Detroit Edison Company's efforts to mitigate the Aurora vulnerability, including any cyber-security training in that regard.

Detroit Edison is deeply committed to providing effective physical and cyber-security for its electric system. We pay close attention to federal advisories and regularly participate in industry efforts to improve the national energy infrastructure. If I can be of further assistance to the Committee please do not hesitate to contact me.

Very truly yours,

Michael O. Lynch

Michael O. Lynch
Chief Security Officer

cc: Hon. Peter T. King
Hon. Michael T. McCaul

Ameren Services

(314) 554-2970
(314) 554-4014 (fax)
jraybuck@ameren.com

One Ameren Plaza
1901 Chouteau Avenue
PO Box 66149
St. Louis, MO 63166-6149

02-11-08A11:09 RCVD

February 8, 2008

VIA EMAIL

Bennie G. Thompson, Chairman
James R. Langevin, Chairman
Subcommittee on Emerging Threats, Cybersecurity,
Science and Technology
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

Dear Chairman Thompson and Chairman Langevin:

This will respond to your letter of January 8, 2008 to Mr. Goatey. We apologize for the delay in responding. However, Mr. Goatey was on a two week vacation when your letter arrived and did not see it until he returned to work and received his mail on January 30, 2008.

As explained to Mr. Jake Olcott of your staff, Mr. Goatey is no longer employed by Ameren. Instead, he elected to take another job with Prairie State Generating Company. Further, his recall is limited on the issues set forth in the Committee's letter.

As a result, in response to the Committee's letter Ameren would like to submit the affidavits of Robin Goatey together with the affidavits of two existing Ameren employees, Mr. Paul Nauert and Ms. Linda Nappler.

If you have any questions about this, or need any additional information please do not hesitate to call me. Thank you.

Sincerely,

Joseph H. Raybuck
Managing Associate General Counsel

JHR/dkp
Attachments (3)

AFFIDAVIT OF ROBIN L. GOATEY

Robin L. Goatey, being first duly sworn, states as follows:

1. My name is Robin L. Goatey. Since February 1, 2008 I have been employed by Prairie State Generating Campus, L.L.C. My business address is 4190 County Highway 12, Marissa IL 62257. Prior to that date, I was employed by Union Electric Company, doing business as AmerenUE, as a Generation Technology Specialist III. I had been employed by AmerenUE or one of its affiliates since 1978. AmerenUE is one of several subsidiaries of Ameren Corporation (Ameren). My last date of employment with AmerenUE was January 31, 2008.

2. The purpose of my affidavit is to respond to the letter of January 8, 2008 which was sent to me by Chairman Bennie G. Thompson and Chairman James R. Langevin of the U.S. House of Representatives Committee on Homeland Security.

3. The Committee's letter of January 8 asked me to provide information about a discussion I had with representatives of the North American Electric Reliability Corporation (NERC) in September of last year. In particular, the letter of January 8 asked me to provide a detailed narrative explaining the discussion I had with NERC representatives at a meeting of its Critical Infrastructure Protection Committee (CIPC) on September 27-28, 2007.

4. Although I do not recall word for word what I discussed with NERC representatives on the dates in question, I recall talking with them about the Aurora vulnerability and Ameren's efforts to address it. In general, I told NERC that Ameren had taken action to eliminate the Aurora vulnerability.

5. During that September 2007 discussion at the CIPC meeting, NERC Staff asked for feedback on Aurora Mitigation preparation by CIPC Members. By Aurora Mitigation, I mean action which involves changing a switch, inside the Rotating Equipment Synchronism Check Relays, from "Allow Remote Access" to "Do Not Allow Remote Access". I told NERC representatives that Ameren went ahead and performed the mitigation because it was determined to be safe practice if there was even a chance of vulnerability. Mr. Paul Nauert of Ameren is submitting an affidavit discussing the actions that Ameren has taken.

6. I do not remember answering a question about cybersecurity training. Ms. Linda Nappier of Ameren is submitting an affidavit which addresses the actions Ameren has taken on this issue.

7. This covers everything that I can recall being discussed with NERC on September 27 and 28, 2007 on the topic of the Aurora vulnerability.

Robin L. Goatey

Subscribed and sworn to before me, the undersigned notary public, this 8TH day of February 2008.

"OFFICIAL SEAL"
KARI GOING
NOTARY PUBLIC—STATE OF ILLINOIS
MY COMMISSION EXPIRES APRIL 24, 2011

Kari Going
Notary Public

AFFIDAVIT OF PAUL J. NAUERT

Paul J. Nauert, being first duly sworn, states as follows:

1. My name is Paul J. Nauert. I am employed by Ameren Services Company (Ameren Services) as a Consulting Engineer in the System Protection group. Ameren Services is one of several subsidiaries of Ameren Corporation (Ameren). I have been employed by an Ameren company since June, 1980. My business address is 1901 Chouteau Avenue, St. Louis, Mo. 63103.

2. The purpose of my affidavit is to respond to one of the issues raised in the letter of January 8, 2008 which was sent to Robin L. Goatey by Chairman Bennie G. Thompson and Chairman James R. Langevin of the U.S. House of Representatives Committee on Homeland Security. In particular, I will address the extent of Ameren's efforts to mitigate the Aurora vulnerability.

3. I have had responsibility for the protection of the Ameren power system, which includes rotating high voltage equipment such as electrical generators and large motors. Along with IT Security Planning, I share responsibility to assure the cybersecurity of digital protective and control devices that are used with such equipment.

4. In response to the June 21, 2007 Advisory from NERC on the Aurora vulnerability, Ameren took the following actions. First, my group at Ameren reviewed the Advisory and participated in several teleconferences with industry representatives from EEI and NERC to assure that we had a proper understanding of it. We then assessed the risk to the Ameren system based on the Advisory. Concurrently, we formed a team of power system protection specialists and addressed each measure in the Advisory. Next for areas

identified as at risk pursuant to the Advisory we confidentially communicated with owners of rotating high voltage equipment. We then determined appropriate actions to mitigate consistent with the Advisory. In general, we reviewed the relevant equipment and devices and determined whether they could be remotely accessed. For those which did allow for remote access, we took action such as eliminating the access. After this, we verified that the necessary changes had been made. Finally, we responded to NERC per a confidential report via an email sent by Ms. Linda Nappier on October, 31 2007 providing our mitigation status report and indicating Ameren had taken action consistent with the Advisory.

Paul J. Nauert

Subscribed and sworn to before me, the undersigned notary public, this 07 day of February 2008.

Notary Public

DEBRA K. PATTERSON
NOTARY PUBLIC - NOTARY SEAL
State of Missouri
St. Louis County
My Commission Expires Oct. 31, 2008
Commission # 04482292

AFFIDAVIT OF LINDA M. NAPPIER

Linda M. Nappier, being first duly sworn, states as follows:

1. My name is Linda M. Nappier. I am employed by Ameren Services Company (Ameren Services) as Manager IT Security Planning. Ameren Services is one of several subsidiaries of Ameren Corporation (Ameren). I have been employed by an Ameren company since 1976. My business address is 1901 Chouteau Avenue, St. Louis, Mo. 63103.

2. The purpose of my affidavit is to respond to one of the issues raised in the letter of January 8, 2008 which was sent to Robin L. Goatey by Chairman Bennie G. Thompson and Chairman James R. Langevin of the U.S. House of Representatives Committee on Homeland Security. In particular, I will address Ameren's cybersecurity training program for its employees.

3. As the Manager of IT Security & Planning, I have responsibility for publishing security policies and for developing security awareness and training for Ameren's employees, such as for those issues included in the Advisory of June 21, 2007 from NERC referenced in the Committee's letter of January 8. In particular, my role has been to ensure that the right subject matter experts at Ameren are brought in to address cybersecurity issues, as we did in response to the June 21, 2007 Advisory.

4. Ameren has an ongoing cybersecurity training and awareness program for communicating our security policies to our employees. Ameren submitted its compliance status with NERC standard CIP-004-R2 as "substantially compliant" as of June 30, 2007. This status was based on instructor-led NERC CIP-002 through CIP-009 cybersecurity training presented to the employees in the control

center, which I personally conducted. Ameren documented its "substantially compliant" status in our self-certification filings with SERC, our Regional Entity, on July 13, 2007. Additional training development requirements were identified in our self-certification filing for CIP-004-R2 which, when implemented as scheduled, will fulfill the requirement to be fully "compliant" by the June 30, 2008 deadline.

Linda M. Nappier

Subscribed and sworn to before me, the undersigned notary public, this 07 day of February 2008.

Notary Public

DEBRA K. PATTERSON
NOTARY PUBLIC - NOTARY SEAL
State of Missouri
St. Louis County
My Commission Expires Oct. 31, 2008
Commission # 04482292

2

Mr. PASCRELL. So let us get to the bottom of this.

I want you, the CEO of NERC, to clarify for all of us what you have been doing since June 21 of last year when the initial advisory went out. As you explain to us what happened, please tell us in answers to these two following questions:

Why did your company provide false and misleading information to this committee?

Second, if you did not send a survey out until 2 days after the hearing and you did not talk to the folks at the St. Louis meeting, which you claimed, where did you get the numbers that you cited in October?

Mr. SERGEL. As I indicated to the subcommittee, first, the responsibility for being clear is entirely ours, and we have failed to

do that. That is clear. Going forward, we will do better. Let me take you back——

Mr. PASCRELL. Excuse me. This is not a question of doing better. This is not a question of doing better. This is a question of telling the truth as to the best of your knowledge like any human being on the face of this Earth. We are all fallible. Only God is perfect. But you and your company two times told us fibs. Why?

Mr. SERGEL. In June, we sent out the initial advisory. Between that time and the committee hearing, we conducted a series of oral interviews. I will have to get to the bottom of whether they took place in St. Louis or in other locations, but I do believe that those interviews took place, but I will have to go back and look at that.

Mr. PASCRELL. Mr. Sergel, you are the electrical reliability organization for this country; is that not correct?

Mr. SERGEL. Yes, sir.

Mr. PASCRELL. In listening to your answer, how is this committee supposed to believe that you are taking the job seriously? FERC had to do a new survey because they thought yours was inadequate. Do you think NERC is really ready to carry out such duties?

We are talking about, Mr. Chairman, life and death. We are not talking about misplaced adverbs here. We are talking about serious business as we were talking about serious business when we looked at the chemical industry.

We want to be friends. We want to be partners with the electrical companies, with the utilities. We want to be partners, but you are not going to sit there and waste my time and tell me that we are doing the job that we were directed to do. At the same time, you have no real answer for these two documents that you sent us. What do you think we are, a bunch of jerks?

Now, let me tell you. I am from Paterson, New Jersey. It is not the most perfect place in the world, but the one thing we do not tolerate on the streets is people telling fibs. If I ask you a question and you do not know what the answer is, fine. That is fair. It is very fair.

Mr. Chairman, considering what we already know about these misleading statements, I think we should look into the processes for holding the—let me get it straight, Mr. Chairman—the North American Energy Reliability Corporation. "Slowly I turn." Do you remember that one? "Slowly I turn." I would like to look into the process for holding this organization in contempt of this committee. I am serious about this, Mr. Chairman. I was just as serious when we went after truth in the chemical industry, and we should be just as serious today because the American people deserve no less.

Would you agree with me or disagree with me?

Mr. LANGEVIN. Well, I certainly agree with the gentleman. I share his anger and frustration over not getting accurate information. I will certainly look into the gentleman's request and recommendation about contempt.

As I have made clear, I do not ever want to hear that kind of testimony, that unclear or misleading testimony, before this subcommittee or the full committee ever, ever again. When someone does not know an answer, the proper response is, "We will take

that for the record," or "I am unsure," but not to just, it seems, make up information or to present unclear information as fact.

I heard the gentleman, Mr. Sergel, in his testimony today say that they will do better in the future. They have acknowledged the mistake. Again, it does not change the fact that there was unclear information that was presented as fact to this committee. I will certainly look into the gentleman's request.

With that, the Chair now recognizes the gentleman from North Carolina, Mr. Etheridge, for 5 minutes.

Mr. ETHERIDGE. Thank you, Mr. Chairman. Thank you for holding this hearing today.

Let me ask a question. All of us remember in 2003 when the blackout covered much of northeastern United States. We have been fortunate we have not had that in recent years, but that blackout was from causes that are still not totally clear but which seem to come to rest on the failure of three transmission lines in Cleveland. We have pretty much come to that realization.

My question is, with utility uses and prices likely to hit record peaks this year, we really cannot afford disruptions that could create additional burdens on business, and all of us know what happens if we lose power with all of the major computer systems that we have. The interconnected nature of our electric grid means that a single point of failure can cause a cascading event that can be devastating, and that certainly shows us what could happen.

So my question is, how likely is it that a single cyber attack on a controlled system could cause a massive disruption of our electrical grid?

Let me go ahead and get a couple more questions in the loop so we will have it all out there.

Second, how would you compare the cyber risks to the electrical sector to other risks?

Finally, are public utilities—this has been touched on a little bit earlier. Are public utilities and private companies taking this threat as seriously as they should before people start paying attention to it? People always pay attention to it when they have a problem. Then once the problem is over with, they figure it is solved, and they move on to something else.

It is in whatever order you want to take those three. How likely is it to cause a massive disruption? No. 2, compare the risks to the electrical sector to other risks. Then public-private utilities in working together.

Mr. KELLIHER. There is some risk that you could be faced with a large regional blackout like we saw in August 2003. August 2003 really was, at least by one count, one of eight large regional blackouts. It was the one that affected the most number of people, but there were blackouts in the summer of 2002 and in the summer of 1996, and they really stretched back to the 1960's. So that is always a risk.

Now, the cyber risk, I am not sure we could qualitatively say the consequence of a cyber attack would be greater than other reliability risks, but the nature of it is very different. It is a national security risk, a national security threat. So the origin of threat is fundamentally different from the other reliability threats. That is why we think at FERC we need to have a different statutory tool,

a different way to guard against that specific risk. We do think current law is adequate to address other reliability threats and that it should not be amended. Section 215 of the Federal Power Act, I do not think, should be amended.

Mr. ETHERIDGE. Let me interrupt you for a moment, please, since you have raised that issue.

What additional authority does FERC need in order to ensure that the utilities and private companies do, in fact, take it seriously and deal with it? That is what this committee is really all about.

Mr. KELLIHER. On your third point, I do think utilities are and utilities and others are taking reliability standards seriously. They are making great efforts to comply, and they are positively trying to comply. We do have enforcement authorities. FERC has penalty authority that Congress gave us just 2½ years ago, and that allows us to impose penalties of up to $1 million a day, and that applies to reliability violations as well as others. So I think utilities are taking it seriously currently, but we do think we need legislative authority that, I think, would operate, roughly, in the following way:

If a national security or intelligence agency identifies a threat, only then could FERC act to establish on its own an interim reliability standard to guard against that national security threat such as a cyber threat. That interim standard would stay in place until the threat disappears or until a permanent standard is developed under the 215 process. I view that as a limited grant because I do not think it would be used very often, and I think it recognizes that 215 is adequate to deal with other reliability threats.

Mr. ETHERIDGE. Mr. Sergel and Mr. McCollum, how do you think the industry should react to FERC's having this additional authority?

Mr. SERGEL. I think there is a gap in what we can do. We are limited to doing things in public. We are not confidential. We are limited to the bulk power system. We cannot act quickly enough in those kinds of circumstances, so there is clearly a gap. I see the Commission as kind of our authorizing agency, and therefore, they would be the appropriate ones, at least with respect to NERC, to have that authority despite the fact that we have a very good relationship with Homeland Security and with the Department of Energy. We have a tighter relationship with the FERC. I think there is a last part of this, which is public policy, which is not kind of a NERC responsibility to comment on.

Mr. ETHERIDGE. So I take that as supportive.

Mr. SERGEL. On the two things that we are responsible for, on those two.

Quickly, to your other question on kind of measuring this risk to the others in the system, they are just fundamentally different. You know, we spend a lot of time on trees and on maintenance and on training and on all the kinds of things that are essential to a reliable bulk power system. It is not the same as someone attacking you, and as a consequence, it is just fundamentally different, fundamentally different.

Mr. MCCOLLUM. TVA is committed to the security of our networks and control systems, and we have moved aggressively to increase the security and to make those controls even more robust,

and we certainly will continue to move ahead to strengthen our defense in depth on our networks to meet or to exceed the requirements of any standards or authority that Congress chooses to put in place.

Mr. ETHERIDGE. So that is an affirmative?

Mr. MCCOLLUM. Yes.

Mr. ETHERIDGE. Okay. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. LANGEVIN. I thank the gentleman.

The Chair now recognizes the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. Mr. Chairman, thank you so very much for the courtesies of this committee and to the ranking member, Mr. McCaul, my colleague from Texas.

I think it is important that our respective committees—the Transportation Security and Critical Infrastructure—continue to cross-pollinate on these very crucial issues, and I thank you for your leadership.

I think it is important to note whether or not the witnesses respectively feel that they are on an ongoing hot seat. We are very much aware that intelligence, classified and nonclassified, suggest that terrorists will not act the same, that they will not be redundant, that they will not be repetitive. To a certain extent, they will look for new and creative ways.

We are well aware of the complete shock and collapse of our intelligence communications that generated the horrific tragedy of 9/11. As one of the early members of the Select Committee on Homeland Security, I am reminded of the constant chatter about what we did not do and how we did not follow up with the linkage of our intelligence to know the potential of these 19 terrorists who did this dastardly act.

So we find ourselves here in 2008 with a new, enormous and growing loophole that has been evidenced by the GAO, which found that the Tennessee Valley Authority had significant problems with cybersecurity, with the Aurora loophole. The idea of this hearing—I hope and view as very important—is to not put your finger in the dam for what could be a horrific and devastating act equaling and surpassing the tragic earthquake that just occurred in China and the horrible cyclone in Burma. This is about life and death. This is about Americans' dying. I know that there is a thought that this may be about the idea of lights going out, but it may also be about the ability to, in essence, shut down a system that would impact the very lifeline of this country.

So I am disturbed as well as a nonmember of this committee to hear of the misrepresentation of materials, and it causes me to think, Mr. Chairman, as we did in chemical security—and I think we worked together on that legislation. There were components of both of our committees as we moved on the chemical security legislation out of the Transportation Security committee and out of this committee. That legislation is imperative. I know that there are initiatives that we have spoken about, but let me raise this question as I raise it for all of the witnesses.

To the Tennessee Valley Authority: Can you tell me why—and forgive me if you have answered it, and I would love a brief an-

swer—you are called the Nation's largest power company, and we are quite proud of the technology of the Tennessee Valley Authority. In fact, we are probably, on the floor of the House, discussing this question of hydropower. Can you tell me why it seems that you have not fully implemented security measures that would operate against a catastrophic event for your entity?

For the other witnesses, speak to the point of legislation with punitive measures—criminal and fines—as an incentive in what is, I think, a very challenging question.

Mr. McCollum, I believe, for the Tennessee Valley Authority, where are you in the implementation of these security measures?

Mr. MCCOLLUM. We have been taking and are taking aggressive action to maintain the security of our networks and infrastructure and to improve those on an ongoing basis. We, in fact, had many actions underway in areas associated with the recommendations of the GAO report prior to the GAO's audit, and we are continuing to move ahead and to take actions on those areas. So we are committed to strengthening on an ongoing basis in a continuous improvement fashion and in a prioritized fashion all of the defense in-depth approach and infrastructure to guard against cybersecurity threats.

Ms. JACKSON LEE. Mr. McCollum, do you think you are going fast enough?

Mr. MCCOLLUM. Yes, I do. I believe that we have taken much action on this issue, and we continue to move ahead.

As Chairman Kelliher noted in his testimony, in order to aggressively move against these threats, we have to understand the threats, understand the issues involved and the mitigation strategies and move quickly to implement those, and that is what I believe we are doing. The GAO report is beneficial to us in terms of clarifying some of the issues around compliance and mitigation strategies, and that is very helpful to us.

Ms. JACKSON LEE. Let me thank you because I have the three witnesses, and I must move quickly, but I do not think, from my perspective, we are moving fast enough and you are moving fast enough.

I know that the representative from the GAO probably does not want to comment—and if you do, please do, but let me just say, do you see the landscape of utilities moving fast enough, from your perspective?

Mr. WILSHUSEN. Overall, I cannot really comment on that because the scope of our work dealt with just TVA.

Ms. JACKSON LEE. Do you see them moving fast enough?

Mr. WILSHUSEN. We have received the responses to our recommendations and the actions that we recommend they do. We have not yet verified their assertions. What we have at this point are assertions.

Ms. JACKSON LEE. And you will provide us a report on that. Was the response timely?

Mr. WILSHUSEN. Yes.

Ms. JACKSON LEE. Thank you.

Mr. Sergel, in light of the unfortunate misstatements that have occurred from the reliability corporation, do we need—well, I am not going to ask whether you need it.

Wouldn't it be helpful to have incentives that were fairly strong, that were fairly harsh about compliance?

Mr. SERGEL. We have standards that we have put in place, and we will enforce them up to the $1 million a day per violation, so we will do that.

I think what is clear to me—and it was clear before, but it is even more so after today—is that, as to the particular nature of our organization, setting standards in an industry public way is not adequate to deal with the issues that have been presented by this committee.

Ms. JACKSON LEE. Maybe your enforcement is not adequate as well.

Mr. SERGEL. Our enforcement of what we have will be as it is limited by the law. Today, it is limited by the law.

Ms. JACKSON LEE. Maybe the law needs to be expanded.

I will conclude, Mr. Chairman, by asking the FERC chairman, and will thank him for his presence here.

Give me a little bit more detail on how you work closely with the Department of Homeland Security. Are you all in periodic dialog? Is there oversight that is done in a combined method? What is your assessment of the grid from your regulatory perspective?

Would you see the value, if you will—and I guess I am asking a regulator because you are civil, if you will—for criminal penalties for those who violate and/or for those who are not adhering to the urgency of this matter?

Mr. KELLIHER. We coordinate with the national security agencies, including Homeland Security, the Department of Defense, the Department of Energy, and others, really, more in the area that is the focus of the hearing today—in the area of cybersecurity—than on other reliability issues.

I just want to reassure you that we can impose penalties for violations of cyber standards as well as other reliability standards. We can impose civil penalties up to $1 million per day per violation. I do not think maximum penalties will be the norm for all reliability violations. I think we would tend to reserve them for the most serious violations. We also want to know not just whether a violation occurred but why it occurred. We are really in the first stages.

Reliability standards became enforceable on June 18 of last year. So we have had less than 1 year of experience with mandatory reliability standards. I think we are developing enforcement programs at the regional level. We have a process that is slow, but it is designed to be slow, frankly, by Congress in the 215 process. That is what we think does not work so well with this cyber threat, and there is the possibility of criminal penalties as well for violations of the Federal Power Act.

Ms. JACKSON LEE. Mr. Chairman, I will yield back with a commitment to review with you these standards that you have brought to our attention. I, frankly, believe that there is the framework of reliability, and then there is the framework of piercing the system by those who would desire to do us harm. That, I guess, is the question I raise, which is whether or not the system is secure enough to rebuff that and whether or not we need to expand the concept of reliability to the concept of rebuffing and intrusion

through cybersecurity and otherwise and whether or not the penalties, whether by the Federal Power Act, are criminal.

I am not trying to lasso you in, but I am trying to emphasize the urgency and the importance of such as to whether or not they are sufficient, as to whether or not the industry is listening, as to whether or not the industry is moving fast enough, and as to whether or not the industry realizes that their challenge is alongside of reliability. It is life and death for Americans who are impacted by your industry.

With that, Mr. Chairman, I yield back. Thank you, and thank you to the ranking member for your courtesies.

Mr. LANGEVIN. I thank the gentlelady for her questions and for her input.

Clearly, this is an area where, I believe, stronger authorities, more comprehensive authorities are needed. I certainly look forward to working with you and with the members of this subcommittee and with the members of the full committee to see how we strengthen those authorities. It is not just enough to have some standards in place; they have to be the right standards. If they are not broad enough or if they are not strong enough—and that is what I believe is the case here—then they do not go far enough. That is why I have stronger confidence in this, in these standards, and the sooner we can move in that direction in adopting those standards, the better off we will be.

These are the kinds of things that keep me up at night, our electric grid, which we all rely on for our way of life, for our national security. Our families depend on the reliability of the electric grid. When we identify a vulnerability such as has been identified in this data threat and particularly in the Aurora threat, it is something that we need to move aggressively to close. This is, again, one of those things of many that this subcommittee deals with that keeps me up at night, and I am not going to be satisfied until we have aggressively moved to close the vulnerability and that our electric grid is 100 percent secure.

With that, the vote has been called. I want to thank the members for their questions. I want to thank the witnesses for their testimony.

Members of the subcommittee may have additional questions that they would ask of the witnesses, and we would ask that you respond expeditiously in writing.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 3:40 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JAMES R. LANGEVIN FOR HONORABLE JOSEPH T. KELLIHER, CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION (FERC)

Question 1. One of our witnesses from the October panel, Joe Weiss, recently commented in the press that "some generation managers considered NERC Reliability Standard compliance a 'game' to remove assets from the standards definition without addressing the reliability threat." For instance, according to Weiss, one manager of a coal-fired power plant was specifically charged by his upper management to ensure that his plant was not considered a critical cyber asset. Another plant manager whose plant had black start capability was subject to CIP–002; however, the company considered it more cost-effective to simply remove its black start capability. They determined that the cost of NERC Reliability Standard compliance, and possible fines, was too much for their facilities. Is there concern on your part that this is becoming a compliance game? What are you preparing to do to address this problem?

Answer. In Order No. 706, issued in January 2008, the Commission directed two actions to ensure proper identification of critical assets. First, we believe that a lack of uniformity in the performance of risk-based assessments of critical assets could make it difficult to compare companies and to check for adequate critical asset lists. Therefore, the Commission directed NERC to develop guidance on the development of a risk-based assessment methodology to identify critical assets. NERC has that effort underway and is expected to post a draft for comments in the fourth quarter of 2008. Second, we directed NERC to revise the reliability standards to require an oversight mechanism for an entity with a wide-area perspective to examine the critical asset lists in order to ensure critical assets were listed. Upon identifying a missing critical asset, the oversight entity could require that the missing asset be added to the list and protected according to the CIP reliability standards. This review procedure will be developed through NERC's reliability standards development process and is expected to be filed for the Commission's review in the second quarter of 2011. Also, the Commission intends to spot check critical asset lists and their determinations by actively participating in some compliance audits of the CIP reliability standards. This is the most direct way for the Commission to not only examine the specific details for the company under consideration, but also to assess the effectiveness of the critical asset identification requirement.

Question 2. Are you familiar with the Aurora mitigation technology that is manufactured by Cooper Industries? Do you know how many companies have purchased this technology? In conversations with industry owners and operators, have you gathered an understanding of how many people have purchased this technology?

Answer. The Commission is aware of the Cooper technology. Based upon discussions with industry members, Commission staff believes that the technology is not being widely used by industry. Their use is limited by industry's need to test the reliability and operation of the devices, as well as by supply issues.

Question 3. Under the Cyber Initiative, all Federal agencies will use a service provided by the US–CERT known as EINSTEIN to monitor their connections to the Internet. EINSTEIN is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. As a Federal entity, the TVA already deploys several EINSTEIN boxes on its networks to monitor traffic. TVA also reports computer incidents to the US–CERT. In the future, do you envision a role for the Federal Government to provide a similar monitoring service for the private sector? To what extent has FERC had these conversations with NERC, DHS, or other intelligence agencies?

Answer. To date, FERC has not been involved with the EINSTEIN project and has not had discussions with NERC, DHS, other intelligence agencies, or TVA about the subject. I note, however, that during the course of the Commission's rulemaking regarding proposed Critical Infrastructure Protection reliability standards and dur-

ing our attempts to assess industry's mitigation steps regarding the Aurora vulnerability, industry has expressed very strong concerns about sharing sensitive security-related information with Federal entities, since the latter have limited legal authority to ensure that information is disclosed only to those who have a need to know the information.

Question 4. Please elaborate on your request for new authority. Would this require legislation? What intelligence agencies would be involved? What is the next step for requesting or establishing this authority?

Answer. I believe new legislation is needed to protect the grid against cyber security threats, given the nature of these threats. I anticipate that the Commission would coordinate with other Federal agencies, as appropriate, such as the Department of Energy, the Department of Defense, the Department of Homeland Security, the Central Intelligence Agency, the National Security Agency, or the Federal Bureau of Investigation. We have been engaging in discussions with affected entities to get input as we consider how to craft legislation appropriately. We have received constructive input from these discussions and are incorporating that input into draft legislative text.

Question 5. In your opinion, do America's intelligence agencies have adequate situational awareness throughout the public and private sector to provide FERC with the appropriate intelligence that would allow FERC to immediately issue temporary mandatory reliability standards to prevent or mitigate a cyber attack launched against the Nation's bulk power system? If not, what could be done to better improve this situational awareness?

Answer. I believe that the intelligence agencies are best suited to assess adversaries, their capabilities, and their intents. The Commission has the knowledge and experience necessary to issue orders addressing needed reliability measures or actions. To the extent feasible, the Commission plans to consult with the relevant entities in order to gain their input regarding the design and implementation of any measures or actions needed to prevent or mitigate a cyber attack launched against the Nation's bulk power system.

Question 6. An article in the National Journal dated May 31, 2008 suggests that the Chinese government may have been responsible for the 2003 New York City blackout and the 2008 Florida Power and Light blackout. Please provide a detailed narrative explaining your position on this article. Please also explain whether such an attack could potentially be carried out. Please explain the cause of the 2008 Florida Power and Light blackout.

Answer. The Commission took part in the investigation and subsequent report on the 2003 blackout. In summary, the Security Working Group analysis provided no evidence that a malicious cyber attack was a direct or indirect cause of the August 14, 2003, power outage.[1] The Commission has no reason to think otherwise today. As for the 2008 Florida blackout, on March 19, 2008, the Commission initiated a non-public, formal investigation into whether any mandatory Federal reliability standards were violated during the Florida blackout. Because the investigation is ongoing and the information gained during the investigation is still non-public, I cannot discuss any causes of the Florida blackout at this time.

Question 7. A common criticism of the NERC standards is that there is not an adequate definition of critical cyber assets for CIP–002, and, as a result, many companies are struggling to determine exactly what is/is not covered under the reliability standards. To what extent has FERC engaged industry in this discussion? What is your guidance to the industry?

Answer. NERC's Glossary of Terms Used in Reliability Standards defines critical cyber assets as cyber assets "essential to the reliable operation" of critical assets. Cyber assets are defined as "[p]rogrammable electronic devices and communication networks including hardware, software, and data." As a result of these definitions, the identification of critical cyber assets involves a two-step process. First, the critical assets must be identified. Then, the associated critical cyber assets must also be identified. Most of the discussions between industry and the Commission on this process have focused on identifying critical assets. See the response to question one above. Regarding the second step, most of the discussions on that aspect of the process have been about the "data" component. That discussion culminated in the Commission's direction in Order No. 706 that NERC consider the designation of various types of data as a critical asset or a critical cyber asset. We also directed NERC to develop guidance on the steps that would be required to apply the CIP reliability standards to such data and to consider whether this also covers the computer systems that produce the data. The Commission also expects that best practices used

[1] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, page 132.

to identify critical cyber assets will be identified during the process of auditing responsible entities for compliance with CIP–002. At that point, the Commission will consider whether additional guidance is called for, or whether the reliability standard needs to be modified.

Question 8. Does FERC have the authority to require companies operating on the bulk power system to undergo "red team" efforts involving remote or onsite attackers? Does FERC have any, operational authority to run "red team" exercises against these companies?

Answer. The CIP reliability standards require responsible entities to conduct vulnerability tests, but not actual "red team" efforts. In theory, a reliability standard could require a "red team" exercise, but there would be associated reliability risks with conducting such exercises. The Commission does not have authority to run such "red team" exercises against industry companies.

Question 9. The Nuclear Regulatory Commission documents all unusual cyber-related events, in contrast to non-nuclear electric facilities that do not make these events public. Does FERC intend to create a catalogue of events on grid facilities to allow for the monitoring of this kind of activity? If not, why not?

Answer. The Commission has no plans at this time to create a public catalog of cyber security incidents. The CIP reliability standards do require responsible entities to report cyber security incidents to the electricity sector information sharing and analysis center (operated by the North American Electric Reliability Corporation), but that information is not all public. At this point, the Commission is more focused on having incidents reported rather than making them public. In fact, the Commission's Order No. 672 indicated a preference for keeping proceedings involving a cybersecurity incident nonpublic because it is possible that bulk-power system security and reliability would be further jeopardized by the public dissemination of information involving incidents that compromise the cybersecurity of a specific user, owner or operator of the bulk-power system. If such information is made public, careful attention will be necessary to be sure sensitive information that could jeopardize the reliability of the bulk-power system is not disclosed.

QUESTIONS FROM CHAIRMAN JAMES R. LANGEVIN TO RICHARD SERGEL, PRESIDENT AND CEO, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

JUNE 23, 2008

Question 1. For the record, please provide a detailed timeline that explains the steps that you took to distribute the industry survey regarding the Aurora mitigation. Please note the discrepancies that were discussed during the hearing, and provide explanations for those discrepancies.

Answer. The responsibility to provide consistent, coordinated, clear and effective communication lies entirely with NERC. We apologize for the confusing, unclear, and misleading communications with the subcommittee. A detailed timeline that describes the steps taken by NERC to distribute the October 19, 2007 written survey to the industry regarding the implementation of the mitigation measures contained in the June 21, 2007 ES–ISAC Advisory is attached (Attachment 1).

The discrepancies discussed during the May 21 hearing appear to us to fall into two categories: (1) the timing and means by which NERC assessed the industry's compliance with the June 21 Advisory, and (2) the representation to the subcommittee of NERC's assessments of compliance with the Advisory. These are discussed below, beginning with the October 17 hearing.

A. The October 17, 2007 testimony of David Whiteley regarding NERC's assessment of the industry's implementation of the mitigation measures identified in the Advisory.

At the October 17 hearing, Chairman Langevin told Mr. Whiteley that staff of the Department of Homeland Security had described to committee staff "a survey that NERC sent out in August 2007 to determine how many owners and operators were implementing the mitigation efforts" identified in the June 21 Advisory. Mr. Langevin then asked Mr. Whiteley to "describe the survey and tell us its findings."

Mr. Whiteley failed to inform Mr. Langevin that the Chairman's understanding was incorrect and that NERC had NOT sent out a formal written survey of the industry's compliance with the Advisory in August 2007. As depicted on the timeline, NERC had prepared a formal survey that was approved by NERC senior management. NERC received FERC's assent to distribute that survey in August. However, the survey had not been sent out at the time of the hearing. By not advising the subcommittee that no written survey had been sent out, Mr. Whiteley's testimony was inaccurate and misleading.

Mr. Whiteley responded as though the survey had been distributed, stating that it was a follow-up to the "guidance that was issued earlier in the spring," and that "we've determined that approximately, at this point, 75 percent of the transmission grid has either taken appropriate actions or is in the process of implementing those actions." This discussion of "75 percent of the transmission grid" appears to have been misunderstood by the subcommittee. Mr. Whiteley's use of the 75 percent number referred to the portion of the transmission grid owned by companies that had been contacted by NERC staff and for which Mr. Whiteley believed that mitigation measures had been implemented, based on information provided to Mr. Whiteley by NERC's Manager, Situation Awareness and Infrastructure Security (NERC SAIS Manager). Mr. Whiteley did not intend by use of this number, as the subcommittee may reasonably have assumed, to state that 75 percent of all transmission users, owners or operators had implemented mitigation measures.

In response to a further question from Chairman Langevin at the October 17 hearing, Mr. Whiteley stated that NERC had "hard data" showing the extent of the industry's compliance with the June 21 Advisory.[1] The basis for Mr. Whiteley's response to Chairman Langevin's inquiry was an e-mail sent to NERC management on October 10 by the NERC SAIS Manager that reported on the status of implementation of the short- and mid-term mitigation measures recommended in the Advisory. That e-mail stated that the "data" gathered from voluntary submissions and from discussions with NERC Critical Infrastructure Protection Committee (CIPC) contacts at "the large transmission owners and operators" "covers at least 75 percent of the BPS in the U.S."

Because the only information NERC had at the time of the October 17 hearing was the information the NERC SAIS Manager obtained in a few voluntary written submissions and his informal discussions with company representatives, it was inaccurate to characterize the information as "hard" or "direct." A complete answer would have described what had been done, i.e., to tell the subcommittee that NERC staff conducted discussions with industry representatives that collectively own or operate 75 percent of the total transmission grid. The response also should have said that NERC had not verified the reports received in these discussions regarding the status of mitigation measures.

B. Responses to follow-up inquiries from the committee.

In responding to follow-up questions for the record of the October 17 hearing on November 20, NERC submitted a copy of the formal written survey sent out on October 19 to assess the status of compliance with the mitigation measures recommended in the Advisory. On December 5, NERC provided a narrative overview of the implementation of the mitigation measures recommended in the June 21 Advisory, along with the survey responses themselves (with the identity of the specific respondents concealed), in response to a further request of the subcommittee.[2]

The narrative overview provided on December 5 stated that:

> 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 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 percent of the transmission grid had received mitigation measures or such measures were in progress.

Following this submission to the subcommittee, the subcommittee counsel contacted NERC on December 6 to schedule a face-to-face meeting and request further detail regarding the September/October "initial assessment" of the industry compliance with the mitigation measures in the June 21 Advisory. On December 20, NERC representatives met with subcommittee staff and provided a letter in response to the staff's request for "a list of phone conversations and meetings that

---

[1] "Mr. Langevin: . . . 75 percent you say is in compliance, . . . this is not just anecdotal? You are talking about this as hard answers to the issue of having implemented all the mitigation strategies?" "Mr. Whiteley: This is a follow-up with most of the large utilities in the country and many of the intermediate-size utilities as well. And it is hard evidence or hard data that we've asked, and they've explained what's been done. So we have direct information."

[2] This further request was made on November 16 in a letter from Chairman Langevin to Mr. Sergel. The narrative overview document was entitled "Assessment of the Implementation of the Mitigation Measures recommended in the June 21, 2007 ES–ISAC Advisory."

these individuals had with sector entities. Please include dates and any information/notes prepared."

The December 20 letter, submitted by NERC's SAIS Manager, stated that "[a]fter issuance of the Advisory on June 21, 2007, I communicated regularly with industry representatives to explain and discuss the Advisory. Beginning in September and October, my communication efforts shifted from explanation of the Advisory to determination of how well the Advisory was being implemented. A reconstructed list of the discussions, to the best of my recollection, is listed below." Contacts made at the September 27–28 CIPC meeting in St. Louis were listed in this letter, as well as phone calls with other individuals conducted in September and October. The letter also provided copies of the three voluntary written submissions that NERC received. In addition to this written response, NERC representatives and subcommittee staff discussed the nature of the information gathering process prior to the distribution of the written survey on October 19.

Committee Chairman Thompson and subcommittee Chairman Langevin sent letters on January 8, 2008 to attendees at the September 27–28 CIPC meeting identified in the December 20 letter. The letter from Messrs. Thompson and Langevin said:

> "The committee recently requested and received documentation from the North American Electric Reliability Corporation (NERC) to help determine the extent of the sector's efforts to implement the security recommendations contained in the June 21, 2007 NERC Advisory. According to these documents, NERC staff met with you individually at the NERC Critical Infrastructure Protection Committee meeting, held from September 27–28 in St. Louis, Missouri, to discuss your company's implementation efforts.
>
> "During this meeting with NERC staff, you answered questions regarding the clarity of the recommendations contained in the NERC Advisory, the extent of your company's efforts to mitigate the Aurora vulnerability, and existence of your company's cybersecurity training program for employees. Please provide the committee with a detailed narrative explaining this discussion with NERC."

The January 8 letter reveals the subcommittee's view that the discussions at the CIPC meeting in St. Louis were more formal than they were. As NERC's December 5 submission indicated, no formal survey was conducted. Although NERC's December 5 narrative overview indicated that information was gathered from sector entities "in phone conversations and at meetings," NERC understands from subcommittee counsel that the subcommittee's January 8 inquiry was sent only to the CIPC meeting attendees.

The responses provided to the subcommittee's January 8 letter do not support Mr. Whiteley's reference to "hard data" showing compliance by 75 percent of the transmission grid in his response to Chairman Langevin at the October hearing. However, several of the responses sent to the subcommittee do describe company interactions with NERC staff at the CIPC meeting and discussions of company compliance with the recommended mitigation measures:

- One company stated the Aurora advisory was discussed during the general CIPC meeting in September, not in an individual meeting. It stated that at the initiation of NERC there was discussion by many attendees in the open forum about the response of their companies to the NERC advisory; details of the response to the advisory were not provided at the meeting due to the sensitive nature of the information on mitigation of the vulnerability.
- Another company submitted detailed affidavits, which reported, among other things, that the company representative recalled talking to NERC staff about the Aurora vulnerability and the company's efforts to address it. The company representative also told NERC that the company had taken action to eliminate the Aurora vulnerability.
- Another company stated it told NERC it had addressed the vulnerability.
- A few companies reported that there was some (limited) discussion of the Aurora vulnerability at the CIPC meeting.

Taken together, the responses the subcommittee received to its January 8 letter would not lead to a conclusion that there was "hard data" for David Whiteley to rely on at the October 17 hearing.

C. Other missed opportunities to correct the record and clarify the status of the implementation of the mitigation measures contained in the Advisory.

- *October 15.*—NERC received a request from subcommittee staff for information about the August 2007 survey. NERC failed to advise the staff that a survey was NOT sent in August 2007.
- *November 20.*—NERC submitted responses to the subcommittee's follow-up questions from the October 17 hearing. The first question asked, "What were

the results of the August 2007 NERC survey sent to owners and operators regarding the status of the sector's implementation of the Aurora mitigation efforts," and also requested a copy of the survey and a narrative of the results. The NERC response enclosed a copy of the October 19 survey and a narrative of the results, as requested, but failed to advise the subcommittee that a formal written survey was NOT sent out in August. By letter dated December 12, 2007 and delivered on December 14, NERC clarified its responses for the record of the October 17 hearing and stated definitively that no survey was sent in August 2007.

- *December 5.*—NERC's response to Chairman Langevin's November 16 letter requesting a copy of the survey and its results failed to clarify that the reference to 75 percent of the grid having mitigation measures completed or in progress was a reference to the percentage of the physical transmission grid, by ownership, not to the percentage of users, owners or operators that had completed mitigation measures.

In summary, NERC did not rigorously survey the implementation of the mitigation measures it had recommended and did not accurately communicate with the subcommittee about what NERC had done. As I testified on May 21, 2008, NERC now has a structure in place—with a formal FERC-approved, three-level system of alerts; a comprehensive list of owners, operators and users of the bulk power system; and mandatory reporting regarding implementation of recommendations and essential actions—to assure that a rigorous and timely analysis of the implementation of recommended measures in future Advisories will be conducted.

Question 2. Publicly and privately owned infrastructures on the grid are so interconnected, weak security controls in one utility can pose harm to another utility that shares a connection. Yet publicly and privately owned infrastructures are subject to different security standards. According to a NIST-sponsored review published in March 2007, an organization conforming to the baseline set of security controls in PS 800–53 will also comply with the management, operational and technical security requirements of the NERC Reliability Standards, though the converse may not be true. For instance, the NERC Reliability Standards allow for the exclusions of telecommunications and distribution equipment from the "critical assets" list. Under the SP 800–53 requirements, however, there is no similar exclusion. This committee—along with NIST and GAO—has suggested that the NERC standards should be more aligned with the NIST 800–53 standards that apply to federally owned infrastructure. What steps are being taken to transition the NERC Reliability Standards toward NIST? Why shouldn't the scope of CIP–002 be changed to include "all equipment that is electronically connected"?

Answer. In Order 706, FERC directed NERC to consult with Federal agencies on the effectiveness of NIST standards and implementation issues, and using the standards development process, address any provisions that would better protect the bulk power system.

In response to this direction, a Standard Authorization Request (SAR) was initiated and posted for a 30-day public comment period from March 20 to April 19, 2008. A SAR drafting team comprised of well regarded subject matter experts from a broad range of industry segments was assembled to review and respond to the comments received during that initial SAR posting. This team includes a representative from a Federal agency that must comply with both NERC and NIST standards.

Presently, the drafting team is considering all comments on the SAR, including those submitted by NIST. The drafting team must prepare written responses to all comments. The end work product will be a SAR that specifies the work scope for the Standard Drafting Team that will ultimately develop the revisions to the standards.

NERC management has formally invited NIST to continue its participation in the standards drafting effort as a formal team member. NIST has agreed.

Regarding the scope of CIP–002, it does not include "all equipment that is electronically connected" for jurisdictional as well as reliability reasons.

- Section 215 of the Federal Power Act limits the ERO's jurisdiction to bulk power system users, owners, and operators. By definition, the bulk power system excludes distribution assets. Similarly, telecommunications common carriers are not users, owners or operators of the bulk power system.
- Section 215 of the Federal Power Act also defines a reliability standard as a requirement that provides for the reliable operation of the bulk power system. The process required in CIP–002 determines which assets of the bulk power system provide for its reliable operations. Those assets are identified through an analysis of the impact that the loss of an asset poses to reliable operation

of the bulk power system. Those assets found to provide for the reliable operation of the bulk power system are critical assets.

- The CIP–002—CIP–009 standards drafting team intentionally focused requirements on cyber assets that were: (1) Essential to the reliable operation of critical assets; (2) whose impact to reliable operation of the bulk power system, if compromised, could be significant; and, (3) had a great number of attack vectors. Cyber assets meeting these criteria are critical cyber assets.

  An electronic perimeter, as required in CIP–005, shields critical cyber assets from potential adverse impacts from external sources such as non-critical cyber assets.

NERC's CIP standards represent the first set of reliability standards requiring a uniform level of cyber security for all users, owners, and operators of the bulk power system. These standards intentionally focus the efforts of those users, owners, and operators on assets most critical to the reliable operation of the bulk power system. The CIP standards expanded the scope of assets beyond those addressed in Urgent Action 1200. The process of focusing resources on those assets with the greatest impact on reliable operations, and protecting them as required in the remaining standards (specifically including the provision of electronic security perimeters), mitigates the need for protection of every other asset that is connected to them. Subsequent cyber security standards may include other assets within the scope of the ERO's jurisdiction.

Question 3. In April 2000, Vitek Boden, an employee at an Australian firm that installed SCADA radio-controlled sewage equipment, packed his car with stolen radio equipment attached to a computer. He drove around issuing radio commands to the sewage equipment that resulted in sewage spills. This is the first widely known example of someone maliciously breaking into a control system. Please explain how a company demonstrating auditable compliance with the NERC CIP standards prevents this incident from occurring, when they are not required to follow any mandatory reliability standards for telecommunications equipment.

Answer. If the referenced event had occurred on the North American bulk power system, it would represent a breach of the "electronic security perimeter," which is required by present NERC Cyber Security standard CIP–005–1. In this particular instance, communications from an invalid source were allowed to be transmitted to, received by, and acted upon by the control equipment for the sewage system. As required by the NERC standards, the system control equipment would be contained within an electronic security perimeter. Any communications across that perimeter (wireless or not) would have to pass through the protections of the electronic security perimeter prior to being sent to the system control equipment.

The electronic security perimeter is implemented using the concept of "mutual distrust", as described in the requirements of CIP–005, which includes requirements to implement a "deny by default" stance, and requires "specific access permissions be specified". It also requires "only ports and services required for operations and monitoring" be allowed to cross the perimeter. In the Boden example, had CIP–005 been implemented, the perimeter controls would have been implemented to disallow control actions from being delivered from addresses not associated with the control center, and would therefore be flagged as suspicious, requiring investigation and reporting of said suspicious activities following the requirements of NERC Standard CIP–008–1.

In this particular case, if the entity in the Boden example followed the change management procedures required by CIP–003–1, the equipment disposal procedures required by CIP–007–1, and the access control review and revocation requirements required by CIP–003–1, CIP–004–1, CIP–005–1, CIP–006–1, and CIP–007–1, the stolen equipment used by Mr. Boden would have been removed from the valid access list, and the illicit communications would have been disallowed at the perimeter.

Question 4. You stated during the hearing that NERC "will push as far as we can to get as much done on the telecommunications side within the standard." However, as it currently stands, the NERC reliability standard excludes telecommunications and non-routable protocols and does not explicitly address wireless systems in the definition of "critical cyber assets." What steps is NERC taking to ensure that telecommunications equipment is covered in the next revision of the standard?

Answer. Section 215 of the Federal Power Act limits the scope of FERC's and the ERO's jurisdiction to only the bulk power system. FERC and NERC standards cannot enforce requirements upon telecommunications providers and their equipment.

However, a Standard Authorization Request (SAR) drafting team is currently considering alternative approaches to address how data and information are received through wired and wireless telecommunications equipment owned or operated by owners, operators and users of the bulk power system. Specifically, it is discussing the merits of protecting the data being transmitted, rather than protecting the

transmission media. This change in philosophy from the initial set of standards will extend the protections to wireless data transmission, will lessen the need for requirements for protecting the transmission media itself, and allow the standards to be enforced regardless of whether the telecommunications system is owned by the jurisdictional entity or a telecommunications provider.

The draft SAR was posted for a 30-day public comment period from March 20 to April 19, 2008. The SAR drafting team met on May 5–6, 2008 to consider comments and refine the SAR. Further refinement took place during a conference call and WebEx on May 30, 2008. Continued refinement is scheduled to take place on a July 2, 2008 conference call and WebEx. The end work product will be a SAR that specifies the work scope for the Standard Drafting Team that will ultimately develop the revisions to the standards.

Question 5. Are you familiar with the Aurora mitigation technology that is manufactured by Cooper Industries? Do you know how many companies have purchased this technology?

Answer. Yes, NERC is aware of this technology. The U.S. Department of Homeland Security informed NERC of the development of the device. NERC subsequently invited Richard Hein of Cooper Industries to participate in a panel discussion during the December 13, 2007 Critical Infrastructure Protection Committee meeting in Orlando, Florida, where he presented information about the rotating equipment isolation device (REID). NERC has supplied Cooper Industries' Web site information to Ameren Corporation who had asked for assistance to learn more about the device.

According to Cooper Industries, only the Department of Defense, to date, has purchased REID devices. The number of devices sold was not disclosed to NERC staff.

Question 6. Under the Cyber Initiative, all Federal agencies (including, for instance, the TVA) will use a service provided by the US–CERT known as EINSTEIN to monitor their connections to the Internet. EINSTEIN is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. As a Federal entity, the TVA already deploys several EINSTEIN boxes on its networks to monitor traffic.

TVA also reports computer incidents to the US–CERT. In the future, do you envision a role for the Federal Government to provide a similar monitoring service for the private sector? To what extent has NERC had conversations with either DHS or FERC about this issue? To what extent have you discussed this possibility privately with your members?

Answer. Neither the Department of Homeland Security, of which US–CERT is a part, nor FERC has briefed NERC management or ES–ISAC staff about a service named EINSTEIN. NERC has not consulted subject matter experts within industry on the subject of EINSTEIN or the potential benefits this government-run monitoring service could provide for the electricity sector.

NERC is aware that in 2004 DHS sponsored a project involving several ISO/RTOs to evaluate intrusion detection system (IDS) tools and analytical capabilities. The 1-year pilot, called the Cyber Log Analysis Project, was conducted by EWA-Canada and Dartmouth College. The results suggested that aggregation of IDS log data could be useful in improving the incident and warning (I&W) capability in the electricity sector and recommended that DHS continue developing more sophisticated and automated shared information analysis techniques and develop open source software for this purpose.

NERC's Reliability Standard CIP–005 requires monitoring of network traffic across the electronic security perimeter to provide early warning of possible unauthorized access attempts. As such, NERC would be open to exploring with FERC and DHS the benefits of implementing an EINSTEIN-like project within the electricity sector.

Question 7. To what extent has NERC involved either NIST or the ISA in the standards-setting process? Will you be inviting individuals from both entities to participate in the new CIP–706 Standard Drafting Team (SDT)?

- Answer. ISA became involved with the standards development effort in 2005 through review and comment on draft three of CIP–002—CIP–009.
  The co-chair of ISA SP99 is a named, formal member of the drafting team charged with scoping the future development of the CIP standards pursuant to FERC Order 706. NERC management has formally invited the co-chair to continue ISA SP99's involvement in the CIP standards drafting process. He has agreed to participate.
- NIST's participation in NERC's standards-setting process began this year. NIST has contributed comments to the current scoping effort, which must be considered and responded to in accordance with the NERC process. Those comments are attached (Attachment 2).

NERC management has formally requested NIST's continued involvement in the CIP standards drafting process. NIST has agreed to participate.

- Federal agencies required to follow both NIST guidance and NERC Standards have been involved in the Cyber Security standards setting process since 2003.
  - An employee of Western Area Power Administration was a named, formal member of the CIP–002—CIP–009 standards drafting team.
  - Bonneville Power Administration, Tennessee Valley Authority, United States Bureau of Reclamation, and the Western Area Power Administration have participated in the review and comment process for CIP–002—CIP–009. The United States Army Corps of Engineers provided comments, as well.
  - An employee of the U.S. Bureau of Reclamation is a named, formal member of the drafting team charged with scoping the future development of the CIP standards pursuant to FERC Order 706. NERC management has formally requested the Bureau's continued participation in the CIP standards drafting process.

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION

2007	
June 7	FERC issues order on NERC compliance filing that states, "the Commission believes that NERC should issue an operations and equipment alert requiring specific actions only under NERC's remedial power."
June 21	NERC acting as the ES–ISAC issues advisory regarding the Aurora Demonstration Test following discussions with Department of Energy and Department of Homeland Security. At the direction of DOE and DHS, the advisory is designated "For Official Use Only". The Advisory states 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.
July 9	NERC files request for clarification or rehearing of FERC's June 7 order stating that NERC should issue an operations and equipment alert requiring specific actions only under NERC's remedial power.
July 30	NERC General Counsel (GC) prepares draft cover letter for survey.
August 1	Discussions between NERC staff and FERC staff regarding the survey. NERC agrees to coordinate with FERC before sending out the survey.
August 3	NERC GC sends a copy of a draft follow-up survey and cover letter to FERC (to the Director, Office of Electric Reliability (Director), and to the then-General Counsel) via e-mail. NERC proposes that the ES–ISAC would distribute the survey and the cover letter, to be signed by the NERC President and CEO. The draft survey proposes a response date of August 24; NERC informs FERC of its desire to send the survey out "by the middle of next week" [week of August 6]. The e-mail implemented NERC's commitment made August 1 to coordinate with FERC before sending out the follow-up survey. NERC solicited FERC's suggestions on the draft letter and the survey. NERC also asked FERC staff "if you have had further thoughts about whether the ES–ISAC should send this letter."

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION—Continued

2007	
Sometime after August 3 and before August 15.	The Director of the FERC Office of Electric Reliability and the NERC CEO discussed the draft ES–ISAC cover letter and survey.
August 16	NERC's GC sends an e-mail to FERC's GC following up on the Director-CEO discussion.
August 21	NERC's GC and FERC's GC discuss FERC staff concerns with the proposed cover letter and survey.
August 21	E-mail from NERC GC to FERC GC acknowledges the Director's concerns regarding "the penultimate paragraph on the instruction sheet to the survey" dealing with the circumstances under which the ES–ISAC would make information available about the status of the mitigation efforts to government agencies.
August 21	NERC GC and FERC GC further discuss the survey/cover letter, and NERC GC recommends a modification to the confidentiality language in the survey instructions. According to an e-mail from the NERC GC to the CEO, the FERC GC said that the "edit solved the immediate problem and we can get the letter out." NERC's GC said that he would work with NERC's Manager, Situation Awareness and Infrastructure Security (SAIS Manager) on getting the survey out.
August 21	NERC's GC transmits the change in language worked out with the FERC GC to the NERC SAIS Manager via e-mail. The NERC GC advises the NERC SAIS Manager that the FERC GC "said that with the change, we can send out the letter." The NERC GC also advises that the proposed August 24 due date for the survey responses would need to be extended by a reasonable amount to account for the delay in distribution of the survey.
August 21	CEO comments on wording of the instructions to the survey in an e-mail to the NERC SAIS Manager, and approves the letter.
August 21	The NERC GC advises the NERC SAIS Manager that "I'm leaving this with you, unless you have further questions, or something else comes up."
September	NERC SAIS Manager has informal, off the record telephone conversations with representatives of major bulk power system entities regarding the implementation of the Advisory. No notes of the discussions were taken.
September 20	FERC issues order granting NERC's request for clarification that NERC has the authority to issue industry alerts in a broader set of circumstances than just violations of reliability standards. FERC requires NERC to change the term "Required Actions" to something else and imposes requirements that NERC must give notice to the Commission prior to issuing alerts and must report back to the Commission on the status of implementing the recommendations of the alerts.

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION—Continued

2007	
September 27–28	CIPC meeting in St. Louis. One agenda item during the meeting was a discussion of the June 21 advisory: "c) ES–ISAC report Stan Johnson 60 min 1. June 21, 2007 DPCD Advisory update—Stan Johnson a. Survey Results b. Status Update c. Lessons Learned—Discussion and Recommendation d. ES–ISAC Participation in TOPOFF 4." There was no systematic attempt to survey meeting participants on the extent of their compliance with the Advisory. "After extensive discussion, CIPC recommended the follow-up survey should be distributed using the NERC compliance registry as this is currently NERC's best mechanism to reach all affected entities." (Minutes of September 27–28 CIPC meeting.)
October 8	NERC SAIS Manager has an informal, off the record discussion of the implementation of the Advisory on a call with ERCOT. No notes of the discussion were taken.
October	NERC SAIS Manager has informal, off the record telephone conversations with representatives of major bulk power system entities regarding the implementation of the Advisory. No notes of the discussions were taken.
October 10	NERC SAIS Manager sends an e-mail to NERC's CEO, NERC's General Counsel, NERC's Executive Vice President, and NERC's Chief Information Officer setting forth the status of the mitigation measures contained in the Advisory. The e-mail reported:

"**Mitigation Measure**	**Status**
Short Term—0 to 60 days:	
1. Plan for taking immediate, drastic action.	100%
2.1.1 Security for remote access	100%
2.1.2 Personnel Security	85%
2.1.3 Sensitive Information	90%
2.1.4 Seal Off open ports	99%
Mid Term—60 to 180 days:	
3.1 Authentication	65%
3.2 Situation Awareness	30%
Long Term—180 days plus:	
4.1 Remote Monitor.	
4.2 Vendors.	
4.2.1 Separate Functionality.	

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION—Continued

2007	
	4.2.2 Seal Breaker Close Function. 4.2.3 Secure Firmware and Software. 5. Superfast Protective Device. 6. Shadow Device. 7. Government Intelligence Agencies. 8. CIP 002–009" The NERC SAIS Manager further advises in the e-mail that this information "has been gathered from voluntary submission by 10 entities (all major players) and from discussions with CIPC contacts at the large transmission owners and operators. The data is current as of last week. The data covers at least 75 percent of the BPS in the U.S." The NERC SAIS Manager's e-mail also states that no written survey had yet been sent out to assess the implementation of the measures in the Advisory: "I have not sent out the formal survey for the following reasons: 1. I do not have a good list to send this kind of survey to. 2. NERC received a great deal of criticism for how the initial advisory was distributed to and who it was not distributed to. Many key entities did not receive it until several weeks afterward. 3. I have been working with the [Regional Reliability Entities] and the trade associations to compile a list but it has not been successful. At the last CIPC meeting in late September, a consensus was reached to use the NERC Compliance Registry and I have been pursuing that option."
October 17	Subcommittee Hearing.
October 19	NERC, acting as the ES–ISAC, sends the Follow-up Survey to "Electric Sector Transmission Owner/Operators and Generation Owner/Operators," asking for a response by November 2. The survey was sent to "major entities in the bulk power system." The cover letter accompanying the survey recommends that a "coordinated effort be made at each entity to compile a single response rather than multiple responses from the same entity." The letter stated further that "The ES–ISAC is working with the regional reliability organizations, EEI, and the [Canadian Electricity Association] to deliver the survey instrument to the right people in the right entities."

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION—Continued

2007	
October 23	FERC requests approval from the Office of Management and Budget to send its own survey requesting detailed information on the status of implementation of the Aurora mitigation measures by owners, operators, and users of the bulk power system. NOTE: NERC did not learn of this request by FERC until December 5.
November 2	Deadline for responses to the October 19 survey. A total of 133 entities respond to the survey.
November 8	NERC circulates questions for the record submitted to David Whiteley as follow-up to the October 17 hearing. NERC GC designates responsibility for the draft responses among NERC staff.
November 9	Chairman Kelliher replies to an October 17 letter from the subcommittee. The letter notes that FERC had directed NERC to report to FERC on the level of compliance with future Advisories within 30 days. The letter discusses FERC's views of NERC's October 19 survey: "[a]lthough we support NERC taking the actions it believes are necessary as ES–ISAC, we do not believe NERC's survey provides sufficient information for the Commission to determine whether further action is appropriate. For example, it does not provide information on what facilities are the subject of the mitigation plans, what steps to mitigate the cyber vulnerability are being taken, when those steps are planned to be taken, and, if certain actions are not being taken, why not. Nor is it clear to the Commission that NERC has received a complete set of responses to its data request." FERC therefore planned to conduct its own survey that would "supplement NERC's action and provide more detailed information on which to assess the status of mitigation efforts." NOTE: NERC did not become aware of this letter until December 5.
November 15	NERC staff sends an e-mail reporting on a call on November 14 from subcommittee counsel requesting a face-to-face meeting and "a copy of all the docs we sent re: esisac cyber recs and surveys."
November 16	Chairman Langevin sends a letter to NERC CEO requesting the results from the ES–ISAC Advisory follow-up survey, with the response due by November 28. NOTE: The letter did not come to light until the CEO returned to the office on November 28. NERC subsequently received an extension of the deadline to submit the materials until December 5.
November 20	NERC submits responses to questions for the record to the subcommittee.

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION—Continued

2007	
December 5	NERC GC prepares draft cover letter for a second survey of the status of industry efforts to implement the Aurora mitigation measures, in preparation for coordination with FERC staff.
December 5	While edits were still being made on the NERC response to Mr. Langevin's November 16 letter, NERC staff obtains a copy of the letter dated November 9 from FERC Chairman Kelliher to the subcommittee in response to the October 17 letter [see November 9 entry above].
December 5	Based on information in Chairman Kelliher's November 9 letter, NERC General Counsel obtains a copy of FERC's request to OMB seeking approval to send survey to owners, operators, and users of the bulk power system requesting detailed information on the status of implementation of the Aurora mitigation measures. After discussions between NERC GC and FERC staff regarding the status of FERC's request to OMB, NERC's plans to send a second follow-up survey in December are put on hold, and references in the NERC response to the November 16 letter to the second survey are deleted.
December 5	NERC submits the final response to November 16 letter to the House Subcommittee, signed by David Whiteley: "Following the issuance of the Advisory, many of the larger transmission owners and operators were contacted by an ES–ISAC representative to help the ES–ISAC make an assessment of the response to the June 21 Advisory and measure the progress in completing mitigation. Additional entities made unsolicited information submissions to the ES–ISAC. Through this process, the ES–ISAC determined that approximately 75 percent of the transmission grid had mitigation measures completed or in progress. This was the basis for my testimony at the October 17 subcommittee hearing.

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION—Continued

2007	
	"A follow-up written survey to formally measure the progress in implementing the recommended mitigation measures was distributed to major entities in the bulk power system on October 19 and responses were requested by November 2. The following information regarding the October 19 survey is enclosed: (1) an overview of the implementation assessment process, which summarizes the survey responses; (2) a blank copy of the survey; (3) the forms supplied by the respondents; and (4) an alphabetical listing of the respondents. To preserve the security and confidentiality of this information, which is a commitment made to the respondents by the ES–ISAC, all entity identification was removed from these forms and a separate listing of the respondents was created. The information submitted confirms the conclusion reached by the ES–ISAC that 75 percent of the transmission grid has implemented the recommended mitigation."
December 6	Subcommittee staff sends an e-mail to NERC staff requesting times for a face-to-face meeting and asking NERC to bring to the meeting: "1. The name and position of the individual/s who conducted the 'initial assessment' on behalf of NERC in September/October; 2. A list of phone conversations and meetings that these individuals had with sector entities. Please include dates and any information/notes prepared; 3. The unsolicited reports issued to the ES–ISAC during this time, including the names of the sector entities who submitted the unsolicited reports."
December 14	Letter dated December 12, 2007 sent to the subcommittee by NERC Executive Vice President clarifying the question of when NERC's survey was sent (October 2007 not in August 2007) and apologizing for any misimpression that the November 20 response may have given regarding the timing of the written survey.
December 20	At a meeting with NERC representatives, subcommittee staff is given a letter from the NERC SAIS Manager formally responding to the 3 questions set out in subcommittee staff's December 6 e-mail. In response to question 2 (list of phone conversations and meetings that these individuals had with sector entities, including dates and information/notes prepared), the letter stated:

ATTACHMENT 1.—TIMELINE OF STEPS TAKEN BY NERC (AS THE ES–ISAC) TO DISTRIBUTE THE INDUSTRY SURVEY OF THE AURORA MITIGATION—Continued

2007	
	"After issuance of the Advisory on June 21, 2007, I communicated regularly with industry representatives to explain and discuss the Advisory. Beginning in September and October, my communication efforts shifted from explanation of the Advisory to determination of how well the Advisory was being implemented. A reconstructed list of the discussions, to the best of my recollection, is listed below." The list identified contacts made at the September 27, 28 CIPC meeting as well as phone calls with other individuals conducted in September and October.
December–January 2008	NERC learns from FERC staff that FERC has changed its plan to send the formal written survey regarding the status of Aurora mitigation measures to all owners and operators; instead, FERC teams are conducting interviews in the field with selected utilities to learn the status of their efforts to mitigate the Aurora vulnerabilities.

ATTACHMENT 2.—NIST COMMENTS ON STANDARDS DEVELOPMENT FOR FUTURE VERSION SAR (06/11/2008)

NIST agrees with the proposed changes in FERC Order 706 and proposes several additional items for consideration listed in the comments section of Question 5 of this comment form.

GENERAL COMMENTS SUMMARY

NIST believes that if the changes specified in FERC Order 706 and the recommendations below are implemented, NERC will have made a positive step toward making the CIPs commensurate with the NIST SP 800–53, Rev 2 moderate baseline. However, there are still differences in coverage and in the level of specificity of the security requirements that need to be addressed. NIST would also like to point out that many of the Federal agencies that own/operate industrial control systems in the bulk electric sector are classifying their systems as High impact systems that implement the High baseline requirements in SP 800–53. NIST is willing and has the resources to work on the NERC standards team in developing the next revision to the standard.

APPROACH

Critical Assets vs. Information System.—NIST understands that in the electric sector, protecting critical assets has been the predominant paradigm, but recommends for future revisions of the standards that an information systems approach rather than critical asset approach be considered.

Our rationale for this suggestion is as follows: While it is important to identify critical assets using a risk-based assessment methodology, NIST suggests that NERC consider applicability of the CIPs at an information system level rather than at the critical asset level. An information system view provides a more natural context for the application of information technology security across an industrial control system composed of multiple components, where some subset of the components is supported by information technology.

Under the current scope of the CIPs, all of the CIP security requirements would be applied to every critical cyber asset. In some cases, application of all of the CIP security requirements to a critical cyber asset may not make sense or may be excessive due to the nature of the asset. When an information system view is adopted, the CIP security requirements would be applied at the information system level, resulting in the allocation of CIP requirements to specific components. All components of the information system are not required to support every information system se-

curity requirement? Just those that are identified as a result of the requirement allocations; thus resulting in significant cost savings.

Using the information system view, there is no need to distinguish between cyber assets and critical cyber assets as all cyber assets within the information system are protected. Comments on Specific Requirements CIP 002 R3.1 NIST strongly recommends that a clear unambiguous definition of "routable protocol" be developed and, based on that definition, all routable protocols currently within the scope of the CIPs should be identified. All data encapsulated within a routable protocol should also be within the scope of the CIPs. CIP 002 R3.2 NIST recommends that "control center" should be replaced by "electronic security perimeter."

Nuclear Facility Exemption.—In reference to section 4.2.1 of each CIP, NIST observes that the electric side of nuclear power plants can have an impact on the bulk electric sector. NIST suggests that the continuity of power aspects of nuclear facilities should be included in the scope of these standards. Therefore NIST recommends that the exemption statement: "Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission be changed to—Specific systems that are regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission (e.g., safety systems)."

Wireless.—NIST observes that the CIPs do not sufficiently address the security of wireless technologies, which include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. There appears to be an assumption in the CIPs that communication occurs solely over media. Consequently, NIST recommends that a clear, unambiguous definition of wireless technology be developed and security requirements for wireless technologies be included in the CIPs.

Media Protection.—NIST recommends that the CIPs media protection requirements be expanded to cover all types of media. Because of the miniaturization and increased portability of digital media, protection of this media by a physical security perimeter is no longer adequate. Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). Information system media are also components of portable and mobile computing and communications devices (e.g., notebook computers, personal digital assistants, cellular telephones). The organization should have policy and procedures to protect and control information system media during transport outside the physical perimeter and restrict the activities associated with transport of such media to authorized personnel. For example, many organizations today prohibit removing laptop computers with unencrypted hard drives from the physical protection perimeter, and enforce this policy with unannounced inspection at the exits. Information system media is also a component of telephone systems that have the capability to store information (e.g., voice-mail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, policy should address the types of information stored on telephone voice-mail systems that are accessible outside of physically protected areas.

QUESTIONS FROM CHAIRMAN JAMES R. LANGEVIN TO MR. GREG WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

Question 1. Please verify that, since the hearing, you have had the opportunity to review TVA's proposed action plan.

Answer. We have not yet received TVA's formal action plan for review. In its written comments to our draft reports, TVA informed us of several actions that it plans to take to address our recommendations to strengthen the security of its control systems but we have not performed audit work to verify that these actions are under way or effective. Agencies are permitted 60 days from the date of an audit report's issuance to submit their action plan to us.

Question 2. Explain the process you will undertake to verify that the corrective actions are underway.

Answer. As part of our audit responsibilities under generally accepted government auditing standards, after conducting and reporting the results of an audit, we follow up with the audited entity to determine the extent to which it has implemented our recommendations. In doing so, we request that the agency provide a copy of the agency's statement of action to serve as preliminary information on the status of open recommendations and we discuss the status of the recommendations with cognizant agency officials; we obtain copies of agency documents supporting the recommendations' implementation or information from the agency's Office of the Inspector General; and we perform sufficient audit work to verify that the rec-

ommended actions are being taken and, to the extent possible, that the desired results are being achieved.

We track the status of agency efforts to implement our recommendations in a publicly available database, which is updated routinely and made available to all Members of Congress, their staffs, and audited agencies. A recommendation is closed when it has been implemented, when actions have been taken that essentially meet the recommendation's intent, or when circumstances have changed and the recommendation is no longer valid.

QUESTIONS FROM CHAIRMAN JAMES R. LANGEVIN TO MR. WILLIAM R. MCCOLLUM, JR., CHIEF OPERATING OFFICER, TENNESSEE VALLEY AUTHORITY (TVA)

Question 1. Publicly and privately owned infrastructures on the grid are so interconnected, weak security controls in one utility can pose harm to another utility that shares a connection. Yet publicly and privately owned infrastructures are subject to different security standards. According to a NIST-sponsored review published in March 2007, an organization conforming to the baseline set of security controls in SP 800–53 will also comply with the management, operational and technical security requirements of the NERC Reliability Standards, though the converse may not be true. For instance, the NERC Reliability Standards allow for the exclusions of telecommunications and distribution equipment from the "critical assets" list. Under the SP 800–53 requirements, however, there is no similar exclusion. This committee—along with NIST and GAO—has suggested that the NERC standards should be more aligned with the NIST 800–53 standards that apply to federally owned infrastructure. Are you concerned that a weakness on a privately owned infrastructure would affect your network?

Answer. TVA understands the importance of protecting its systems and takes that responsibility seriously. Good security practice requires that the higher security zone consider connections to other security zones as potentially hostile.

Accordingly, we treat all external connections as potentially hostile in order to appropriately protect our systems.

TVA does not believe that a security weakness at other electric utilities could impact the security or integrity of TVA's control systems. Computer network connections to control systems require multiple layers of security, as addressed by both NIST and NERC standards. The security controls in these layers must be, and in TVA's case are, sufficiently strong to compensate for any weaknesses in the other network.

Question 2. As control systems are becoming more connected, the more vulnerabilities are exposed. For instance, several months ago, a penetration-testing consultant named Ira Winkler gave a presentation at a conference describing an attack that he performed on a power company. Winkler was hired by the company to test the security of its network and the power grid it oversees. He set up an attack that paired social engineering with corrupting browsers on a power company's desktops. By the end of a full day of the attack, they had taken over several machines, giving the team the ability to hack into the control network overseeing power production and distribution. According to GAO, the interconnections between your control system networks and the corporate network mean that security weaknesses on the corporate network could affect control systems networks. As a result, TVA's control systems were at an increased risk of unauthorized access or disruption via access from the corporate network. Why shouldn't all control systems be isolated from the business network? How is TVA addressing this issue?

Answer. TVA agrees that control systems should be isolated from the business network. To the largest possible extent, this isolation should be a physical separation. In cases where there is a strong business or regulatory basis for interconnection with other networks, segmentation must be implemented through network architectural schemes that include layered security controls and effective intrusion detection systems.

TVA has implemented and will continue to strengthen a defense in depth strategy. This plan includes isolation and/or levels of segmentation that meet or exceed NIST, NERC, and other applicable standards.

Question 3. What specific efforts are underway to address the GAO report? Please provide the committee with a timeline for completing the recommendations.

Answer. TVA will continue to remediate the GAO recommendations according to our scheduled commitments in our response to the GAO report. Effective February 2008, cyber security is positioned at the enterprise level and is responsible for all management, administration, and control of cyber security at TVA including control systems. The GAO report made 19 recommendations that focused on our need to improve and extend our existing security program for process control systems. TVA

was already addressing 17 of the 19 recommendations prior to the GAO audit. The other two were completed in April. The LOUO GAO report identified 73 additional recommendations. Fifty percent of those recommendations will be complete by September 30, 2008. Seventy-five percent will be complete by December 31, 2008. Most of the remaining recommendations will be complete by September 30, 2009.

Question 4. Has the TVA performed all mitigations recommended by the ES–ISAC advisory for the Aurora vulnerability? Have you met with FERC staff to discuss these mitigations?

Answer. TVA has implemented all the mitigations from the ES–ISAC advisory that were determined to be necessary, based on a June 2007 assessment. Given that it has been a full year since TVA responded to the ES–ISAC advisory, we have conducted a fresh, zero-based assessment and have validated that currently digital relays on TVA's generation units either have no wiring installed for reclosing or have no remote communications connections. In accordance with the ES–ISAC advisory, TVA completed an emergency plan in August 2007. TVA's Nuclear Power Group (NPG) completed the required assessments consistent with these requirements on August 20, 2007.

TVA and FERC representatives spoke via conference call prior to the hearing to discuss the mitigations. At the conclusion of the call, both agencies agreed that a good next step is to meet in person. TVA is working with FERC to schedule this meeting.

Question 5. There is at least one company that manufactures a device that specifically mitigates the Aurora vulnerability. Has the TVA purchased this protective device?

Answer. No, TVA has not purchased this protective device, which is designed for those systems in which relays are capable of reclosing breakers, thereby damaging generation units. Since TVA relays dedicated to generation units have remote communication disconnected or are configured in a way that cannot reclose breakers, TVA has no need for this particular device.

TVA believes the best general solution is that digital relays, like the one used in the Aurora experiment, must be protected by strong cyber security controls if they must be connected to a computer network.

Question 6. Has DHS provided you with more EINSTEIN boxes since your previous discussions with the committee? How many boxes are you deploying in total?

Answer. TVA has four primary external connections and has installed or will be installing a device at each connection in support of the EINSTEIN initiative. DHS has provided TVA with the four EINSTEIN boxes with the exception of a card for one of these boxes. The installation of three of the four boxes is complete and the final installation will be scheduled based on the arrival of the necessary card.

Question 7. The committee is concerned not only with the security of the electric sector, but also the nuclear sector. Brown's Ferry nuclear plant is operated by the TVA. In August 2006, two circulation pumps at Unit 3 failed, forcing the unit to be shut down manually. The failure of the pumps was traced to an unintended incident involving excessive traffic on the control system's network. In 2007, the committee wrote to the NRC requesting an investigation into the source of this data storm; unfortunately, to this day, the NRC has been unable to conclusively determine the cause. Why don't we know what happened at Brown's Ferry? What has TVA done to determine what happened?

Answer. Consistent with our Nuclear Power Group (NPG) procedures, a root cause analysis using the Kepner-Tregoe methodology was performed by a multi-disciplinary team at the Browns Ferry following the incident.

The root cause analysis determined that excessive network traffic on the Unit 2 and 3 Integrated Computer System network caused the pumps to fail. TVA had network intrusion devices monitoring the connection between the business network and the internet at the time of the incident. Examination of logs from those devices for the August 2006 event showed no indication of outside influence. As stated in the NRC's letter to Chairman of the Committee on Homeland Security dated July 20, 2007, "The licensee [TVA] determined that the cause of the event was a malfunction of the recirculation pump variable frequency drive (VFD) microprocessor-based controller. The controller failure was attributed to excessive traffic on the internal network. Since the control network is physically and electrically independent of networks that interface outside the plant, the NRC is confident that the failure was not the result of a cyber attack."

TVA will continue to strengthen the security of our control systems. In performing our mission, the safety of our employees and the public is paramount in all of our operations.

○