THE CYBER THREAT TO CONTROL SYSTEMS: STRONGER REGULATIONS ARE NECESSARY TO SECURE 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

FIRST SESSION

OCTOBER 17, 2007

Serial No. 110–78

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

48–973 PDF WASHINGTON : 2009

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
VACANCY

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
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

ROSALINE COHEN, *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
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MICHAEL T. MCCAUL, Texas
DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
PETER T. KING, New York *(Ex Officio)*

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

CONTENTS

Page

APPENDIXES

THE CYBER THREAT TO CONTROL SYSTEMS: STRONGER REGULATIONS ARE NECESSARY TO SECURE THE ELECTRIC GRID

Wednesday, October 17, 2007

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 call, at 2:16 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, Thompson, McCaul, Brown-Waite, and Broun.

Mr. LANGEVIN. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on "The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid."

I will begin by recognizing myself for the purposes of an opening statement.

Today's hearing provides us with a prime opportunity to assess the future of cybersecurity and critical infrastructure protection in the United States. Today we will discuss two major issues: the efforts to implement cybersecurity standards within the electric sector and a cyber vulnerability, known as Aurora, which was recently made public.

Now, I will be blunt, if this administration doesn't recognize and prioritize these problems soon, the future isn't going to be pretty.

The bulk power system in the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800 megawatts of generating capability, serving over 300 million people. The effective functioning of this infrastructure is highly dependent on control systems, which a computer-based system is 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. As such, the cyber risk of these systems is increasing.

Intentional and unintentional control system failures on the bulk power system could have a significant and potentially devastating impact on the economy, public health and national security of the United States. For a society whose every function depends on reli-

able power, the disruption of electricity to chemical plants, banks, refineries, hospitals, water systems and military installations presents a terrifying scenario.

Now, we will not accidentally stumble upon a solution to these problems. Instead, we must dedicate a lot of hard work and resources to secure our systems. To this end, the Federal Energy Regulatory Corporation, FERC, has recommended protecting the bulk power system against disruptions from cyber attacks by approving a set of reliability standards developed by the North America Electric Reliability Corporation, or NERC.

Now, the proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electric access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information.

Two weeks ago, members of this committee, including myself, Chairman Thompson, Mr. McCaul, submitted comments to FERC Rulemaking. We believe that the standards proposed by NERC do not sufficiently ensure the production or delivery of power in the event of intentional or unintentional cyber incidents involving critical infrastructures. The NERC standards focus on the reliability of the bulk power system as a whole, yet ignoring the Homeland Security impact that loss of power in a region can have. The standards, for example, won't cover a significant number of assets that are critical to providing power throughout the country.

As several witnesses will testify today, the NERC standards won't require electric-sector owners and operators to secure their generation units, distribution units or telecommunications equipment. But we know from countless real-world examples that these units are highly vulnerable to intentional or unintentional cyber events. Knocking any of these units off could affect the power supply to our Nation's critical infrastructure.

The readiness standards that would preclude these elements just isn't good public policy. The technical experts agree with this assertion. According to research performed for NIST, the NERC standards are inadequate for protecting critical national infrastructure. And GAO concurs with those findings.

Now, I am concerned about the narrow scope of the standards, particularly in light of recent events. CNN recently reported that DHS researchers at the Idaho National Laboratory successfully destroyed a generator through an experimental cyber attack. This experiment was code-named "Aurora." And we are going to have a brief video at the end of the testimony of our witnesses here that are here this afternoon.

But officials tell me that malicious actors, insider terrorists, or nation-states could use the same attack vector against larger generators and other critical rotating equipment, that they could cause widespread and long-term damage to the electric infrastructure. DHS, working through Idaho National Labs and DOE, have been deploying mitigation measures for many of the critical infrastructure sectors. Naturally, we expect owners and operators of critical infrastructure would mitigate these vulnerabilities as quick as possible. Unfortunately, I have reason to believe that the mitigations

developed by DHS and DOE have not been fully implemented across the electric sector.

Today, the ranking member and I sent a letter to FERC Chairman Joe Kelliher and asked him to commence an investigation to determine the extent to which the electric-sector owners and operators have implemented these mitigation efforts.

Despite the comments from industry that suggest otherwise, we in Congress believe that this is a serious problem. This subcommittee will continue its vigorous oversight of this critical aspect of our Nation's homeland security. These are important issues.

And, without objection, I would like to introduce into the record our comments to the FERC Rulemaking that we submitted on October 5th, as well as the letter I provided Chairman Kelliher yesterday, requesting the investigation.

PREPARED OPENING STATEMENT OF THE HONORABLE JAMES R. LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE

Today's hearing provides us with a prime opportunity to asses the future of cybersecurity and critical infrastructure protection in the United States. We will discuss two major issues today: the efforts to implement cybersecurity standards within the electric sector and a cyber vulnerability known as "Aurora" that was recently made public. I'll be blunt—if this Administration doesn't recognize and prioritize these problems soon, the future isn't going to be pretty.

The bulk power system of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability serving over 300 million people. The effective functioning of this infrastructure is highly dependent on control systems, which are computer-based systems 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. As such, the cyber risk to these systems is increasing.

Intentional and unintentional control system failures on the bulk power system could have a significant and potentially devastating impact on the economy, public health, and national security of the U.S. For society whose every function depends on reliable power, the disruption of electricity to chemical plants, banks, refineries, hospitals, water systems, and military installations presents a terrifying scenario. We will not accidentally stumble upon a solution to these problems. Instead, we must dedicate a lot of hard work and resources to secure our systems.

To this end, the Federal Energy Regulatory Corporation (FERC) has recommended protecting the bulk power system against disruptions from cyber attacks by approving a set of reliability standards developed by the North American Electric Reliability Corporation (NERC). The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information.

Two weeks ago Members of this Committee, including myself, Chairman Thompson, and Mr. McCaul, submitted comments to the FERC rulemaking. we believe that the standards proposed by NERC do not sufficiently ensure the production or delivery of power in the event of intentional or unintentional cyber incidents involving critical infrastructures. The NERC standard focuses on the reliability of the bulk power system as a whole, ignoring the homeland security impact that loss of power in a region can have.

The standards won't cover a significant number of assets that are critical in providing power throughout the country. As several witnesses will testify today, the NERC standards won't require electric sector owners and operators to secure their generation units, distribution units, or telecommunications equipment. But we know from countless real world examples that these units are highly vulnerable to intentional and unintentional cyber events. Knocking any of these units off could affect the power supply to our nation's critical infrastructure.

Writing a standard that would preclude these elements just isn't good public policy. The technical experts agree with this assertion. according to research performed for NIST, the NERC standards are "inadequate for protecting critical national infrastructure." GAO concurs with those finds. I'm concerned about the narrow scope of the standards, particularly in light of recent events. CNN recently reported that

DHS researchers at the Idaho National Laboratory successfully destroyed a generator through an experimental cyber attack. This experiment was code-named "Aurora."

Officials tell me that malicious actors—insiders, terrorists, or nation states—could use the same attack vector against larger generators and other critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure. DHS, working through Idaho National Labs, and DOE have been developing mitigation measures for many of the critical infrastructure sectors. Naturally, we would expect owners and operators of critical infrastructure would mitigate these vulnerabilities as quickly as possible. Unfortunately, I have reason to believe that the mitigations developed by DHS and DOE have not been fully implemented across the electric sector.

Today, the Ranking Member and I sent a letter to FERC Chairman Joe Kelleher and asked him to commence an investigation to determine the extent to which electric sector owners and operators have implemented these mitigation efforts. Despite comments from industry that suggest otherwise, we in the Congress believe that this is a serious problem. This Subcommittee will continue its vigorous oversight over this critical aspect of our nation's homeland security.

Mr. LANGEVIN. With that, that concludes my opening statement. And the Chair now recognizes the ranking member of the subcommittee, the gentleman from Texas, Mr. McCaul, for the purposes of an opening statement.

Mr. MCCAUL. I thank the Chairman. I apologize for being a little bit late. It is not every day you see the President award the Dalai Lama the Congressional Gold Medal of Honor.

I want to thank you for holding this hearing. And we have been working in a very bipartisan way on this issue because it is an issue of national security that impacts the American people and the security of the American people.

The electric power grid and the generation and distribution equipment associated with it are amongst the most critical pieces of our country's infrastructure. These systems, commonly known as the power grid, are the largest, most complex machines on the continent, enabling power to be generated, transmitted and distributed to millions of individuals and businesses across North America.

Despite the fact that the grid is highly reliable and has built-in redundancy, the grid is dependent on its various parts. Due to the physics of transmitting electricity, the entire bolt power operates at the same frequency, so the grid could be vulnerable to cascading failures and long-term outages if the systems that control the production and flow of electricity are compromised. As we saw with Aurora, these systems can be compromised, and they are vulnerable.

Another example would be the East Coast blackout in 2003, when an ordinary power outage, caused by a line coming in contact with a tree, was exacerbated by a software bug, leading to an alarm system failure that rippled across the East Coast. The 2003 blackout was unintentional and, while costly, didn't cause major disruption for more than 24 to 36μhours. But it does, however, demonstrate that no grid can be threatened, when a relatively small number of systems fail. It also demonstrates that the grid can be threatened.

Industrial control systems, computer systems designed to monitor and control industrial processes, have been increasingly controlled over networks and the Internet. This has created a much more efficient and easy-to-use system, but has also created a whole host of vulnerabilities. These vulnerabilities are exacerbated by the

fact that traditional cybersecurity solutions are not as easy to implement because the systems must run smoothly and continuously.

Recently, the consequences of these cyber-based attacks have come to light, primarily on CNN. And it is crucial and critical that we move quickly in this country to secure these vulnerable systems.

The Department of Homeland Security has multiple initiatives under way to secure systems, as do a number of other agencies, as well as the private sector. The Department should take this opportunity to consolidate those initiatives and draft an overall strategy that minimizes overlapping efforts and prevents gaps so that these critical systems are secured as quickly and effectively as possible.

I look forward to this discussion and the discussion from the second panel, who will talk about cybersecurity standards and best practices within the industry.

I believe that we can work together within the existing structure to ensure that the industry's assets are adequately and safely protected from threats and vulnerabilities.

With that, I want to thank the witnesses for being here. And I yield back.

Mr. LANGEVIN. I thank the ranking member.

The Chair now recognizes the chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman. And I thank you for your leadership on cybersecurity in this Congress and your continued oversight on this issue.

Mr. Chairman, I often talk about vacancies within the Department of Homeland Security, because I think it affects our ability to protect and defend the United States. In that vein, I am concerned about the Department's efforts in cybersecurity, particularly given the extraordinary number of vacancies that have opened up in the National Cybersecurity Division. Three critically important individuals—the director of the National Cybersecurity Division, the deputy director of outreach and awareness, and the director of the Control Systems Security Program—have all left the Department in recent months. I hope Assistant Secretary Garcia can provide us information today about where we are in filling these important positions.

Of course, this is nothing new for DHS or the Cyber Division. The Control Systems Security Program, the subject of today's hearing, has gone through countless program managers over the years. I believe the high rate of vacancies and turnover is affecting the Department's ability to really move this country forward on control systems.

Take the control systems strategy, for example. In 2005, DHS started working with interagency partners to develop a comprehensive control systems strategy that would encompass the public and private sectors, set a national vision to secure control systems, describe roles and responsibility, and identify future requirements for resources and action. It is almost 3µyears later, and not one product has been delivered.

A Department working without key leadership sends a bad message to the private-sector owners and operators, who are essential

to securing critical infrastructure. How is the Department supposed to develop long-term relationships with these companies and individuals when there is a different DHS face in every meeting?

Similarly, how is the private sector supposed to react to the cyber initiative that was reported last month in the Baltimore Sun? According to that article, NSA will be working with DHS and other Federal agencies to monitor critical infrastructure networks to prevent unauthorized intrusions. According to the article, up to 2,000 people will be assigned to this endeavor.

I wonder how this initiative is going to impact the public-private partnership that DHS has been developing. I have asked the Department to brief me numerous times on this initiative, but we haven't heard a peep. I hope the Assistant Secretary can provide us with feedback today.

Mr. Chairman, the American people deserve better. They deserve better leadership on this issue. And I hope that the next administration will reverse this unfortunate and dangerous path. I thank you for your leadership on this issue, and I yield back.

Mr. LANGEVIN. I thank the gentleman.

Other members of the subcommittee are reminded, under the committee rules, opening statements maybe submitted for the record.

I want to begin now by welcoming our first panel of witnesses.

Our first witness, Mr. Greg Garcia, Assistant Secretary for Cybersecurity and Communications. Assistant Secretary Garcia oversees the Department of Homeland Security's mission to prepare for and respond to incidents that could degrade or overwhelm the operation of the Nation's information-technology and communications infrastructure.

I want to welcome you here, Secretary Garcia.

Our second witness, Gregory Wilshusen, is the director of information security issues at GAO, where he leads information-security-related studies and audits the Federal Government.

I appreciate you being here, Mr. Wilshusen.

And our third witness is Mr. Tim Roxey, the technical assistant to the president of Constellation Generation Group for Security. He is the deputy to the Chairs for both the Nuclear Sector Coordinating Council and the Partnership of Critical Infrastructure Security, and is the team lead for the Aurora mitigation efforts for the private sector.

Mr. Roxey, thank you for being here, as well.

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 Assistant Secretary Garcia.

And, Secretary, with all the vacancies that Chairman Thompson mentioned in his opening statement, I am glad to see that you are at least still on the job. Welcome. And thank you for being here.

STATEMENT OF GREGORY GARCIA, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, DEPARTMENT OF HOMELAND SECURITY

Mr. GARCIA. Thank you very much, Mr. Chairman.

Chairman Thompson, Ranking Member McCaul and members of the subcommittee, I do appreciate the opportunity to speak with you today about DHS efforts to strengthen the security and resiliency of our Nation's critical infrastructure.

It is fitting that you are holding this hearing during National Cybersecurity Awareness Month, because it really helps to raise public consciousness about the importance of control systems security to our economic well-being and to our homeland security.

I would also like to personally thank you and Mr. McCaul and your colleagues for your leadership in cosponsoring House Resolution 716, which endorses the ideals of National Cybersecurity Awareness Month, and for your continued efforts to raise awareness of this critical issue.

Control system—that is a term, a general term that encompasses several types of systems, including SCADA, that are most often found in the industrial sectors and critical infrastructures. The systems typically are remotely controlled devices used to operate physical processes in industries such as electricity, oil and gas, and water.

Control systems are particularly important for the security of our country's electric grid because of the significant interdependencies inherent with the use of energy in all other critical-infrastructure sectors. Therefore, securing control systems is vital to maintaining our Nation's strategic interests, the public safety and economic prosperity.

It is important to note that, because the private sector owns and operates 90 percent or so of the critical infrastructure that we need to protect, responsibility for securing our Nation's control systems lies heavily with the private sector. That said, as lead for coordinating national critical infrastructure protection and cybersecurity, DHS established a Control Systems Security Program. And the goal is simple: to lead a cohesive effort between Government and industry, focused on reducing the risks to control systems that operate our critical infrastructure.

How do we do this? We have a comprehensive approach to reduce risk by working closely with public and private partners. And it looks like this: We work with the control-systems vendor community to produce more secure systems; we work with the owners and operators to better secure their systems; and we work with the national labs and the National Institute of Standards and Technology to develop technical guidance. And we are proud of these efforts to assist our public—and private-sector partners to identify and mitigate direct risks to control systems.

We have made significant progress toward this goal, and today I would like to highlight just a few of these successes.

First, a key principle for our mission is that you can't enhance security if you don't know where your vulnerabilities are. In collaboration with several Department of Energy national labs, we developed the first widely available Control Systems Cybersecurity Self-Assessment Tool. It employs a systematic and repeatable approach for owners and operators to assess the cybersecurity posture of their control systems. Further, it offers recommendation based on industry standards that are customized to the operating characteristics of each control systems facility.

VerDate Nov 24 2008 13:19 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00011 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-78\48973.TXT HSEC PsN: DIANE

The response to the tool has been tremendous. For instance, a key industry association for industrial manufacturing professionals has found the tool so valuable that they are making it available to their entire membership of over 30,000 professionals worldwide.

Second, we sponsor the SCADA Procurement Project to help acquisition officials ensure that control systems they are buying or upgrading have the best security available. Government and industry representatives, including the multi-State ISAC, the Information Sharing and Analysis Center, the SANS Institute, and the DOE Idaho National Lab, developed this comprehensive guidance document. It offers standardized procurement language that companies can write into their contracts when they purchase new control systems. The guidance is available at no charge, and over 450 copies have been downloaded each month since it was posted in January of 2007.

Third, people are at the heart of addressing the cybersecurity challenge, and control systems are simply no different. That is why we are focused on training and educating control systems professionals on the best methods for securing and maintaining their systems. Since 2005, we have trained nearly 7,000 IT and control system professionals through both classroom and Web-based instruction modules. We have also developed curriculum for master's degree programs to aid faculty in teaching our future business leaders the importance of control systems security. To date, it has been distributed to more than 100 faculty members at universities and related institutions.

Fourth, an important aspect of our work in control systems security is in the area of standards. We have worked closely with NIST and other partners to improve technical guidance in their special publication series. In addition, we are about to release a catalog of control systems security standards that will serve as a foundational document, available for any industry to develop and implement cybersecurity standards specific to their operational requirements. The catalog is a compilation of practices inventoried from across the industry standards bodies and will provide a mechanism to identify gaps in existing standards and improve overall security.

And fifth, applying the risk management and partnership framework outlined in the NIPP, the National Infrastructure Protection Plan, we lead recent activity to identify, validate and mitigate a control systems vulnerability affecting several critical-infrastructure sectors. Federal agency partners worked with industry, technical experts, to assess the vulnerability and to jointly develop sector-specific mitigation plans. This enabled owners and operators to take specific actions to reduce the risk associated with the vulnerability. And this is a great example of collaboration. This is exactly what was envisioned in the NIPP process.

And we have also developed processes for sharing sensitive information with Government and industry stakeholders. Our US–CERT, the Computer Emergency Readiness Team, is charged with recording response to cyber attacks and is responsible for analyzing and disseminating cyber threat warning information. Control systems security program personnel are currently collocated and work closely with US–CERT. This close relationship benefits the CERT, in terms of having the expertise necessary for control systems. And

they make themselves immediately available for assisting with responses to incidents and the management of vulnerabilities related to control systems.

I will wrap up.

All of these efforts are informing our work to develop a comprehensive control systems strategy with our Federal and our private-sector partners. The strategy lays out a national vision, roles and responsibilities, and identifies feature requirements for national control systems security. Our goal is to release a final version of this national strategy in the first quarter of fiscal year 2009.

In conclusion, Mr. Chairman, securing control systems within our critical infrastructure, specifically within the electric grid, is a priority for DHS. The work we have accomplished thus far exemplifies a successful collaboration model for strengthening the security posture of our Nation's control systems. It has also deepened our understanding of the challenges that lay before us as we work to enhance the security and resiliency of our Nation's critical infrastructure. DHS is committed to continuing to work with our partners to strengthen our national control systems preparedness and our protection posture.

Thank you for your time today, Mr. Chairman. And I am happy to answer any questions from the subcommittee.

[The statement of Mr. Garcia follows:]

PREPARED STATEMENT OF GREGORY GARCIA

Chairman Langevin, Ranking Member McCaul, and Members of the Subcommittee, I appreciate the opportunity to speak about the role the Department of Homeland Security (DHS) plays in securing control systems, including the tools and resources we have made available to owners and operators of control systems, our efforts to collaborate and share information with both the public and private sectors, and analysis of control system vulnerabilities to strengthen the Nation's control system security posture. These efforts support one of the Department's primary missions of advancing preparedness. As October is National Cyber Security Awareness Month, I think it is particularly appropriate to highlight the importance of control systems security and to discuss our efforts to date to raise awareness of the challenges and solutions to securing these important systems. I would also like to recognize Chairman Langevin's and Ranking Member McCaul's leadership in promoting National Cyber Security Awareness Month's goals, objectives, and activities among their colleagues and constituents through their Dear Colleague letter and co-sponsorship of the Congressional Resolution. Raising awareness about protecting our critical infrastructures among home users, academic institutions, and businesses, including our control systems owners and operators, is fundamental to improving our preparedness posture.

As the Assistant Secretary for Cybersecurity and Communications within DHS' National Protection and Programs Directorate (NPPD), I oversee our mission to prepare for and respond to incidents that could degrade or overwhelm the operation of our Nation's information technology (IT) and communications infrastructure. This responsibility includes the goal of ensuring the security, integrity, reliability, and availability of our IT and communications networks. Reducing risk to that portion of the 17 sectors designated as critical infrastructures is among Secretary Chertoff's highest priorities, and I am pleased to share with you the Department's ongoing efforts to address this priority.

"Control system" is a general term that encompasses several types of systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. Control systems typically are remotely controlled devices used to operate physical processes in industries such as electricity, water, oil and gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). These control systems are critical to the safe and secure oper-

ation of our highly interconnected and mutually dependent critical infrastructures. A successful cyber attack on a control system could potentially result in physical damage, loss of service, and/or economic impact.

Ensuring the security of these systems is essential, and that responsibility lies heavily with the private sector, which owns and operates over 85 percent of the Nation's critical infrastructures. DHS works closely with private sector owners and operators to provide expertise, analytical products, and education and training materials that help control systems stakeholders identify and reduce direct risks for control systems. DHS communicates and collaborates with many diverse organizations, including government agencies, industry associations, national laboratories, equipment vendors, and asset owners and operators to identify improvements and drive their adoption across the infrastructure community. Through its involvement in the community and public-private partnerships, DHS is able to successfully engage with private sector owners and operators on significant control systems cyber security challenges and enable their voluntary cooperation and participation in implementing improvements to enhance the overall preparedness and resilience of the Nation's critical infrastructure.

DHS has three main objectives for reducing cyber risk and securing control systems: provide guidance, develop and enhance partnerships, and prepare for and respond to incidents. DHS also leverages the expertise and activities of operational programs and strategic initiatives from across the Department and the U.S. Government and integrates these activities to reduce risk, respond to incidents, and foster a culture of preparedness within the control systems community.

DHS utilization of several information sharing mechanisms allows the Department to manage effectively the collection and dissemination of sensitive vulnerability information, which ultimately enables us to raise awareness of vulnerabilities and risk management efforts among the control systems community, influence security practices to reduce risk, and raise the security bar across all the critical infrastructure sectors.

First, DHS **provides guidance** to the control systems community through several mechanisms and activities, including risk reduction products, such as security implementation guidelines and recommended practices; outreach and awareness through education and training; and technology assessments to identify vulnerabilities.

One of our recent accomplishments with regard to risk reduction products is the development and implementation of the Control Systems Cyber Security Self Assessment Tool (CS2SAT), which employs a systematic and repeatable approach that allows owners and operators to assess the cyber security posture of their control systems. Through the CS2SAT, users input facility-specific control system information. The tool then provides users with a picture of their control systems architecture and an assessment of their cyber security posture. It also makes recommendations for improvements. The recommendations are derived from industry cyber security standards and are linked to a set of specific actions that can be applied to mitigate the identified security vulnerabilities. The Instrumentation, Systems and Automation Society (ISA), one of the largest global organizations for control systems, announced on October 4, 2007 that it will make the CS2SAT available to their membership, which consists of over 30,000 automation professionals.

Another risk-reduction tool DHS sponsors for the control systems community is the Multi-State Information Sharing and Analysis Center (MS–ISAC) SCADA Procurement Project. We have worked closely with the MS–ISAC, the SANS Institute, the Department of Energy (DOE) Idaho National Laboratory, and representatives from government and industry to develop common procurement language that owners and regulators can incorporate into contracting mechanisms to ensure the control systems they are buying or maintaining have the best available security. The long term goal is to raise the level of control systems security through the application of robust procurement requirements. The Procurement Project has received very positive feedback from users, and the document has averaged more than 450 downloads per month from the MS–ISAC website where it was posted in January 2007.

DHS also provides education and training for our industry and government partners. Through our control systems security training courses, we have provided training to nearly 7,000 IT and control systems professionals on a range of topics, such as identifying control systems vulnerabilities, conducting risk assessments, and applying standards-based mitigation measures to improve security. We offer both classroom and web-based instruction modules and will be launching a new operations security course later this month. The web-based training has been especially popular with our partners with geographically dispersed systems and personnel.

In addition, in coordination with academia we developed a graduate school curriculum for Masters of Business Administration and Masters of Public Policy programs to aid faculty in developing courses on the security of critical infrastructures with an emphasis on control systems security. The curriculum provides materials on public policy, technical issues, and managerial principles associated with critical infrastructure resiliency. To date, the curriculum has been distributed to more than 100 faculty members at universities and related institutions.

DHS is working with the National Institute of Standards and Technology (NIST) to strengthen Federal standards and guidance regarding control systems security. Over the past year, NIST has been developing cyber security guidance and a compliance framework specifically tailored to control systems. The guidance component, Special Publication (SP) 800–82 (2nd draft), "Guide to Industrial Control Systems (ICS) Security," provides an overview of control systems, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. The compliance component, Special Publication (SP) 800–53, "Recommended Security Controls for Federal Information Systems," defines the minimum security controls for Federal systems and was originally published in 2005 by NIST in accordance with the requirements outlined in the Federal Information Security Management Act (FISMA). We have worked closely with NIST to develop SP 800–82, and to ensure that control systems security was incorporated into the updated revised SP 800–53. These NIST standards together will provide important baseline security guidance for adoption by Federal owners and operators of control systems.

We are also working with NIST and several of the DOE National Laboratories to develop a catalog of control system security standards. This comprehensive catalog represents a compilation of practices inventoried from across the industry standards bodies and provides recommendations for enhancements to standards to increase the security of control systems from both cyber and physical attacks. While many of today's standards appropriately address security factors, detailed guidance is needed to ensure adequate protection from cyber attacks on control systems. This catalog is specifically designed to provide a framework for developing or enhancing technical aspects of security standards. When completed, the catalog will serve as a foundational document available for any industry using control systems to develop and implement cyber security standards specific to their individual operating requirements.

Second, we are **developing and enhancing dynamic, cooperative relationships** with government, industry, academia, and our international counterparts to promote control systems security and leverage existing initiatives being conducted by government and industry. For example, DHS partners with other agencies to support research and development of secure technologies for control systems. Public-private partnerships are essential in our efforts to improve the security of control systems because, as noted previously, the private sector owns and operates most critical infrastructure.

The National Infrastructure Protection Plan (NIPP) framework and supporting Sector-Specific Plans (SSPs) provide a coordinated approach to critical infrastructure protection roles and responsibilities for Federal, State, local, tribal, international, and industry security partners. Utilizing the NIPP framework, DHS directed recent activity to validate and mitigate a control systems vulnerability affecting a number of critical infrastructure sectors. Numerous Federal agency partners worked closely with industry technical experts to assess the vulnerability and to develop sector-specific mitigation plans. We are pleased with the results of this partnership: it produced jointly developed mitigation guidance and allowed owners and operators within the affected sectors to take deliberate and decisive actions to reduce significantly the risk associated with this vulnerability.

Recognizing the importance of engagement with industry, DHS sponsors a number of groups to foster close collaboration and information sharing among the control systems community. The Process Control Systems Forum (PCSF) was established to accelerate the design, development, and deployment of more secure control systems. The PCSF includes a variety of stakeholders including both national and international representatives from government, academia, owners and operators, systems integrators, and vendors.

The Control Systems Cyber Security Vendors' Forum, a subgroup under the PCSF, facilitates communication in a trusted environment between industrial automation and equipment suppliers and control system service providers. The Vendors' Forum consists of 50 members from 27 domestic and international companies comprising 90 percent of the market share providing service to all 17 critical infrastructure sectors.

An example of this collaboration occurred earlier this year when members of the Vendors' Forum worked together to address the potential effects on control systems caused by the date change in the Daylight Saving Time (DST) standard. The change in DST impacted control systems in over 19 countries. The control systems community recognized the importance of this issue and worked with the DHS National Cyber Security Division's United States Computer Emergency Readiness Team (US–CERT) to develop a Technical Information Paper, "Daylight Saving Time Changes for 2007." The paper provided guidance to industry on mitigation measures and has been downloaded from the US–CERT website more than 500 times between April and July 2007.

Third, to **prepare for and respond to incidents,** DHS is improving situational awareness, analyzing vulnerabilities, and sharing information. Owners and operators can report general cyber incidents and vulnerabilities, including those related to control systems, to the US–CERT. Control systems technical experts are integrated into the US–CERT operations center to provide timely situational awareness information and assist with incident management.

DHS has developed processes for sharing sensitive information related to control systems vulnerabilities with Federal, State, and local governments, and control systems owners, operators, and vendors to improve control systems security within and across all critical infrastructure sectors. This process addresses the information flow from vulnerability discovery, to validation, public and private coordination, and outreach and awareness, as well as identifies the deliverables and outcomes expected at each step in the process. Information sharing between the government and the private sector is essential to this process, and it allows both sectors to identify gaps in preparedness capabilities among public and private sectors, as well as identify policy issues that affect response and recovery.

The process incorporates existing entities across the public and private sectors, including the Government and Industry Sector Coordinating Councils, the US–CERT, the Homeland Security Information Network (HSIN), and Information Sharing and Analysis Centers (ISAC). It also builds on established Departmental practices and procedures for the identification, validation, coordination, and communication of vulnerabilities across the critical infrastructure sectors.

As part of this process, DHS relies on three primary mechanisms to communicate vulnerability information about control systems to the various stakeholders. The US–CERT National Cyber Alert System is utilized as a mechanism to share information about vulnerabilities to a broader audience. Vulnerability information is conveyed via several products, including *Vulnerability Notes* that are released on a regular basis to stakeholders in the control systems community. More detailed analyses of cyber vulnerabilities that may impact control systems are published via the *Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems,* whose recipients include governments and members of the control systems community. Both of these reports are posted on the US–CERT Control Systems Portal and are available to all portal members with access to the control systems section of the website, which encompasses representatives from the Federal, State, and local governments, Sector Specific Agencies, and control systems owners, operators, and vendors.

In addition, DHS works with vendors, owners, and operators to perform vulnerability assessments of selected systems to identify cyber vulnerabilities based on emerging exploits and partners with industry to develop mitigation strategies. DHS also works with control systems vendors, owners, and operators to share sensitive information through the Protected Critical Infrastructure Information (PCII) program so that private sector vulnerability data may be appropriately safeguarded.

Finally, in Fiscal Year (FY) 2007, we began working with our Federal partners to identify baseline individual agency activities to serve as the foundation for developing a comprehensive control systems strategy that will encompass the public and private sectors, set a national vision to secure control systems, describe roles and responsibilities, and identify future requirements for 5¶resources and actions. The Department has developed a timeline to complete this action, building on work that has already been completed. In the first quarter of FY 2008, a draft of the Federal sector portion of the strategy will be released for review by government stakeholders. Working with sector representatives from the Partnership for Critical Infrastructure Security under the NIPP framework, we will then begin to develop a private sector component to integrate into the strategy. We intend to have a final comprehensive strategy ready for release in the first quarter of FY 2009.

Conclusion

Securing control systems is an important priority for DHS because they are unique elements of our critical infrastructure. They are deployed ubiquitously and perform such vital functions that their disruption could severely impact citizens' daily lives. DHS has developed a program that includes the development and dissemination of tools, products, and guidance to the controls systems community, established mechanisms to work with our partners in both the government and industry, and developed capabilities to prepare for and respond to incidents.

Ongoing education and training for the control systems community is imperative, as well as regular assessments of systems. We must continue to raise awareness of the threats to and vulnerabilities of control systems through our information sharing mechanisms and continue to incorporate security measures in control systems standards. The development, execution, and maintenance of a national control systems security strategy is essential to managing our current and future efforts. The work we have accomplished so far has deepened our understanding of the challenges that lay before us, and we continue to work to strengthen our national control systems preparedness and protection posture.

Thank you for your time today, and I am happy to answer any questions from the Subcommittee.

Mr. LANGEVIN. Thank you, Mr. Secretary.

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

GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Langevin, Ranking Member McCaul and members of the subcommittee, thank you for the opportunity to testify at today's hearing on the cyber threats to control systems.

Control systems are computer-based systems that are used in many industries to monitor and control sensitive processes and physical functions. These systems provide vital functions in many of our Nation's critical infrastructures, including electric power generation, transmission and distribution.

Today I will discuss the cyber threats, vulnerabilities and impact of attacks on control systems, as well as private-sector and Federal initiatives to strengthen the security of these systems.

Mr. Chairman, critical infrastructure control systems face increasing risk to cyber threats, vulnerabilities and the potentially severe impact of an attack. Cyber threats can be intentional or unintentional, targeted or nontargeted, and can come from a variety of sources. Intentional threats include both targeted and nontargeted attacks, while unintentional threats can be caused by software upgrades or system maintenance procedures that inadvertently disrupt systems.

Sources of these threats include foreign nation-states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled insiders working inside or within an organization. Federal and industry experts believe that critical infrastructure control systems are more vulnerable today than in the past, due to the increased standardization of technologies, the increased connectivity of control systems to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems.

The impact of a serious attack could be devastating, as the following examples demonstrate. In an intentional targeted attack, an individual who is rejected for a job opening reportedly used a radio transmitter to remotely break in to the controls of an Australian

sewage-treatment system. He altered electronic data for sewage pumping stations, which subsequently resulted in them to malfunction, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.

A foreign hacker penetrated security at a Harrisburg, Pennsylvania, water-filtering plant and installed malicious software that was capable of infecting the plant's water-treatment operations. The infection occurred through the Internet and did not seem to be an attack that specifically targeted the control system.

And in an unintentional incident, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant failed, forcing the plant to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.

The private sector and Federal agencies have multiple initiatives under way to help secure control systems. Industry-specific organizations in various sectors, including the electricity, oil and gas, and water sectors, have ongoing initiatives to develop standards, publish guidance and host workshops.

Federal agencies, including DHS, DOE and others, have also initiated efforts to improve the security of critical infrastructure control systems. These include coordinating with the US–CERT to provide timely information about vulnerabilities and incidents, developing a Control System Cybersecurity Self-Assessment Tool for control system owners and operators, establishing the National SCADA Test Bed Program and publishing security guidance.

However, DHS has not yet established a strategy to coordinate the various control systems activities across Federal agencies and the private sector. In addition, more can be done to address specific weaknesses in DHS's ability to share information on control system vulnerabilities.

In a report being released today, we recommend that the Secretary of Homeland Security develop an overarching strategy to guide efforts for security control systems and establish a rapid and secure process for sharing sensitive vulnerability information with control system stakeholders.

Until DHS implements these actions, increased risk exists that the Federal Government and private sector will with invest in duplicative efforts, miss opportunities to learn from the activities of others, and not be timely informed about key vulnerabilities that expose control systems to an increased risk of disruption.

Mr. Chairman, this concludes my statement, and I would be happy to answer any questions that you or members of the subcommittee may have.

[The statement of Mr. Wilshusen follows:] [1]

Mr. LANGEVIN. Thank you, Mr. Wilshusen.

I want to now recognize Mr. Roxey to summarize your statement for 5 minutes.

[1] See committee file.

STATEMENT OF TIMOTHY E. ROXEY, TECHNICAL ASSISTANT TO THE PRESIDENT OF CONSTELLATION GENERATION GROUP

Mr. ROXEY. Chairman Langevin, Ranking Member McCaul and members of the subcommittee, thank you very much for allowing me the opportunity to come and talk to you today.

As previously indicated, I am the team lead for the Aurora mitigation efforts in the private sector, and that is part of my hat for deputy to the Partnership for Critical Infrastructure Security.

I am here today to discuss the successful private-public partnership model of the national infrastructure plan and how this partnership brought about successful mitigation without any need for significant regulatory action by any Federal agency. My discussion will fall into three areas: actions taken within the private-public partnership model, preliminary lessons learned and some concluding remarks.

The actions taken started when the private sector was approached in late February by Department of Homeland Security. The information being conveyed to us at that time was stressed as being very sensitive, and we were also told the Department of Homeland Security was keeping this information at the FOUA level, rather than classified, because, in recognition of the fact that 85 to 90 percent of the Nation's critical infrastructure is owned, operated and secured by the private sector, the classification of such information would make it very difficult, if not impossible, to rapidly move forward to mitigation.

Mitigation actions were developed by my team and the electric sector team, with the partnership of Homeland Security and the Idaho National Labs subject-matter experts. And they fell into basically two categories: the short-term, mid-term, long-term mitigation strategies, which are things that you can do to step through and reduce and mitigate exposure; and then a set of immediate actions that, had this risk been brought out into the public a lot earlier, we may have had a threat, therefore we may have had to step briskly into some immediate actions. It is gratifying to state right now that that has not been the case.

Support from DHS, DOE and the national labs was essential in the development of these strategies. In addition, DHS has maintained a very strong presence within the nuclear sector throughout the mitigation strategy's implementation phase. This effort is, in our opinion, a very strong example of effective public-private partnership.

When the mitigation documents were completed, roughly June, June 13th I believe, of this year—so between March and June 13th, we developed these documents. They were approved by the Nuclear Sector Coordinating Council, the Electric Sector Coordinating Council, and transmitted through those councils to the sectors on June 20th and 21st.

The NRC also put out a letter on June 20th, and coordinated with the nuclear sector document, requesting that at 60 days and 180 days we report back to the NRC the progress that we had made in implementing those developed strategies. Each of the sector mitigation strategies, like I said, identified a 60—and 180-day requirement in the nuclear sector. And the NRC's letter was their

regulatory footprint on this issue to try and drive an understanding of the concern to get mitigation accomplished.

Some have asked why the nuclear sector took this initiative on as a commitment. The nuclear power sector, one of the 18 critical infrastructures within the Partnership for Critical Infrastructure Security, is probably the most bounded sector in the United States. There are 65 physical sites, 104 power plants and a well-organized Nuclear Energy Institute, our industry association. We have a strong regulator in our area, the Nuclear Regulatory Commission. So it is a very tight box, and we can driving solutions on this very quickly. And it was felt that we could make these actions a commitment on ourselves and execute them within a time frame.

On June 20th, these actions started off. September 20th, these actions were 100 percent successfully mitigated in the nuclear sector and all electric-sector assets that are adjacent to nuclear-sector assets. That is a very substantial accomplishment.

A few lessons learned, if I could.

Effective, voluntary public-private partnership is the key to timely mitigation of security vulnerabilities. Proactive industry actions, endorsed by a Federal agency with oversight responsibilities, led to reducing the risk to our Nation's nuclear infrastructure in a timely manner.

Trust the technical experts and involve them in all communications. Bring them along to meetings and briefings.

Bring a vetted industry group into the conversation as soon as possible to validate and partner with researchers. Sector leads from PCIS may be an appropriate group, along with their technical experts. PCIS is an appropriate vehicle to ensure that there is a broad review across many sectors.

Consistent common messaging provides consistent common mitigation, a common message that all affected sectors received. In this case, there are some mixed messages, but we worked very hard to fix that.

Single point of contact facilitates effective coordination. We did have a single point of contact within the Department of Homeland Security, and that was a very effective tool for us to use as we stepped through.

Concluding remarks: I would like to just jump right to the-additionally, the public-private partnership model should be nurtured and continued. Early engagement of private-sector leadership through interaction between DHS, PCIS and the vulnerability researchers is an excellent way to fully vet the emerging vulnerability with both DHS and the SMEs from other Federal agencies and the private sector.

These efforts should start with effective awareness campaigns to educate all sectors about the risks that they currently face, followed with clear guidance on appropriate mitigation measures for the newly discovered risk. This guidance should contemplate all aspects of the technology life cycle, including improved development standards, implementation guidelines, operating procedures and incident response.

Good progress has been made by progressive asset owners, industry-initiated infrastructure protection leadership, and by vendors willing to anticipate larger market-driven requirements for more

security. Security, including cybersecurity, is best enhanced by continuing to build trust relationships and voluntary coordination and cooperation using the sector partnership framework. The nimbleness that effective security requires in the modern world makes these trust relationships our best defense.

Finally, the nuclear sector, in close coordination with our Government coordinating council partners, did mitigate and close off this vulnerability before the threat became known and without new regulations.

Thank you very much. I would be happy to answer any questions.

[The statement of Mr. Roxey follows:]

PREPARED STATEMENT OF TIMOTHY E. ROXEY

Mr. Chairman and Members of the Subcommittee:

I am Tim Roxey, Technical Assistant to the President of Constellation Generation Group for security and Deputy to the Chairs for both the Nuclear Sector Coordinating Council (NSCC) and the Partnership for Critical Infrastructure Security (PCIS). I am also the team lead for the Aurora mitigation efforts for the Private Sector.

In this last role I collaborate with subject matter experts (SME) (Research Engineers from Idaho National Labs (INL) and their contractors. . .who discovered the present vulnerability, Industry SME from all of the impacted Critical Infrastructure Sectors, Department of Homeland Security (DHS) and Department of Energy (DOE) SME and officials) in order to develop mitigation strategies to thwart the exploitation of the cyber vulnerability which threatens our critical infrastructure. Before becoming a Technical Assistant and Deputy to the Chairs of NSCC and PCIS I was a director of IT at one of our Nation's Nuclear Power Plants. In this role I was responsible for all telecommunications, IT applications and Cyber Security for the entire nuclear fleet. In addition, I was the nuclear sector's Chairman of a standing committee dedicated to Cyber Security. I was a founding member of the Nuclear Energy Institute's (NEI) cyber security task force; formed shortly after 9/11, the task force's purpose was to write an assessment and mitigation guidance document for nuclear power plants. This document, NEI 04–04: Cyber Security Program for Power Reactors was endorsed by the NRC and found an acceptable method to address cyber security. Since the endorsement of NEI 04–04 the NRC has proposed regulations for cyber security that are consistent with NEI 04–04.

I have also had former senior level governmental interactions when I worked with Vice President Al Gores' National Performance Review as a private sector Industry Sector Liaison. In this capacity I was charged with bringing Industry's requirements for regulatory interactions into a discussion with various federal sector agencies.

I am here today however, to discuss the successful use of the Public-Private Partnership model discussed in the National Infrastructure Protection Plan (NIPP). This partnership brought about the mitigation of the recently identified control system vulnerability (CSV) without the need for significant regulatory action by any federal agency. My discussion will fall into two areas as they relate to the present vulnerability. These areas are:

(1) Actions taken within the Public-Private partnership - structures and processes which reduce risk of vulnerability

(2) Preliminary lessons learned—a look back on this effort to help improve the performance of the Public/Private Partnership model's performance.

(3) Concluding Remarks

Actions Taken

The Nuclear Sector was approached by DHS about the Aurora vulnerability in February of 2007. At this initial briefing it was decided that a more through briefing would be given to a select sub-group of the NSCC. It was also stressed that this subject is very sensitive and hence needed to be protected from disclosure.

To this final point DHS worked very hard to make sure that the Aurora issue remained at a FOUO level rather than being classified at a higher level. This decision was based on the fact that it is the private sector that owns, operates, and secures roughly 85% of all of our nation's critical infrastructure and key resources. By having the knowledge of this vulnerability classified it would have been difficult if not impossible for the private sector to develop and implement mitigation strategies as rapidly as it has.

In late February DHS officials from Infrastructure Protection briefed the details of the Aurora vulnerability to the NSCC. At this meeting the nuclear sector decided to take aggressive action to develop and implement mitigations that would reduce the exposure of the nuclear power facilities to this vulnerability.

A multilevel structure was developed within the nuclear sector and individuals assigned. The structure consisted of an Executive Review Board that reported to the NSCC and a Technical Task Team that was charged with development of guidance document for industry to use to perform mitigation activities.

The nuclear sectors' Aurora Technical Team worked in close coordination with the Electric Sectors' technical team in the development of mitigation documents. The nuclear sectors Technical Team also worked in close coordination with its government partners including strong coordination with the NRC.

The various mitigation actions that were developed were divided into two areas. One area was short-term, mid-term, and long-term actions and the second area was a set of actions designed to be implemented immediately if the specific vulnerability was actually being exploited. It is gratifying to say that the immediate actions have not been needed. The shortest term actions were targeted at substantially reducing the exposure to the vulnerably and the longest term actions were designed to make improvements in the supply chain and stand up programmatic actions.

The support from DHS, DOE, and the national labs (such as Idaho National Labs) in the rapid development and implementation of these mitigation documents was essential. In addition DHS has maintained a strong presence with the nuclear sector throughout these mitigation efforts. This effort is an example of the very effective Public-Private partnership.

When the mitigation documents were completed they were routed through the NSCC and ESCC for approval and then scheduled for release to industry. The release of the Nuclear Sectors mitigation document was coordinated with the release of the Electric Sectors (ES) Information Sharing and Analysis Centers (ISAC) Advisory which was released one day after the Nuclear Sector mitigation document.

Based on the endorsement of the NSCC, the Nuclear Sector Technical Task Team added additional resources such as a Project Manager to manage the actual implementation phase of the mitigation work. A kick off meeting was held in Washington DC on June 13 with a final release to the industry of mitigation documents made the following week.

Within the nuclear sector a series of weekly meetings between the nuclear sector Technical Team (comprised of representatives from INL, DHS, and Industry) and the various points of contact for all of the nation's nuclear power plants was convened and mitigation efforts began. To monitor the sectors performance the Technical Task Teams' PM prepared status reports for the Executive Review Board and DHS. These reports were updated every week based on the weekly meeting report out by all of the nuclear utility participants.

Each of the sector mitigation documents urged that actions be taken within 60 days and then again different actions within 180 days. The NRC in a letter, coordinated for release along with the sectors' mitigation document, requested that the nuclear sector licensees provide an update to the NRC on progress made at the completion of the 60 days and 180 day efforts.

Why did Nuclear take this initiative on as a requirement? The nuclear power sector took this opportunity to demonstrate its commitment to security. The sector recognized the validity of the vulnerability, and because the sector is well structured to handle these types of emergent issues, with only 65 physical sites and 104 power plants and a well organized industry association (the Nuclear Energy Institute), it was feasible to develop a uniform mitigation plan that sector members could implement within the desired time frame.

Lessons Learned

1. ***An effective, voluntary public-private partnership is the key to timely mitigation of security vulnerabilities.*** Proactive industry actions, endorsed by a federal agency with oversight responsibilities, are effective in reducing the risk to our nation's nuclear infrastructure in a timely manner without the delays or exposure of sensitive information that the due process requirements of regulatory action could necessitate.

2. ***Trust the technical experts and involve them in all communications.*** Bring them along to meetings and briefings for support. Several times it seemed that the message changed as it moved from the technical experts to the policy experts. When non-technical people brief on technical aspects to technical people there is a high risk of losing credibility and it becomes difficult to recover.

3. ***Bring in a vetted industry group ASAP to validate and partner with researchers.*** This group will validate the conclusions of the researchers and fa-

cilitate expedient response by private sector owners and operators, because their involvement lends credibility to the message. Sector leads from PCIS may be an appropriate group, as long as they bring their technical experts to the table as well. In this regard, PCIS is an appropriate vehicle to ensure that there is a broad review across many sectors.

4. ***A multi-sector implementation plan is needed to provide cross-sector coordination.*** An implementation plan should be developed that addresses the sequence of sector engagement based upon a full discussion between the public sector and private sector. Although in the present effort this was performed successfully this step needs to be institutionalized so that future discoveries can benefit from this step. This plan should address the sector and assets to address first then second then third, etc.

5. ***Consistent common messaging provides consistent common mitigation.*** There should be a common message that all effected sectors receive. In this particular case there are mixed messages. After 16 months of research and 5 months of multi-sector mitigation strategy development there are still some messages saying this is not a significant issue because of the difficulty of exploiting it and others saying it is.

6. ***Single point of contact facilitiates effective coordination.*** The establishment of a single point of contact within DHS was of great utility to the Private Sector. This single point of DHS contact provide for consistent and sustained coordination with the subject matter experts of INL and the private sector team of subject matter experts and the Aurora Technical Team's lead. This support was instrumental in the achievement of nuclear sectors 60 day mitigation and the electric sectors mitigation of nearby electric sector assets.

Concluding Remarks

The course of action that is recommended for any future discovered vulnerability, in light of the success of the present mitigation efforts, leads to the conclusion that continued decisive and coordinated private sector partnerships leads to a better vetting of vulnerabilities and a faster response via mitigation. In addition, these actions can take place much faster than the regulatory rule making process. This was shown to be the case within the nuclear sector.

Additionally, the course of action that is recommended for any future discovered vulnerability, in light of the success of the present mitigation efforts, leads to the conclusion that continued decisive, coordinated, and committed effort by government, and private sector leadership within the framework of the Public Private Partnership model should be nurtured and continued. Early engagement of private sector leadership through interaction between DHS, PCIS and the vulnerability researchers is an excellent way to fully vet the emerging vulnerability with both DHS (and SME's from other federal agency's) and the private sector.

These efforts should start with effective awareness campaigns to educate all sectors about the risks that they currently face, followed with clear guidance on appropriate mitigation measures for the newly discovered risk. This guidance should contemplate all aspects of the technology lifecycle, including improved development standards, implementation guidelines, operations procedures, and incident response. Good progress has been made by progressive asset owners, industry-initiated infrastructure protection leadership and by vendors willing to anticipate larger market-driven requirements for more security. Security, including cyber security, is best enhanced by continuing to build trust relationships and voluntary coordination and cooperation using the sector partnership framework. The nimbleness that effective security requires in the modern world makes these trust relationships our best defense.

Mr. LANGEVIN. I want to thank the witnesses for their testimony.

And I will remind the members that each member will have 5μminutes to question the panel.

And I recognize myself now for the purpose of asking questions.

Secretary Garcia, I would like to start with you. In your written statement, it says that you were pleased with the results of the public-private partnership on Aurora because you developed mitigation guidance. Now, guidance is good, but this committee is most concerned about mitigation implementation.

So my question is, what percentage of the electric-sector owners and operators do you believe implemented the Aurora recommendations issued by NERC?

Mr. GARCIA. Yes, Mr. Chairman, we would rely on the industry sector leads to collect that information, as that is something that we don't collect nor compel. But we do understand that the mitigation strategies were sent out to hundreds of electric-sector owners and operators. And, as Mr. Roxey indicated for the nuclear sector, he reported about 100 percent mitigation.

So we are looking to continue the partnership with the private-sector leads to monitor how well that implementation is going. But for specific numbers, I don't have that for you today.

Mr. LANGEVIN. But Mr. Roxey, in the comments that he was making, was speaking specifically about the nuclear sector and not the electric grid. So we may have had success on the nuclear side and in securing SCADA systems, but not necessarily on the electric side.

Now, I think that is an area where Homeland Security has to be much more proactive, in making sure that the mitigation strategies were actually implemented.

Mr. GARCIA. Absolutely, sir.

Mr. LANGEVIN. We clearly don't want to find out that we knew there was a problem, we expected mitigation to take place, and yet it wasn't. And we don't want to find that out only after something were to happen, an attack occurs or, whether it is intentional or unintentional, something shuts down the power grid.

Mr. GARCIA. Yes, sir. And we also rely heavily on our Federal partner on this, FERC, who you will be hearing from in the next panel, who is keeping up that close relationship with the electric sector to monitor progress in that area.

But this is something that DHS takes very seriously. And we continue to push on this with all sectors, because we are concerned with common vulnerabilities, control systems vulnerabilities, across all the critical sectors. So we are trying to raise awareness of this not just in the electric sector and nuclear, but to many other critical sectors.

Mr. LANGEVIN. Well, Assistant Secretary Garcia and Mr. Wilshusen, have you reviewed our comments to the FERC Rulemaking? And, if so, do you agree with our assessment that the narrow definition of critical assets allows the electric industry to avoid securing many connective devices?

Mr. WILSHUSEN. Yes, we have taken a preliminary look at your comments, as well as those of the requirements that NERC has established and the reliability standards. And, yes, we do have some concerns about the extent to which these standards and regulations apply to those types of assets.

We believe that, in many cases, that they do not appear to consider, one, the interdependencies of critical infrastructure on the bulk electrical system. And they also appear to identify only those assets which could have an impact on the availability or reliability of the bulk electrical system, and does not necessarily identify those assets or cover those assets that, while they may not have an impact on the overall bulk electrical system, they could have a significant localized impact on critical infrastructures that are supported by the bulk electrical system.

Mr. LANGEVIN. Yes, that is an important point.

Secretary Garcia?

Mr. GARCIA. Mr. Chairman, we are trying to get standards that all industry sectors can deploy against vulnerabilities to their control systems. And certainly, the NIST standards ought to be heavily considered in all critical infrastructure control systems standards development, in addition to sector-specific operational requirements.

So while we don't have specific guidance on each sector for what standards they ought to deploy, we think that they ought to be able to effectively combine the NIST standards with those that are specific to their sector.

And on the electric sector, I think our friends in FERC may have more comment on that.

Mr. LANGEVIN. But do you agree that our assessment that the narrow definition of critical assets allows electric industry to avoid securing many connected devices?

Mr. GARCIA. I would actually prefer, on a question of that specific detail, to defer to FERC on making the judgment about the sectors implementation.

Mr. LANGEVIN. Mr. Wilshusen, the committee asked GAO to compare the NERC standards with NIST 800–53. Can you briefly describe your conclusion?

Mr. WILSHUSEN. Yes. We found that the NERC reliability standards contained less stringent security requirements and guidelines than the NIST guidance. The NERC standards do not provide levels of protection from cyber attacks commensurate with the mandatory minimum low-baseline level of protection required by NIST.

For example, NERC standards addressed only a subset of a low—and moderate-baseline control set specified in 800–53. And this subset may not be adequate for protecting critical national infrastructure control systems, especially when considering the interdependencies of the critical infrastructures. And further, it may not be adequate for all electrical energy systems when the impact of regional and national power outages is considered.

Mr. LANGEVIN. I thank you, Mr. Wilshusen.

The Chair now recognizes the—before I turn it over to the ranking member, I think this is something we are going to have to take a harder look at. Because why NERC would have standards that are below NIST when the Federal Government has to comply with NIST standards and the larger impact potentially would be in the private sector and why NERC would adopt standards which aren't on par to NIST is beyond me. And this is something we are going to pay particularly close attention to. If need be, legislation would be required to require that standard to be on par.

With that, the Chair now recognizes the ranking member for 5µminutes.

Mr. MCCAUL. I thank the Chairman. And, as you know, we are in agreement on that issue.

I recall being briefed, I think it was last January—we had just got sworn into the new Congress, and we got briefed on this significant vulnerability—and at that time, it was a closed-door session; it has come out on the news now—but the vulnerability that could potentially shut down our power grids in this country and bring tremendous destruction.

We know that 25 nations have developed cyber warfare programs, so the capability, this type of capability in the wrong hands of a rogue nation or a terrorist state could be devastating.

But I also believe that credit is due where it is due. And I think that the fact that we discovered this, through the Idaho National Labs, on our own, proactively, and Mr. Garcia, working with the Department Homeland Security, and, Mr. Roxey, your coordination on the mitigation strategy with the private sector, is to be commended.

And that is really what, I think, in the Congress, we want to see, is instead of being behind the curve and catching up—and we know the vulnerabilities are huge and the intrusions happen all the time. This was actually a good-news story and an example of where we discovered the vulnerability, not some foreign entity or some criminal. We found it first. We fixed it. And then by June, Mr. Roxey, you put your plan of action, mitigation strategy into action. Within 60 days, the nuclear sector was protected. The electricity, I think it will take 120 days.

But I think that is an important point to make. I mean, you are really to be commended for what you did. I know sharing information, which we require you do with the Congress, always makes you a little nervous, because you don't know what is going to happen with that information. But this was a good-news story. I mean, we really stopped a serious thing from being a serious threat to the United States. And I think it is great news.

And, Mr. Wilshusen, I agree with you. I think an overarching strategy is what we need at the Department of Homeland Security.

Mr. Garcia, I know you are working on that.

And I think the coordination with the stakeholders through the private sector is critically important. And, Mr. Roxey, through your testimony, I think you've demonstrated that, in large part, that is working, through the ISACs, the Information Sharing Analysis Centers. That is what was actually put into place through the mitigation strategy, and it is working.

My question, without going into a sermon up here, is, what can we do to see more of this?

What can you do, Mr. Garcia, at the Department of Homeland Security to proactively find vulnerabilities that are out there, before our enemies do, and then fix them and then mitigate the potential damage that can be done?

And that is for the entire panel.

Mr. GARCIA. Congressman, thank you for the question and for the compliment. I very much appreciate it.

My response as to what you can do is, you are doing it right now. Having public hearings like this that are raising the issue and raising the awareness about the range of vulnerabilities that we face to our critical infrastructure really is the first step to get people to sit up and pay attention, particularly the owners and operators of the infrastructures that they have responsibility for protecting.

You are correct that this was a vulnerability that we initially identified, hypothesized that this could actually happen. We understood that, as Mr. Wilshusen has pointed out, that the control systems vulnerability—we have known for some time that there are vulnerabilities in control systems. What made this one different is

that the vulnerability was susceptible to cyber attack that would have a physical impact on a structure such as a generator.

And since the time that we had gone through the mitigation strategy with the private sector, with nuclear and electric, we learned quite a lot about how to work this process. I mean, this case, this really was the first instance that we had put the National Infrastructure Protection Plan, the sector-specific plans to work. This was a model for how Federal agencies work together, to work with their private-sector counterparts. So DOE, Defense Department, DHS, several other agencies worked very closely with their industry counterparts.

We have a number of lessons learned out of that process that I can tell you we are only going to be more effective and more expeditious as we continue to look for and discover, identify vulnerabilities to various other control systems. And since nuclear and electric, we have worked with the private sectors from chemical, oil and natural gas, dams and water. And last month, in September, those industry sectors sent out mitigation strategies for their control systems.

So we are moving apace, with all due diligence and good speed, to attack these vulnerabilities very quickly.

Mr. MCCAUL. Thank you.

And Just very briefly, Mr. Roxey.

Mr. ROXEY. I would like to add to what Mr. Garcia just said, that, by pursuing and nuturing the public-private partnership model, you are going to be doing exactly what you are after. The other sectors, the water/dam, chemical, oil and gas sector, that are out there right now on their 60-day clock—that is where the 180-day clock for electric is—they are going to be calling their electric sectors in to mitigate those assets as well.

So I think that this was—and we appreciate the kudos. Thank you very much. By looking at the lessons learned from this and implementing those, I think we are only going to get better from here. Thank you.

Mr. WILSHUSEN. And I would just like to add, too, that one of the key things that both the public and private sector will need to do as they increasingly use IP protocols, in terms of being able to connect to their control systems with other company networks on the Internet, to be aware of the risk of the increased accessibility and interconnectivity. And then to learn from the examples that are legion in the regular Federal IT space, that there are significant risks and vulnerabilities associated with interconnecting systems, and to take the appropriate steps to mitigate those risks by developing the policies, procedures and controls, and then testing those techniques and controls to make sure that they are effectively implemented and operating as designed.

And then, once you have that, as we have discussed and the other members have mentioned, is to make sure to keep the lines of communication open and share this information of vulnerabilities and of new threats among all the parties within this space.

Mr. MCCAUL. Just in closing, Mr. Chairman, I think this is a great exercise and experience that we can really draw upon to have lessons learned but also use as a model for future cases.

And I want to commend the gentlemen again. Thank you.

Mr. LANGEVIN. I thank the gentleman.

And briefly, to comment on the ranking member's opening comments, in many ways there are elements of this being a good-news story. First of all, I commend the gentleman from Idaho National Labs who first detected the problem and then brought it to the attention of the Congress and also Department of Homeland Security. And then the Department of Homeland Security did put in place the Tiger Teams to try to address this.

Where we want to make sure this continues to be a good-news story is that we actually, in coming up with the mitigation strategies, that we see these strategies actually implemented. We need to have a high degree of confidence that when something of this seriousness and magnitude is identified, mitigation procedures are prescribed, that there is follow-through and not left to just hoping that it is not going to happen them or a particular sector; that they actually take it seriously, and that the electric or gas or oil sectors actually follow through and implement the strategies.

With that, the Chair now recognizes other members for questions they may wish to ask of the witnesses. In accordance with our committee rules and practice, I will now recognize members who were present at the start of the hearing, based on the seniority on the subcommittee, alternating between minority and majority. Those members coming later will be recognized in order of their arrival.

With that, the Chair now recognizes the gentleman from New Jersey for 5µminutes.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Garcia, a cybersecurity attack on our energy grid is certainly one of the emerging threats and security vulnerabilities that need to be thoroughly studied, addressed through the proper security regulations to hear what the private sector has to say about it, to hear what regulations or recommendations will come out of the Federal Government, and so we can have a meeting of the minds. We are not trying to impose, but we want to protect.

So I have had many concerns about the management over at the Department of Homeland Security. Specifically, this committee has discovered that, as was mentioned earlier, many of the most important areas within the Department are unfilled at the senior-management level, leaving critical security areas with what we would consider to be less-than-adequate leadership.

My question is, how many program managers have been in charge of the Control Systems Security Program in the last 3 years?

Mr. GARCIA. Congressman, I am not certain of the number. Our last control systems manager had been with us for more than a year.

But we at CSMC and my component, National Cybersecurity Division, take very seriously our need to retain our talent and to recruit additional talents. I am happy to report that we are aggressively filling the control systems director position. The job has been posted, and we will move aggressively to fill that, as with the other vacancies in the organization.

Mr. PASCRELL. Would you get back to me on that?

Mr. GARCIA. I would be happy to. Thank you.

Mr. PASCRELL. How much is being spent on the control systems security at DHS?

Mr. GARCIA. Our fiscal year 2008 budget is currently $12 million. And it is important to note that we are leveraging the resources not just within the control systems program but across NCSD that provides input and expertise with other aspects of the control systems issue. And additionally, we are leveraging our partnership with——

Mr. PASCRELL. What was the 2007 budget, fiscal year budget?

Mr. GARCIA. I will have to get back to you on that number. It does represent an increase.

Mr. PASCRELL. Who was in charge of this program, and at what grade is this person?

Mr. GARCIA. This is a GS–15, and this is the individual we expect to have the post filled, backfilled very quickly.

Mr. PASCRELL. There is no person there?

Mr. GARCIA. That person left for personal reasons; that is correct.

Mr. PASCRELL. Mr. Chairman—

Mr. GARCIA. It is now being handled by our acting director of the National Cybersecurity Division.

Mr. PASCRELL. My last question is this. DHS issued regulations in 2007 on chemical security. This committee, on a bipartisan basis, was very clear on what it wanted. It also added a cybersecurity component to existing regulations. Was your office consulted on this?

Mr. GARCIA. Oh, absolutely. We were part of that development, and we currently are working with all the private sectors to consider specific mitigation strategies for all of their control systems, rather than try to apply a regulatory overlay on all of the other——

Mr. PASCRELL. So, at least in this area, one hand knows what the other is doing?

Mr. GARCIA. That is correct.

Mr. PASCRELL. That is healthy. That is very healthy.

Mr. Wilshusen, in your statement, you asserted that the annual cost to the energy sector for maintaining control systems, to maintain the networks, to maintaining equipment and personnel, was around $400 million. You said that in your statement.

Can you speculate how much more would it cost if the proposed recommendations in the National Science and Tech Standards—that is 800–53—if they were adopted instead of the NERC-proposed standards, do you have any idea what the difference in cost would be? And is that relevant?

Mr. WILSHUSEN. No, sir, I don't have that information on how much that would cost.

Mr. PASCRELL. Is it relevant?

Mr. WILSHUSEN. Certainly. Relevant in terms of its consideration in implementation of controls, because when you determine whether or not to implement a particular control, you need to make sure that that control cost-effectively will reduce the risk to an acceptable level. And so, certainly, cost is a factor.

Mr. PASCRELL. So, if one set of standards implement—and I am giving an example here. Cost would be simply be one of the factors that would be involved to decide which one we would try to implement. Is that a fair statement?

Mr. WILSHUSEN. I would say cost is a factor in the determination of which controls to implement, sure. But so is the adverse impact or harm that could occur should that control not be implemented and such a vulnerability or weakness be exploited.

Mr. PASCRELL. Thank you very much.

Thank you, Mr. Chairman.

Mr. LANGEVIN. The Chair now recognizes the gentlelady from Florida, Ms. Ginny Brown-Waite.

Ms. BROWN-WAITE. Thank you very much.

I still remember when we first learned about the problem, and I couldn't help but think about whether it was TVA, with the dams, or even in Florida, where we have control structures that, you know, would have a wide range of repercussions if anything happened.

And I would like to address this to Mr. Wilshusen. While I understand the grave risks facing our control grid, could you elaborate on how the countless power and energy providers would be impacted by having to comply?

And I am sorry, you may have answered this before I got here. I apologize.

Mr. WILSHUSEN. Well, one of the things—if they are now in compliance with the NERC reliability standards, and they were to try to go implement the controls to be in compliance with the NIST standards, because the NERC reliability standards contain just a subset of the NIST standards, it would impact them to the extent that they would need to implement additional controls in order to be in compliance with those standards.

In some cases, it is also important to realize that the NIST standards and minimum security requirements, in certain cases, may not be appropriate or practical or feasible for certain control systems because of the environment that it is, but that——

Ms. BROWN-WAITE. Would you give me an example of one that it wouldn't be appropriate for?

Mr. WILSHUSEN. Here is one that the industry representatives have identified. For example, one would be having password controls over some of the control systems. Their thinking was that, in the event of an emergency, it is imperative that the operator be able to log on to their system and react immediately, and that the use of passwords could potentially disrupt that or make it more difficult for that individual to log on in a timely manner.

Ms. BROWN-WAITE. Are nuclear power plants—and I happen to have one in my district. Some people consider it a blessing; others consider it less of a blessing. Are nuclear power plants certainly at the top of the risk category?

Mr. WILSHUSEN. I would say—well, it depends on which perspective, but in terms of a security breach or vulnerability, I would say that they are probably near the top. But I really couldn't say that without specific evidence that we haven't really looked at that to see which of the industries are most at risk.

Ms. BROWN-WAITE. Okay. I appreciate that. Thank you.

And I yield back, Mr. Chairman.

Mr. LANGEVIN. I thank the gentlelady.

The gentlelady from California, Ms. Lofgren, is recognized now for 5 minutes.

Ms. LOFGREN. Thank you very much, Mr. Chairman, and to the witnesses.

I just have a couple of questions. Actually, the GAO report makes me very anxious. One of the concerns that we have had here is our exposure in the cyber area. And that is why, when Mr. Thornberry was on this committee, he and I worked together, and it was really one of those high points of my career in Congress to work in such a collaborative fashion, in a bipartisan fashion, to create the position that you now hold, Mr. Garcia, with the idea that we really needed the kind of attention that this threat was not getting.

And here is my concern, that the GAO really identifies the same deficiencies that the outside critics have identified in the scope of the NERC CIP standards and specifically on the interconnections and the possibility of cascading failures.

Ms. LOFGREN. [Continuing.] And so the question is, what are you going to do about it? What leadership are you going to show to make sure that these gaps are remedied?

Mr. GARCIA. First of all, Congresswoman, thank you very much. Thank you very much for creating the position that I now fill. I am very eager to demonstrate some very tangible accomplishments throughout my tenure here, and I think control systems rank amongst the highest.

I think we have already shown tremendous progress in control systems across the board, not just in the electric and nuclear sectors, but in the other sectors that I have mentioned that we are now taking action on. And I go back to the point that as 85 to 90 percent——

Ms. LOFGREN. Could I interrupt to follow up on that point? Are you suggesting that the points that the GAO has made and that some of the outside—I see Mr. Weiss—I always see him on the airplane—sitting in the audience—have made that you have already started the remedies on those and that you are well under way?

Mr. GARCIA. Are you talking about the electric sector specifically or just generally?

Ms. LOFGREN. Yes.

Mr. GARCIA. On the electric sector and through our private sector partners in the electric sector; and our Federal partners developed collectively mitigation strategies——

Ms. LOFGREN. So the criticism that the GAO is making on the deficiencies in the NERC standards, that is no longer accurate?

Mr. GARCIA. On the specific standards, I think that the FERC witness coming up in the next panel will have more to discuss about specific standards. Our role at DHS is one as a coordinator, to try to bring together the various parties who——

Ms. LOFGREN. Well, if I may, I don't believe that is the case, and it is certainly not what we intended in Congress. Clearly, we have a collaborative and coordinating role to play, but part of the problem is that we haven't made any progress on the cybersecurity front, or haven't for a long, long time; and we expect the Department to show some leadership.

I mean, I don't want to pick on the power industry, but this is true in any sector that is not the tech sector. They are looking at what they see, but they may not see the whole picture. And so that

is our job, to see the interconnections, to see the possibilities of interconnecting, cascading failures; and to insist that measures be taken to secure the cyber space that that sector may not see because the public's interest is larger than just their narrow interest. And I don't mean to diminish their narrow interest, but we have a broader scope here.

So the question really isn't to FERC. It is to you. What are you going to do about it?

Mr. GARCIA. Absolutely, Congresswoman. We take very seriously every sector's responsibility for securing their infrastructure. Absent regulatory authority, we are relying on the framework devised in the National Infrastructure Protection Plan and their component, sector-specific plans and our partnerships with the Federal agencies that have specific responsibility, regulatory or otherwise, to specific sectors.

Ms. LOFGREN. Let me ask you this because my time is about to run out and we also have votes on the floor.

I would like to get in follow-up to this meeting kind of where we are on the specific issues raised by the GAO and to the extent it is different from the outside critics; and then get from you your assessment of what you can do to meet the standard identified by GAO in terms of scope; and then, if you can't do it with the tools that you currently have, recommend what additional tools you think would be necessary.

Could you do that?

Mr. GARCIA. Yes, ma'am. We would be happy to come up and go through this in much more detail.

Ms. LOFGREN. Thank you very much.

I thank you, Mr. Chairman.

Mr. LANGEVIN. I thank the gentlelady for her questions. And on that very point, we are in lockstep. I agree that you should have the tools to make sure that we have these strategies put in place and acted upon. And if not, whether it is—I am not at all satisfied that enough is being done here, and if we need to give additional tools either to DHS or FERC to make sure that—particularly, when if you are talking about actionable intelligence or information that needs to be acted on quickly—that the tools are in place and we actually make sure that they have them. So the steps—that the mitigation factors take place.

So, with that, I am going to—since there are votes on, I am going to dismiss this panel. We will recess for about 20 minutes and then call up the second panel.

I thank the witnesses for their testimony.

And the subcommittee now stands in recess.

[Recess.]

Mr. LANGEVIN. The subcommittee will come to order. Let me begin by thanking the second panel of witnesses for being here today. And let me just begin by introducing and welcoming Mr. Joe McClelland, the Director of Electric Reliability for the Federal Energy Regulatory Commission. Mr. McClelland was previously Director of the Division of Reliability at FERC since 2004. He came to the Commission with more than 20 years of experience in the electric utility industry.

Thank you for being here.

Our second witness is Mr. David Whiteley, the Executive Vice President of North American Electric Reliability Corporation. Mr. Whiteley is responsible for overseeing the performance of four NERC program standards: reliability, readiness training, education and personal certification, and members' forums. Thank you for coming.

And our third witness is Mr. Joe Weiss, Managing Partner of Applied Control Solutions. Mr. Weiss is a nuclear engineer who spent more than 30 years working in the commercial power industry. He is a member of many groups working to improve the reliability and availability of critical infrastructures and their control systems.

Without objection, the witnesses' full statements will be inserted in the record.

Mr. LANGEVIN. Before I go to Mr. McClelland for his testimony, we had hoped to air a brief video before the start of the first panel, that just testified. The video was not ready. I am told that it is now ready to be shown. This will give members of the committee a visual understanding of the degree of concern I and many others have and how serious the potential problem could be with respect to the control systems being corrupted.

So, with that, I am going to ask the technical people to begin the video. I am told that everything is in order and should work. So, with that, we can start the video.

[Video plays.]

Mr. LANGEVIN. Well, that just, as I said, puts a visual to how potentially serious this problem could be if not addressed quickly.

I take this seriously; I know the ranking member does as well, and we are going to do all we can to exercise maximum oversight to ensure the worst-case scenario that was potentially spoken about in that piece we just saw never occurs.

With that, I now ask each witness to summarize their statement for 5 minutes, beginning with Mr. McClelland.

Mr. McClelland, thank you for your testimony and for being here today. Welcome.

STATEMENT OF JOSEPH MCCLELLAND, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

Mr. MCCLELLAND. Thank you, Mr. Chairman, Ranking Member McCaul and subcommittee members for providing this opportunity to appear today.

I am the Director of the Federal Energy Regulatory Commission's newest office, the Office of Electric Reliability. My office's mission is to help protect and improve the reliability and security of the Nation's bulk power system under authority granted to the Commission in the Energy Policy Act of 2005.

I am here today as a Commission staff witness. My remarks do not necessarily represent the views of the Commission or of any individual commissioner.

New section 215 of the Federal Power Act, or FPA, requires that the users, owners and operators of the Nation's bulk power system abide by mandatory reliability standards. Under the new statutory framework, these standards are developed and proposed by the Electric Reliability Organization, or ERO, to the Commission.

Standards become mandatory only after they are approved by the Commission.

To meet its obligations under section 215, the Commission has certified the North American Electric Reliability Corporation, or NERC, as the ERO. We have approved eight delegation agreements for the regional entities that will be assisting NERC in its efforts and approved 83 of 107 proposed reliability standards while simultaneously directing that 56 of the approved standards be improved.

The approved standards became mandatory on June 18, 2007. Violations of these new mandatory rules can trigger significant penalties and enforcement actions by the Commission itself, or more typically by the ERO, subject to the Commission's oversight.

Section 215 of the FPA specifically covers cybersecurity for the bulk power system. In August 2006, NERC proposed eight cybersecurity standards for the Commission's approval, requesting that auditable compliance not begin until mid-2009, continuing through 2010.

We have been reviewing NERC's proposed cybersecurity standards in our rulemaking proceeding, thereby engaging all of the affected industry and stakeholders. Using this process, the Commission has issued both a staff preliminary assessment and a notice of proposed rulemaking, considering over 1,300 pages of comments from over 100 industry and stakeholder entities.

Although the Commission has proposed to approve the standards in the Notice of Proposed Rulemaking, it has also expressed a need for immediate revisions to the standards, such as the elimination of the overly broad, quote, "reasonable business judgment," end quote, approach and narrowing of the term, quote, "technical feasibility," end quote.

Stakeholder comments on the rulemaking proceeding have raised issues concerning equipment operating costs and the appropriate scope of industry discretion. Other commenters, such as Members of Congress, including members of this subcommittee, have asked that the Commission consider and incorporate features from the standards being developed by the National Institute of Standards and Technology, or NIST. The Commission currently is considering all the comments it has received.

With respect to the NIST standards, I note that the Commission has indicated in the NOPR, or Notice of Proposed Rulemaking, that it expects the ERO to evaluate any provisions in the NIST standards that would better protect the bulk power system. If there are NIST provisions that would improve cybersecurity protection, the Commission can order the ERO to initiate a standards development process, or the ERO on its own can initiate a standards development process to incorporate such NIST provisions in the mandatory reliability standards.

In response to recent events and news reports, the Commission is examining its options for timely responses to urgent cybersecurity risks to the bulk power system. By law, the reliability standards process used by the ERO has to provide for reasonable notice, the opportunity for public comment, due process, openness and balance of interests in developing the standards.

In practice, this has meant that the reliability standards proposed by the ERO are based on consensus from industry. Con-

sequently, the process is not nimble and can take years to develop proposed standards.

The Commission is assessing ways to more promptly address urgent cybersecurity risks while protecting sensitive information involving national security. If the Commission determines that it needs additional authority to accomplish this task, it will recommend appropriate legislation to meet its responsibilities under EPAct 2005.

To protect the Nation's bulk power system, the Commission is encountering new staffing and program needs. In particular, the Commission needs more engineering to review and help develop proposed reliability standards, conduct bulk power event analyses and investigate potential violations. The Commission has requested additional funds for 2008 to be recovered through the Commission's self-funding process. I encourage you to support the Commission's efforts to obtain more funding.

In conclusion, I stress that the Commission is taking all the steps it can under its new reliability authority to protect the bulk power system and is dedicated to fulfilling Congress' goals.

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

Mr. LANGEVIN. Thank you, Mr. McClelland.

[The statement of Mr. McClelland follows:]

PREPARED STATEMENT OF JOESPH MCCLELLAND

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to appear before you to discuss the cyber threat to the electric grid's control systems. My name is Joseph McClelland. I am the Director of the new Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (Commission). The OER's mission is to help protect and improve the reliability and security of the Nation's bulk-power system through effective regulatory oversight as established in the Energy Policy Act of 2005 (EPAct 2005). I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

My testimony summarizes the Commission's recent efforts to improve the security of the Nation's electric power system. Congress's recent legislation has greatly expanded the Commission's ability to anticipate and respond to cybersecurity threats to a critical component of the Nation's infrastructure, the interstate bulk-power system. The Commission has met its statutory deadlines and provided a solid foundation for ongoing regulatory efforts. Ongoing efforts focus on the approval of Reliability Standards governing the planning and operation of the interstate bulk-power system as mandatory rules with appropriate penalties, subject to the Commission's oversight and approval.

The Commission continues to work with the North American Electric Reliability Corporation (NERC) to protect the bulk-power system from cybersecurity threats. NERC has proposed cybersecurity standards for the industry and the Commission has issued a notice of proposed rulemaking addressing these standards. The Commission is reviewing comments on these standards and is committed to ensuring that the resulting standards are consistent with and effectively implement recommendations proposed in response to the 2003 blackout affecting the Northeast United States and Canada.

The Commission is assessing its options for immediately and effectively addressing urgent cybersecurity risks to the electric system. The Reliability Standards process, which focuses on consensus from industry representatives, typically takes considerable time to implement. If the Commission determines that its authority to promptly address cybersecurity risks is inadequate, it will seek additional legislation.

As the Commission meets its responsibilities under EPAct 2005 to protect the Nation's bulk-power system, it is encountering new staffing and program needs. In particular, the Commission needs to hire more engineers to review and enforce Reliability Standards affecting the hundreds of entities that use the bulk-power system.

Therefore, the Commission has requested additional budget authority for 2008, the costs of which would be recovered through the Commission's existing self-funding process.

Background

In August 2005, Congress enacted EPAct 2005 entrusting the Commission with a major new responsibility to oversee mandatory, enforceable Reliability Standards for the electric grid. This authority is in section 215 of the Federal Power Act (FPA). Section 215 requires the Commission to select an Electric Reliability Organization (ERO). The ERO 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. 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. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

The Commission may approve proposed Reliability Standards or modifications 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, FPA 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 but, for most violations, will only review the enforcement actions of the ERO.

The Commission is qualified to perform all of these tasks and, in anticipation of reliability legislation being passed, it established a reliability group at the agency even before the passage of EPAct 2005. Commission staff played a key role in the U.S.-Canada Power System Outage Task Force formed to investigate the August 2003 blackout that affected eight states, one province and an estimated 50 million people in the U.S. and Canada. When the Task Force issued its report in April 2004 (Blackout Report), the Commission acted quickly to implement the report's recommendations addressed to the Commission. For example, the Commission announced that no new independent system operator or regional transmission organization would be approved until its reliability capabilities were functional. The Commission also adopted a policy statement on several other issues, such as recovery of prudent reliability costs, cooperation with the States, and the interpretation of reliability-related provisions in transmission tariffs. On this last point, the Commission stated that tariff requirements to follow "good utility practice" would include compliance with the then-voluntary standards developed by NERC's predecessor, the North American Electric Reliability Council.

With this experience, the Commission has been able to implement FPA section 215 diligently. 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. And, just last month, the Commission's Division of Reliability in the Office of Energy Markets and Reliability was established as its own program office, the OER, to reflect the growing importance of the Commission's reliability responsibilities.

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 and the Nuclear Regulatory Commission. And, 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.

The Commission's Proposed Cybersecurity Regulations

FPA section 215 defines "reliability standard[s]" as including requirements for the "reliable operation" of the bulk-power system and for "cybersecurity protection." Section 215 defines reliable operation to mean operating the elements of the BPS within certain limits so instability, or 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 2003, before the passage of EPAct 2005, NERC approved the "Urgent Action 1200" standard (UA 1200), the first comprehensive, although temporary, cybersecurity standard for the electric industry. This voluntary standard applied to control areas (i.e., balancing authorities responsible for ensuring that a specific area's supply matches demand at any moment in time), transmission owners and operators, and generation owners and operators that perform certain functions. Specifically, UA 1200 established a self-certification process relating to the security of system control centers.

In May 2006, NERC approved eight new cybersecurity standards to supersede UA 1200. These new standards, known as the Critical Infrastructure Protection (CIP) standards and discussed below, are broader in scope and applicability than UA 1200 and, if approved by the Commission, would be mandatory. In August 2006, NERC submitted the new standards to the Commission for approval under FPA section 215. Citing the expanded scope of facilities and entities covered by the CIP standards, and the investment in security upgrades required in many cases, NERC proposed an implementation plan under which certain requirements would be "auditably compliant" by 2009 and the others would be so by 2010.

In December 2006, the Commission issued an assessment by its staff of NERC's proposed CIP standards, and allowed 60 days for public comments. The staff's assessment was limited to a technical review, and made no final determinations on compliance with FPA section 215's legal requirements.

After receiving and analyzing the nearly 500 pages of comments from 38 entities, the Commission issued a Notice of Proposed Rulemaking in July 2007 proposing to adopt the CIP standards subject to further comment from the public. The Commission also proposed to concurrently direct NERC to develop modifications addressing specific concerns identified by the Commission.

The eight CIP standards contain over 160 requirements. Generally, the CIP standards would require the following actions:

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.

Public comments comprising more than 800 pages from 69 entities on the Commission's proposed actions were filed as of October 5. The Commission's staff has begun reviewing these comments, and the Commission intends to take final action expeditiously.

One of the Commission's goals is to ensure that the cybersecurity standards are consistent with the lessons learned from the August 2003 blackout. Thirteen of the 46 Blackout Report recommendations relate to cybersecurity. See the Blackout Report at pp. 163—69. They address topics such as strict control of physical and electronic access to operationally sensitive equipment; capability to detect wireless and remote wireline intrusion and surveillance; and improvement and maintenance of cyber forensic and diagnostic capabilities. The Blackout Report recommendations are a sound basis for action.

The Commission recognizes that the CIP standards must strike a reasonable balance. Overly prescriptive standards may become a "one size fits all" solution despite the significant differences in system architecture, technology and risk profile. However, CIP standards lacking sufficient detail will provide little useful direction, make compliance and enforcement difficult, allow flawed implementation and result in inadequate protection.

A major concern with cybersecurity is the prevalence in the industry of "legacy equipment" which may not be readily adaptable for purposes of cybersecurity protec-

tion. If this equipment is left vulnerable, it could be the focal point of efforts to disrupt the grid. Replacing this equipment or retrofitting it to incorporate cybersecurity protection could be costly. But a successful cyber attack could damage our bulk-power system and economy in ways that cost far more. This risk often may justify retrofitting the legacy equipment, adding a perimeter of defensive security measures or replacing the equipment before its useful life ends.

In its July 2007 Notice of Proposed Rulemaking, the Commission stated its concern with the breadth of discretion left to utilities by NERC's proposed CIP standards. For example, NERC's 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, NERC's proposal would allow a utility at times *not* to take certain action if the utility documents its "acceptance of risk." The Commission proposed to direct NERC to modify the standards to remove the terms "reasonable business judgment" and "acceptance of risk" while narrowing "technically feasible."

For certain other requirements in the CIP standards, the Commission proposed to address this concern about discretion by requiring external oversight of utility decisions. 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.

The National Institute of Standards and Technology (NIST) has commented that its cybersecurity standards are more advanced and could provide a model for improvements to the CIP standards. NIST has recommended that the Commission consider a transition to standards identical to, consistent with, or based on NIST standards and guidelines. The Commission's proposal so far is to not require incorporation of the NIST standards and guidelines. However, the Commission has said it would expect NERC to monitor the development and implementation of the NIST standards to determine if they would provide better protection. Certain federal entities, such as the Tennessee Valley Authority and Western Area Power Administration, are required to comply with both the NIST standards and the CIP standards, and thus may be able to provide unique insights on this issue. The Commission expressed its expectation that NERC will seek and consider comments from these federal entities on the effectiveness of the NIST standards versus the CIP standards. Any provisions in the NIST standards that will better protect the bulk-power system should subsequently be addressed in the standards development process as improvements to the CIP standards. In addition to this consideration, the Commission proposes to revisit this issue in future proceedings as part of a continuing evaluation of existing standards, the need for new standards, or as part of assessing NERC's performance as the ERO.

Confronting Urgent Risks

The procedures used so far for adoption of Reliability Standards have allowed multiple opportunities for industry and public input and taken significant time, as explained below. However, urgent risks may at times require immediate action, and the Commission currently is exploring the scope of its authority under existing law to take swift and effective action to prevent opportunities for cyber attacks or address other critical matters.

FPA 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, 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 and can take years to develop standards for the Commission's review.

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 NERC staff; drafting or redrafting of the standard by an assigned team; 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 currently under consideration, 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 will issue a "Final Rule," adopting or modifying its proposed actions.

Generally, the procedures used by NERC and the Commission are appropriate in allowing extensive opportunities for industry and public comment. The public and our economy depend critically on having a reliable supply of electricity, and Reliability Standards usually should be adopted only after thorough and open vetting of all relevant considerations.

Certain circumstances, however, may require immediate action. If a significant vulnerability in the bulk-power system is identified, procedures used so far for adoption of Reliability Standards may take too long to implement corrective steps. Also, those procedures would widely publicize the vulnerability and the possible solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

Recently, CNN broadcast a story alleging the existence of a cybervulnerability on the electric grid. The story included video of a small generating unit allegedly being damaged by a cyber attack, and also showed an economist stating that there could be a $700 billion dollar impact to our economy if generating facilities serving one-third of our Nation's electric load were disabled for three months through such attacks.

This story has prompted the Commission to reexamine its authority to quickly mitigate verified cybervulnerability risks and to protect security-sensitive information from inappropriate disclosure. If the Commission determines that it does not have adequate authority to promptly address cybersecurity risks and adequately protect security-sensitive information, or that its authority needs to be clarified, it will seek additional legislation.

The Commission Needs More Funding for Reliability

As noted above, the Commission has certified NERC as the ERO; approved the first set of mandatory and enforceable Reliability Standards (83 of NERC's initial 107 while calling for significant modifications to 56 of the 83); and approved delegation agreements between NERC and eight Regional Entities. With these steps, the Commission is well positioned to implement FPA section 215. However, more resources are needed by the Commission in all areas of reliability, including physical and cyber standards development, compliance and enforcement, investigation and analysis, and reports and assessments. In addition, the new Reliability Standards, including cybersecurity standards, will take significant work by the Commission, the ERO and the industry, and thus competition for experienced personnel, particularly engineers, is strong. Oversight of the reliability of the Nation's bulk-power system is one of the most important functions ever undertaken by the Commission and the Congress's budget support in providing necessary resources is critical.

The Commission will continue to work with the ERO and industry to strengthen Reliability Standards. Our staff will monitor and engage in the standards development process to provide timely feedback to stakeholders. NERC and industry stakeholders have requested the Commission's staff to be involved in the standards development process. We believe the process will work better if the Commission's staff is involved from the beginning, to help ensure that necessary improvements to the standards are made timely and comport with Commission directives. This is important because section 215 does not give the Commission explicit authority to revise or write the standards. Instead, the Commission can only direct the ERO to submit a standard on a specific matter or remand a proposed standard to the ERO with directions for modification, and the standards development and revision process is lengthy.

In addition, Commission staff will participate with the Regional Entities in a number of regular compliance audits and in analyzing selected incidents on the bulk-power system. Staff also will analyze and/or prepare reports on various issues concerning the reliability and security of the bulk-power system.

The Commission has moved quickly to fulfill the Congressional intent of FPA section 215. However, after we completed the actions cited above, we came to understand better the resource needs for our new reliability responsibilities. For example, approximately 1500 U.S. utilities or users of the bulk-power system are now "registered" by NERC to comply with the Reliability Standards. The Commission's jurisdiction to implement and enforce FPA section 215 for such a large number of entities serving the entire United States bulk-power system is a significant responsibility and requires a significant commitment of resources.

Thus, in June of this year, the Commission's Chairman wrote to the Chairmen and Ranking Members of the House and Senate Appropriations Committees, seeking an additional $9 million for our reliability work in fiscal year 2008. This would provide for an additional 55 Full-Time Equivalents (FTEs) to support its reliability program. These FTEs would consist primarily of electrical engineers, power system experts, auditors and lawyers. The Commission's Chairman also asked for authorization to hire electrical engineers non-competitively up to the GS–15 level, and to hire six additional executive senior level (SL) staff in support of its reliability program. As you may know, the Commission is a self-supporting agency and would recover the additional appropriations through fees and annual charges, as it does all of its costs, and will operate at no net cost to the taxpayer. I encourage you to support these requests by the Commission.

Conclusion

I stress that the Commission is taking all the steps it can to protect the bulk-power system and is dedicated to fulfilling Congress's goals. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

Mr. LANGEVIN. The Chair now recognizes Mr. Whiteley to summarize your statement for 5 minutes.

STATEMENT OF DAVID WHITELEY, EXECUTIVE VICE PRESIDENT, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. WHITELEY. Thank you, Mr. Chairman, Ranking Member McCaul and members of the subcommittee. I am pleased to appear on behalf of the North American Electric Reliability Corporation to explain how we and the electric industry are working to protect the security of the control systems of the bulk power grid.

My comments this afternoon will focus on three points: first, that NERC takes very seriously its responsibility in protecting the overall reliability of the bulk power system; second, that NERC's critical infrastructure protection, or CIP, reliability standards will enhance the cybersecurity of control systems and grid reliability; and third, that continuous improvement in NERC's reliability standards will allow for further coordination with cybersecurity standards and guidelines, such as the NIST guidelines, that are relevant for control systems.

NERC was established in 1968 with a mission to develop and implement standards to ensure the reliable operation of the bulk power system in North America. When Congress passed the Energy Policy Act of 2005, it codified this responsibility in the Federal Power Act, and Congress charged FERC with certifying an Electric Reliability Organization, or ERO, that will develop and enforce reliability standards to provide for the reliable operation of the bulk power system but only the bulk power system.

NERC is committed to exercising to the fullest extent the authority to ensure grid reliability within the limits provided in the law.

The Energy Policy Act expressly excluded local distribution facilities from the definition of bulk power system. That said, NERC has worked diligently to implement the reliability authority as FERC's certified ERO.

The system of voluntary standards administered by NERC for more than 30 years was replaced on June 18 with a new set of mandatory reliability standards applicable to all users, owners and operators of the bulk power system.

NERC realizes that cybersecurity of grid control systems is an important element of the overall reliability of the system and has

been an increasing priority for every sector of the U.S. economy since the turn of the century. NERC has recognized and responded to this challenge first through the voluntary cybersecurity standard and now through proposed mandatory CIP reliability standards. FERC approval of the standards, along with parallel action by Canadian authorities, will enhance the reliability of the transmission grid in North America. These standards will improve the resiliency of control systems' cyber assets and increase the ability of these systems to withstand cyber-based attacks. Cybersecurity requirements will be applied to functions and to companies that have never been subject to standards in the past.

In the course of developing the CIP standards, NERC evaluated NIST's ongoing work to apply its recommended security controls for Federal information systems along with other NIST work to the bulk power system. NERC determined, and FERC agreed, that the NIST guidelines cannot substitute for reliability standards developed specifically for the bulk power grid. The existing guidelines from NIST for information security are not directly applicable to control systems.

NIST has continued to work in this area and has released additional draft guidance. However, because mandatory cybersecurity standards to secure grid reliability are needed now, issuance of the CIP reliability standards could not be delayed in order to await completion of the NIST process. In addition, the substitution of NIST guideline development for information systems into a mandatory reliability standard for electric grid control systems would not meet the requirements of the Federal Power Act that governed the process and procedures developed by NERC.

Another consideration is that the bulk power system is interconnected within North America. This means that the bulk power system reliability standards must also be recognized in Canada, and the NERC standards development process requires Canadian input. Because the NIST guideline development process does not have to take into account the international aspect of the bulk power grid, they would not necessarily be applicable for cross-border application.

We will evaluate how all of our reliability standards work in practice, will monitor industry and technology developments and determine on an ongoing basis whether these standards should be improved or new standards should be developed.

In summary, the key to improving the reliability of the North American power system is to put good standards in place as soon as possible and then make them better. The CIP reliability standards are a sound starting point for the electric industry, and with regard to cybersecurity issues, a sound starting point as well. They can and should be made effective promptly.

This concludes my prepared remarks, and I look forward to answering your questions.

Mr. LANGEVIN. Thank you, Mr. Whiteley.

[The statement of Mr. Whiteley follows:]

PREPARED STATEMENT OF DAVID A. WHITELEY

Mr. Chairman and Members of the Subcommittee, the North American Electric Reliability Corporation[1] ("NERC") is pleased to provide this testimony on how we and the electric industry are working to protect the security of the control systems for the bulk power grid throughout North America pursuant to the authority set forth in Section 215 of the Federal Power Act ("FPA"), as enacted through the Energy Policy Act of 2005 ("EPAct 2005").[2] Protecting the overall reliability of the bulk power system, including ensuring the security and reliability of grid control systems, has been a high priority for NERC since well before the enactment of EPAct 2005, and we take this matter very seriously. As the Committee is aware, under the authority of FPA Section 215, NERC has proposed eight Critical Infrastructure Protection Reliability Standards for approval by the Federal Energy Regulatory Commission ("FERC" or "Commission"). FERC approval of the standards that NERC has proposed in this area, along with parallel action by appropriate governmental authorities in Canada, will enhance the cybersecurity of these control systems and the reliability of the interconnected electric transmission grid.

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 proposed mandatory Critical Infrastructure Protection ("CIP") Reliability Standards for the bulk power grid. These mandatory standards are intended to assure that the electricity industry will devote the necessary organizational resources to securing control systems, and that the industry will identify, respond to and report cyber security incidents related to critical cyber assets.

Since its establishment in 1968, NERC's mission has been the development and implementation of standards to ensure the reliable operation of the interconnected North American bulk power electric grid in the U.S. and Canada and Mexico. The system of voluntary standards administered by NERC for more than 30 years was replaced on June 18, 2007, with a new set of mandatory Reliability Standards applicable to all users, owners and operators of the "bulk power system." NERC stands ready to take additional steps as warranted to protect the reliability and cybersecurity of the grid.

Mandatory and enforceable Reliability Standards under Section 215 of the FPA are to provide for the reliable operation of the bulk power system only. Section 215 expressly excludes local distribution facilities from the definition of "bulk power system." Moreover, Section 215 does not extend any authority for the regulation of reliability or cybersecurity beyond that which is necessary for reliable operations of the transmission grid. While critical infrastructures in various sectors of the U.S. economy are dependent upon the bulk power system, NERC's authority to propose and enforce reliability standards is confined to a single sector of the economy.

We will evaluate how all of our Reliability Standards work in practice, monitor industry and technology developments, and determine on an ongoing basis whether these Standards should be improved, or new standards should be promulgated. The key to improving the reliability of the North American bulk power system is to put in place good standards, as soon as possible. The CIP Reliability Standards are a sound starting point for the electric industry. They can and should be made effective promptly so that they can be implemented now.

In the course of developing the CIP Reliability Standards, NERC evaluated the National Institute of Standards and Technology's ("NIST") ongoing work to apply its Special Publication (SP) 800–53, Recommended Security Controls for Federal Information Systems, to control systems, and other work underway at NIST to develop guidance on securing control systems. However, the need for mandatory cybersecurity standards to secure grid reliability is immediate, and issuance of the CIP Reliability Standards could not be delayed in order to await completion of the NIST process.

Importantly, bulk power system reliability standards also must be acceptable to regulators in Canada and Mexico. We are not addressing only U.S. facilities with these standards. The NERC standards development process provides a carefully crafted mechanism designed to ensure that final standards proposals have been de-

[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 FPA.

[2] Energy Policy Act of 2005, Pub. L. No. 109–58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005).

veloped with Canadian (and Mexican, where appropriate) input. Because the NIST guideline development process does not have to take into account the international aspect of the bulk power grid, the U.S. government standards for U.S. government facilities resulting from that process would not necessarily be acceptable.

Moreover, there are also important substantive and process-related reasons why any future final NIST guidelines cannot substitute for Reliability Standards developed specifically for the bulk power grid. First, the guidelines available from NIST for information security when the CIP Reliability Standards were being developed were not appropriate for control systems. Second, Section 215 of the FPA sets forth requirements for the process and procedures through which NERC, as the ERO, may establish Reliability Standards. FERC has approved the NERC standards-setting process. The conversion of a NIST guideline developed for information systems directly into a mandatory Reliability Standard for electric grid control systems would not comply with the statutory procedural requirements under which NERC operates.

NERC will continue to monitor the progress of the NIST process, and as CIP Reliability Standards continue to evolve, there will be future opportunities to continue to reflect NIST documents and guidance as appropriate.

I. *BACKGROUND*

A. NERC.

NERC's mission is to ensure 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 future adequacy; evaluates owners, operators, and users for reliability preparedness; and educates, trains and certifies industry personnel. NERC is a self-regulatory organization that relies on the diverse and collective expertise of industry participants. FERC certified NERC as the electric reliability organization ("ERO") in July 2006.[3]

Because Reliability Standards are applicable to the entire, interconnected North American bulk power system, NERC is subject to oversight by the governmental authorities in both Canada and the United States. In the U.S., with oversight from FERC, as of June 18, 2007, NERC has legal authority to enforce reliability standards applicable to all owners, operators, and users of the bulk power system, rather than relying on voluntary compliance. NERC is seeking similar recognition by governmental authorities in Canada, including eight provinces and the National Energy Board, and will seek recognition in Mexico at the appropriate time.

B. Statutory Authority Over Bulk Power System Reliability.

Section 215 of the Federal Power Act establishes the framework for mandatory and enforceable Reliability Standards applicable to all users, owners and operators of the bulk power system. Section 215 assigns to the Commission the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk power system. Section 215 requires the Commission to issue rules for the certification of an ERO charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215 also gives the Commission the regulatory responsibility to approve standards that protect the reliability of the bulk power system.

Consistent with the law, the development and enforcement of Reliability Standards is now the responsibility of the ERO. As noted above, FERC's certification of NERC as the ERO places this responsibility squarely on NERC. However, NERC's authority pursuant to Section 215 relates solely to ensuring the reliability of the bulk power system. FPA Section 215(a)(1) defines the term "bulk power system" to mean

> (A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and
>
> (B) electric energy from generation facilities needed to maintain transmission system reliability.

The statutory definition expressly excludes "facilities used in the local distribution of electric energy."

FPA Section 215 defines the term "Reliability Standard" to mean:

a requirement, approved by the Commission. . .to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to

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

provide for reliable operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.

FPA Section 215(a)(3). Under FPA Section 215(a)(4), "reliable operation," as used in the definition of Reliability Standard, means operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.

The statute also defines a "cybersecurity incident" that the Reliability Standards developed by the ERO are to guard against:

"cybersecurity incident" means 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.*

FPA Section 215(a)(8) (emphasis supplied).

Congress spent eight years considering the need for reliability legislation and refining the legislative language, choosing its words carefully to be very specific about the extent of and limitations on the jurisdiction of FERC and the ERO with respect to enforceable reliability standards. Congress also was clear that it wanted to capture the expertise of the industry in developing Reliability Standards and in monitoring and enforcing compliance with Standards through an audited self-regulatory system. For this reason, and because Reliability Standards apply not only in the U.S. but also in Canada, FERC's role is one of approving standards, not developing them in the first place, and in overseeing the activities of the ERO. FPA Section 215(d)(2) provides that in executing its responsibilities to review, approve and enforce mandatory reliability standards, the Commission is authorized to approve those proposed standards that the Commission finds are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Moreover, the Commission "shall give due weight to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed reliability standard. . . ." Further, the statute requires that in applying its expertise and developing Reliability Standards, the ERO certified by the Commission must have established rules that "provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards. . . ." *See* FPA section 215(c)(2)(D).

II. *RESPONSE TO ISSUES IDENTIFIED BY THE COMMITTEE*

A. NERC's Authority To Prescribe Critical Infrastructure Protection Rules Is Limited To The Electric Power Sector Only And Does Not Extend To Regulation Of Distribution Systems Or Other Infrastructures.

As described above, the authority granted to the ERO pursuant to Section 215 of the Federal Power Act is not unlimited. FPA Section 215 does not convey authority to apply mandatory and enforceable reliability standards to the distribution system. The authority of the ERO extends only to elements of the bulk power system as defined in the statute. The only entities that under the law must comply with ERO-developed reliability standards are "users, owners and operators of the bulk-power system." Subject to FERC's approval, NERC has developed a compliance registry that identifies these entities, consistent with the statutory requirements.

The standards that NERC has proposed to the Commission are consistent with Section 215 of the FPA. We believe those standards, when taken as a whole and as they develop over time, will continue to provide a level of reliability that is commensurate with the statutory requirements.

B. The CIP Reliability Standards Were Developed Through A Rigorous Process That Took The NIST Guidance Into Account.

Section 39.5(a) of the Commission's regulations requires the ERO to file with the Commission for approval each reliability standard the ERO proposes to become mandatory and enforceable in the United States, and each proposed modification to a reliability standard. NERC and the Commission have made substantial progress in proposing and approving reliability standards to be mandatory and enforceable in the United States. NERC filed a petition for approval of 102 existing Reliability Standards in FERC Docket No. RM06–16 on April 4, 2006. NERC filed a second petition for the approval of proposed reliability standards August 28, 2006, submitting 16 new standards for approval and revisions to 11 of the reliability standards previously submitted. Of the 16 new standards submitted, eight were Critical Infrastructure Protection cyber security standards.

On December 11, 2006, the Commission Staff issued an assessment of the cyber security standards as a basis to solicit comments on those proposed standards. On July 20, 2007, the Commission issued a Notice of Proposed Rulemaking ("NOPR") generally proposing to approve the CIP Reliability Standards as mandatory and enforceable, while also proposing to require NERC to make specific modifications to certain of the standards.[4] The deadline for comments on the NOPR was October 5, 2007, and the Commission has received approximately 100 comments on the staff assessment and the proposed standards.

1. Background of Proposed Cyber Security Standards.

The initial work on the proposed cyber security standards dates back to 2002 when NERC's Critical Infrastructure Protection Advisory Group ("CIPAG")[5] drafted cyber security language that ultimately appeared in Appendix G of the Commission's "Standard Market Design' NOPR.[6] Since then, NERC has continued to raise the bar on cyber security, first by adopting Cyber Security Urgent Action Standard 1200 in 2003,[7] and again with the proposed standards filed with the Commission in August 2006.

Reflecting Congress's objective in FPA Section 215 that industry expertise should be brought to bear in the development of Reliability Standards, the proposed cyber security standards have been crafted with significant industry input by experts in the area and a debate of key issues through a process accredited by the American National Standards Institute ("ANSI"). The Standard Authorization Request ("SAR") for the cyber security standards was submitted to NERC on May 2, 2003. After two public comment periods, the industry reached a consensus on the scope and justification for the standards. The Standards Authorization Committee ("SAC") appointed a drafting team of security experts to begin development of these standards in May 2004.

Drafting team members brought significant experience and expertise from a broad spectrum of security related disciplines including information technology security, physical security, compliance auditing, personnel and training, energy management systems ("EMS"), and system control and data acquisition ("SCADA") system operations. Drafting team members also brought expert knowledge of existing government regulations affecting security such as Sarbanes-Oxley and the Federal Information Security Management Act of 2002 ("FISMA"), as well as existing security related standards such as International Standards Organization ("ISO") Standard 17799 and the body of work promulgated by NIST. A number of members of the drafting team held professional security certifications. Membership on the drafting team fairly represented ownership segments in the electric industry and a balance between U.S. and Canadian participation.

---

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection,* Docket No. RM06–22, 120 FERC ¶ 61,077 (2007). FERC's NOPR described the proposed CIP Reliability Standards as "the most thorough attempt to date to address cyber security issues that relate to the Bulk-Power System." NOPR, P 13. Given the nature of the cyber security threat, the Commission acknowledged that "cyber security strategies must comprise a layered, interwoven approach to vigilantly protect the Bulk-Power System against evolving cyber security threats." NOPR, P 15. FERC proposed to approve NERC's proposed Implementation Plan for the CIP Reliability Standards, which sets forth "a timeline by calendar quarters for completing various tasks and prescribes milestones for when a responsible entity must: (1) "begin work;" (2) "be substantially compliant" with a requirement; (3) "be compliant" with a requirement; and (4) "be auditably compliant" with a requirement." NOPR, PP 43,47. FERC also proposed to approve the 162 proposed Violation Risk Factor assignments proposed by NERC that correspond to the requirements of the CIP Reliability Standards and to direct NERC to revise 43 of them, as well as to assign Violation Risk Factors to additional requirements under the CIP Reliability Standards. NOPR, P 325. Violation Risk Factors indicate the potential or expected impact to the reliability of the Bulk-Power System of the violation of a particular Reliability Standard requirement. Violation Risk Factors are used by NERC in setting penalty amounts for violations of a Reliability Standard.

[5] The CIPAG was a predecessor organization to NERC's current Critical Infrastructure Protection Committee ("CIPC").

[6] *Remedying Undue Discrimination through Open Access Transmission Service and Standard Electricity Market Design, Notice of Proposed Rulemaking,* 67 Fed. Reg. 55,452 (Aug. 29, 2002), FERC Stats. & Regs. ¶ 32,563 (2002). The Standard Market Design NOPR was never finalized.

[7] Cyber Security Urgent Action Standard 1200 was a voluntary standard that applied to control areas, transmission owners and operators, and generation owners and operators performing certain specific functions. The voluntary standard established a self-certification process relating to the security of system control centers of covered entities. The Urgent Action 1200 standard was effective on a voluntary basis until June 1, 2006, when it was replaced by the eight CIP Reliability Standards that are the subject of the current FERC rulemaking.

Throughout the development process, the drafting team insisted on looking beyond generally accepted "best practices." They sought to establish relevant, thorough requirements with unambiguous measures for determining compliance. Three versions of the cyber security standards were posted to solicit input from the industry and other interested parties. More than 2,500 pages of comments and responses to the comments were provided in response to the three postings of the draft standards. The fourth and final version was submitted to ballot of the stakeholders. The number and volume of comments received represented an extraordinary level of involvement by the industry during the development process.

2. NERC's CIP Reliability Standards Proposal.

In the August 2006 submission to FERC, NERC proposed eight new cybersecurity standards (CIP–002–1 to CIP–009–1) to provide a comprehensive set of requirements to protect the bulk power system from malicious cyber attacks. Because there are unique aspects of cyber protection for each entity and its assets, the standards require bulk power system owners, operators, and users to step through a sequence of establishing a risk-based vulnerability assessment method and using that method to identify and prioritize critical assets and critical cyber assets. Once the critical cyber assets are identified, the standards require the responsible entities to establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. The proposed cyber security standards propose the most comprehensive set of requirements ever utilized on a widespread basis in the electric industry.

Because of the expanded scope of facilities and entities covered by these standards, and the investment in security upgrades required in many cases, the implementation plan calls for a three-year phase-in to achieve full compliance with all requirements. The transition builds progressively from the requirements that were previously in place with the 1200 Urgent Action Standard. In other words, the industry is improving its security measures in stages from the level established in 2003 with the interim standard to an extraordinarily robust set of auditable requirements by end of year 2009.

The proposed standards will apply to 11 categories of "Responsible Entities," including NERC itself, the Regional Reliability Entities, reliability coordinators [which may include Regional Transmission Organizations or Independent System Operators], balancing authorities, interchange authorities, transmission service providers, transmission owners, transmission operators, generator owners, generator operators, and load serving entities. As set forth in the NOPR, the proposed standards address:

- **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 critical cyber assets identified pursuant to CIP–002–1.
- **CIP–004–1—Cyber Security—Personnel & Training:**
Requires personnel with access to critical cyber assets to have an identity verification and a criminal check. Also requires employee training.
- **CIP–005–1—Cyber Security—Electronic Security Perimeters:**
Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the risk-based assessment methodology required by CIP–002–1.
- **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 cyber security standards proposed by NERC provide firm requirements that can be implemented by all participants in the electricity sector regardless of size, staffing levels, or levels of sophistication. Some members of the electricity sector already meet or exceed the proposed standards. However, the standards may be a significant burden on some entities that have not heretofore been required to implement cyber security programs. Throughout the development process, the drafting team attempted to push the bar beyond the generally accepted industry best practices, and to ensure that every component part has at least the minimum protection necessary to protect the reliability of the bulk power system as a whole. The resulting standards represent a balanced set of outcomes in a diverse industry. These standards are rigorous, but compliance can be achieved by all "owners, operators and users" of the bulk power system.

The proposed cyber security standards fulfill relevant portions of Recommendations 32 and 32.A of the *United States/Canada Power System Outage Task Force* report. These recommendations state, in part, that NERC should finalize and implement the CIP–002–1 to CIP–009–1 standards, that NERC standards related to physical and cyber security should be made mandatory and enforceable, and that NERC should take actions to better communicate and enforce these standards. To help the industry understand and implement these standards, NERC held a series of ten industry workshops on the standards for bulk power system owners, operators, and users that were conducted across North America.

NERC also believes that these cyber security standards are a landmark for the implementation of mandatory cyber security in a non-business environment. These standards represent, for the first time, a set of mandatory security requirements for an entire industry. Other statutory and regulatory attempts have not been as proscriptive or as specific as these standards.

These proposed standards are different from traditional information technology security standards. The CIP Reliability Standards apply information technology security principles, which are commonly accepted in the business environment, to bulk power system control systems which were not designed with these security principles in mind. As such, the security principles must be carefully applied to ensure that there are no unintended consequences that undermine bulk power system reliability. These standards must prescribe what is required of real-time critical bulk power system operating systems. This differs from what can be prescribed for secured business systems.

Promulgating standards for the bulk power system that draw too closely on the standards appropriate for secured business systems could result in a *less reliable* bulk power system, either because of decreased operations or decreased security. Two examples of this are (1) the use of password-protected screen savers on computers, and (2) automatic lockout of accounts following invalid passwords. Both of these are accepted business system security practices, but they lead directly to reduced ability to reliably operate a real-time control system, and thus to a less reliable bulk power system. In the case of a password-protected screensaver, the business justification is to reduce the release of confidential information or misuse of the computing resources; in a control system, it results in a lack of visibility of key real-time operating parameters that must be constantly observed to ensure reliable operations. In the case of password lockout, business systems use the lockout as a preventative measure to ensure that information and computer resources cannot be used following an concerted attack; in a control system the need to rapidly be able to get access to a system under all circumstances may result in mis-typed passwords, which could lead to the complete inability to monitor or take corrective actions to maintain reliable operations. In both cases, control systems implement alternate mitigating controls, including increased physical security and additional personnel that the business systems cannot assume, to ensure that the systems are not misused.

The proposed cyber security standards will increase the reliability of the bulk power system by improving the resiliency of the control system cyber assets and improving their ability to withstand cyber-based attacks. Cyber security requirements will be applied to functions and companies where they have never before been applied. NERC has applied cyber security standards to control centers through prior standards; however, the Standards currently before the Commission are the first to require cyber security in either a substation or generating plant environment.

3. Interaction Between NERC and NIST Processes.

The FERC NOPR addresses the relationship between the CIP Reliability Standards and other existing standards for cyber security, both governmental standards and industrial standards. See NOPR, PP 87—88. Specifically, the Commission received a recommendation that Federal Information Processing Standards ("FIPS") 199, FIPS 200, and NIST Special Publication 800–53 Revision 1, Recommended Security Controls for Federal Information Systems ("SP 800–53") be used as the basis for cyber security requirements applicable to the electric power sector. The National Institute of Standards and Technology recommended that FERC consider a transition to cyber security standards identical to, consistent with or based on SP 800–53 and related guidelines.

The Commission declined to propose such a transition in the NOPR:

> The Commission declines to propose at this time that NERC incorporate any provisions of the NIST standards into the CIP Reliability Standards. However, the Commission expects NERC to monitor the development and implementation of the NIST standards to determine if they contain provisions that will better protect the Bulk-Power System. Several federal entities, such as the Tennessee Valley Authority and Western Area Power Administration, are subject to both the NIST standards and the Reliability Standards, and therefore are likely to have unique insights into the NIST standards. The Commission expects the ERO to seek and consider comments from those federal entities on the effectiveness of the NIST standards and on any implementation issues. Any provisions that will better protect the Bulk-Power System should be addressed in the ERO's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new Reliability Standards, or as part of assessing NERC's performance of its responsibilities as the ERO.

NOPR, P 88 (footnote omitted).

NERC agrees fully with the Commission's determination. During the development of the CIP Reliability Standards discussed above, participants in the standards development process acknowledged that NIST's existing FISMA guidance is not appropriate for control systems. NIST has continued its work in this area, and has developed guidance, which is still in the draft stage, on applicable actions to be performed in support of FISMA compliance to control systems. To date, NIST has released two public draft versions of its revised guidance (in July 2005 and June 2007). As of this date, however, the guidance has not been approved by NIST, nor issued in final form. Given the importance of the cybersecurity standards and the critical need to have standards in place and enforceable as soon as possible, it would not have been appropriate to delay the NERC standards development process in order to await the final outcome of the NIST process.

Additionally, as described above, NERC's procedures for the development of reliability standards are governed by the Federal Power Act. In certifying NERC as the ERO, FERC approved NERC's ANSI-approved standards development process as consistent with the statutory requirements. This ANSI-approved process is essentially the same as that used by other standards organizations, including the IEEE, ISA, and ANSI itself. In contrast, the NIST process is not an ANSI-accredited process, and does not include a stakeholder ballot. As all of the Reliability Standards developed by NERC and submitted to FERC for approval must be developed through the FERC-approved ANSI process, NERC cannot simply adopt a NIST guideline as a Reliability Standard. While the NIST proposals can be (and have been) considered in the ERO standards development process, the resulting standard cannot be the NIST document or guideline.

C. While Interdependency Is A Significant Issue, The CIP Reliability Standards Can Only Address Critical Assets In The Electricity Sector.

Another issue addressed in the NOPR, and in the FERC staff assessment proposed CIP–002–1 regarding the identification of critical assets, concerned the "interdependency" with other infrastructures. The staff assessment asked for comments on whether CIP–002–1 should address this matter, and whether there should be coordination and collaboration in the future with other industries and government agencies. In the NOPR, FERC concluded that:

> While broader interdependency issues cannot be ignored, the Commission intends to revisit this matter through future proceedings and with other agencies. This work will help to inform the electric sector and this Commission about the need for future Reliability Standards, especially when the interdependent infrastructures affect generating capabilities, such as through fuel transportation.

NOPR, P 118.

NERC concurs that the interdependency issue raised in the NOPR is an important one; however, the issue is too broad to be restricted to a single agency or industry sector. We believe that it is best raised through direct cooperation with other critical infrastructure sectors through existing cross-sector initiatives such as the Partnership for Critical Infrastructure Security ("PCIS") and the Information Sharing and Analysis Center Council ("ISAC Council"), with the lead federal government agency being the U.S. Department of Homeland Security. Once specific issues directly relating to the reliability of the bulk-power system are identified through these organizations, standards creation activities can be initiated through the ERO to address them.

III. *CONCLUSION*

The approval by FERC of the proposed CIP Reliability Standards will represent an important milestone in the transition to the system of mandatory and enforceable reliability standards envisioned by Congress in the Energy Policy Act of 2005, that will ensure grid reliability by improving the resiliency of the control system cyber assets and improving their ability to withstand cyber-based attacks.

Going forward, standards development requires progressive and continuous improvement. NERC's rules, and a condition of accreditation by the American National Standards Institute, require that each standard be reviewed at least every five years. NERC anticipates completing the review and upgrade of all standards over a three-year period, beginning with the highest priority standards in 2007. NERC's standards development procedure provides a systematic approach to improving to the standards and documenting the basis for those improvements, and should serve as the mechanism for achieving those improvements.

These CIP Reliability Standards already represent a significant improvement of cyber security for the electricity industry. Since our process requires that standards be continuously improved, the standards will be reviewed, modified and improved by necessity of the process. This will result in an ever-increasing improvement to the level of cyber security throughout the electricity industry. However, the process must start somewhere with a set of standards. Based on NERC's development process, and the demonstrated broad base of support, the standards currently before the Commission represent the most appropriate starting point for today's environment.

SUMMARY:

Mandatory and enforceable Reliability Standards under Section 215 of the Federal Power Act are to provide for the reliable operation of the bulk power system only. Section 215 does not extend any authority for the regulation of reliability or cybersecurity beyond that which is necessary for reliable operations of the transmission grid. While critical infrastructures in various sectors of the U.S. economy are dependent upon the bulk power system, NERC's authority to propose and enforce reliability standards is confined to a single sector of the economy.

NERC will evaluate how all of Reliability Standards work in practice, monitor industry and technology developments, and determine on an ongoing basis whether these Standards should be improved, or new standards should be promulgated. The key to improving the reliability of the North American bulk power system is to put in place good standards, as soon as possible. The CIP Reliability Standards are a sound starting point for the electric industry. They can and should be made effective promptly so that they can be implemented now.

In the course of developing the CIP Reliability Standards, NERC evaluated NIST's ongoing work to apply its Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, to control systems, and other work underway at NIST to develop guidance on securing control systems. The guidelines available from NIST for information security when the CIP Reliability Standards were being developed were not appropriate for control systems. Moreover, Section 215 of the FPA sets forth requirements for the process and procedures through which NERC, as the ERO, may establish Reliability Standards. The conversion of a NIST guideline developed for information systems directly into a mandatory Reliability Standard for electric grid control systems would not comply with the statutory procedural requirements under which NERC operates. Because of the pressing need for mandatory cybersecurity standards to secure grid reliability, issuance of the CIP Reliability Standards could not be delayed in order to await completion of the NIST process. NERC will continue to monitor the progress of the NIST process, and as CIP Reliability Standards continue to evolve, there will be future opportunities to continue to reflect NIST documents and guidance as appropriate.

Mr. LANGEVIN. The Chair now recognizes Mr. Weiss to summarize your statement in 5 minutes.

STATEMENT OF JOSEPH M. WEISS, MANAGING DIRECTOR, APPLIED CONTROL SOLUTIONS

Mr. WEISS. Good afternoon, Mr. Chairman, Ranking Member McCaul and members of the committee. I would like to thank the committee for your commitment to a comprehensive examination of the cybersecurity of control systems utilized in our Nation's electric grid. I also want to thank you for the opportunity to be here today to discuss this very important topic.

As you mentioned, I am a nuclear engineer that has been involved in control systems for over 35 years and control systems cybersecurity specifically for over 7 years. I have been part of the NERC cybersecurity standards process since its inception. I have been working with government organizations, end users, equipment suppliers, domestic and international standards organizations and others. I am also a utility stockholder and ratepayer, both of which can be affected by what we are discussing today.

The issue at hand is the protection of the interdependent critical infrastructures of electric power, water, oil, gas, et cetera. Control systems form the backbone of these infrastructures, and the threat of a cyber attack is the central issue. There are only a handful of control systems suppliers, and they supply industrial applications worldwide.

The control systems architectures and default passwords are common to each other. Consequently, if one industry is vulnerable, they all could be. I am aware of more than 90, 9–0, cases where control systems have been impacted by either intentional or unintentional incidents. These incidents have occurred in electric power transmission and distribution systems, power generation including fossil, hydro, gas turbine and nuclear, water, oil, gas, chemicals, paper and agribusiness. The damage from the cyber incidents has ranged from trivial to significant environmental releases to significant equipment damage to even deaths.

When the NERC cybersecurity standards process originated, it was meant to address utility control systems with the only exclusion being mainstream business applications. Over time, the scope significantly narrowed. The approach has resulted in the following shortcomings: the ambiguousness and exclusions of the NERC CIP process, and this includes telecom, electric distribution, market systems, serial communications, nuclear plants; and even the fact of not requiring actual appropriate control systems policies would not meet a cybersecurity assessment of the human resources computer system, yet we are using this as a basis for our most important critical cyber assets. The banking industry is concerned about the security of a single open access point on a laptop. On the other hand, the electric industry is determined by using the NERC substandards that an entire section of the United States has no critical generation assets. How can this be considering NERC's input on the aurora vulnerability?

In my written testimony, I have provided four actual control system cyber events the NERC substandards would not have addressed, including one that was identified in an electric sector ISAC advisory in 2003. This is not aurora. As can be seen, this lack of any real security being addressed by NERC is alarming at best and negligent at worst.

There is a better approach that, in fact, is already mandatory for all Federal agencies, which includes TVA, BPA, and the Bureau of Reclamation among others. This approaches the NIST framework, which has been expanded to specifically address control systems. We have conducted a line-by-line review between the NERC CIPs and NIST 800–53; the results were that NIST 800–53 is more comprehensive.

Why should Federal power agencies be held to a higher standard? But, more so, why should they be placed at risk where non-Federal agencies connect with them using a less comprehensive approach? This doesn't make any sense.

My recommendation is, Congress should empower FERC with the authority and responsibility for development of control systems cybersecurity requirements and compliance criteria similar to the role of the Nuclear Regulatory Commission. In so doing, Congress should also provide FERC with the authority to separate ERO

VerDate Nov 24 2008 13:19 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00051 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-78\48973.TXT HSEC PsN: DIANE

functions so that NERC is responsible for traditional electric system reliability standards, and have a separate organization, very possibly ISA, be responsible for the cybersecurity aspects of critical infrastructure protection.

Finally, Congress should take action so that the ERO function is funded by the government, not by industry as is now the case, to better ensure that conflicts of interest do not interfere with doing what is right and necessary and not just what is convenient.

Thank you for allowing me to provide my thoughts and concerns, and I would be happy to answer any questions.

[The statement of Mr. Weiss follows:]

PREPARED STATEMENT OF JOSEPH M. WEISS

Good afternoon Mr. Chairman and Members of the Committee. I would like to thank the Committee for your invitation to discuss the need for appropriate cyber security of the control systems utilized in our nation's critical infrastructure, in particular, the electric infrastructure.

I am a nuclear engineer who has spent more than thirty years working in the commercial power industry designing, developing, implementing, and analyzing industrial instrumentation and control systems. I have performed cyber security vulnerability assessments of power plants, substations, electric utility control centers, and water systems. I am a member of many groups working to improve the reliability and availability of critical infrastructures and their control systems, including the North American Electric Reliability Council's (NERC) Control Systems Security Working Group (CSSWG), the Instrumentation Systems and Automation Society (ISA) S99 Manufacturing and Control Systems Security Committee, the National Institute of Standards and Technology (NIST) Process Control Security Requirements Forum (PCSRF), Institute for Electrical and Electronic Engineers (IEEE) Power Engineering Society Substations Committee, International ElectroTechnical Commission (IEC) Technical Committee 57 Working Group 15, and Council on Large Electric Systems (CIGRE) Joint Working Group D2.22. As a control system cyber security expert, citizen, stockholder, and ratepayer, I am very concerned about the electric industry's approach to securing the electric grid. I would like to state for the record that the views expressed in this testimony are mine. I am not representing any of the groups in which I am involved.

Until 2000, my focus strictly was to design and develop control systems that were efficient, flexible, cost-effective, and remotely accessible, without concern for cyber security. At about that time, the idea of interconnecting control systems with other networked computing systems started to gain a foothold as a means to help lower costs and improve efficiency, by making available operations-related data for management "decision support." Systems of all kinds that were not interconnected with others and thereby could not share information ("islands of automation") became viewed as an outmoded philosophy. But at the same time, there was no corresponding appreciation for the cyber security risks created. To a considerable extent, a lack of appreciation for the potential security pitfalls of highly interconnected systems is still prevalent today, as can be witnessed in a recent article in the September 2007 issue of Power Magazine.[1] As such, the need for organizations to obtain information from operational control system networks to enable ancillary business objectives has often unknowingly led to increased cyber vulnerability of control system assets themselves.

Generally cyber security has been the purview of the Information Technology (IT) department, while electric control system departments have focused on grid and plant operations efficiency and reliability—not cyber security. This has led to the current situation where some parts of the organization are now sensitized to security while others are not as yet aware of the need. Industry has made progress in identifying control system cyber security as an issue while not appreciating the full gravity of the matter. In other ways, particularly concerning the proposed NERC Critical Infrastructure Protection (CIP) cyber security standards,[2] I believe we have fallen short of the mark. The timing of this hearing is fortuitous as more than 70

[1] Makansi, Jason, "Integrated Software Platform Eludes Many Owner/Operators", *Power Magazine*, September 2007.

[2] NERC Cyber Security Standards, http://www.nerc.com/filez/StandardsStandards/Cyber-Security-Permanent.html

organizations have recently submitted commentary responses to the Federal Energy Regulatory Commission's (FERC) Notice of Proposed Rulemaking (NOPR) RM06–22.[3] These submittals provide a detailed view into the electric power industry's intended approach to securing the cyber assets used to operate the grid.

How Mainstream IT and Control System Cyber Security are Different

Control systems include distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems, and related networked-computing systems. Control systems are designed and operated differently than mainstream IT business systems. Traditionally, the emphasis in securing business IT systems is to employ the best practices associated with the well-established "Confidentiality, Integrity, Availability" (CIA) triad model—in that order of importance. Typically extra emphasis is placed on rigorous human end user access control and data encryption to satisfy the important function of confidentiality. In control systems, however, confidentiality has less urgency than system availability and data integrity, because in actual control system operation, the typical "users" are other computer-based devises (e.g. PLCs and field devices), not humans. This distinction, and the fact that most extant control systems are outfitted with older microprocessors with little compute power, lies at the heart of the issue of securing control systems in a manner appropriate to current need.

Unfortunately, today very few people possess thorough understanding of control system cyber security. This understanding requires prior detailed knowledge of the control system application, how it is designed and operated, as well as how it communicates and is interconnected with other systems and ancillary computing assets, before appreciation of cyber vulnerabilities of the system as a whole can begin. Figure 1 generally characterizes the relationship of the different types of specialty technical skills needed for control system cyber security expertise, and also reflects the relative quantities of each at work in industry today. Most people now becoming involved with control system cyber security typically come from a mainstream IT background and not that of control systems. This has, in some cases, inadvertently resulted in making control systems less reliable without providing increased security, such as the example of the uninformed use of mainstream IT port scanners on older generation PLC networks.

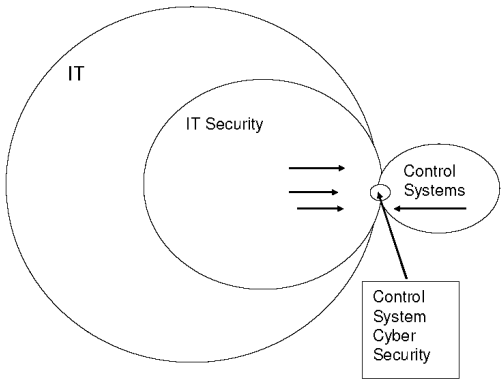

FiGure 1—Relationship and Relative Availability of Control System Cyber Security Expertise

[3] Federal Energy Regulatory Commission Docket RM06–22, http://www.ferc.gov/docs-filing/elibrary.asp

It is often mistakenly assumed that a cyber security incident is always a premeditated targeted attack. However, NIST defines a Cyber Incident [4] as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional." Unintentional compromises of CIA are significantly more prevalent and can have severe consequences. In fact, statistics collected over roughly the past 20 years in mainstream IT have consistently shown that about two-thirds of all cyber security incidents originate from within an organization, and that the cause of most of those are unintentional human error. This phenomenon must also be addressed by cyber security standards if they are to be effective.

Use of mainstream operating system environments such as Windows and UNIX for running control system applications leave them just as vulnerable as these operating systems are when used anywhere else, and application of mainstream IT security technical solutions and/or methods can be applied to help secure our more modern control system host computers and operator consoles (i.e., PCs). At the same time, however, application of mainstream IT security technologies and methods can also adversely affect the operation of control systems, such as causing components on networks of older generation PLCs to freeze-up upon use of port scanning tools, as noted. Furthermore, DOE's Idaho National Laboratory (INL) has conducted demonstrations of how a hacker can manipulate widely used "middleware" software running on very current mainstream computer systems without a great deal of difficulty, e.g., using vulnerabilities in OPC code ("OLE for Process Control"). In this sobering demonstration the system appears to be functioning properly even though it is not; while displaying incorrect information to, or withholding correct information from, system operator consoles.

Inadequacy of NERC CIP Standards as Effective Regulation

Prior to NERC becoming the Electric Reliability Organization (ERO), NERC was an industry sponsored, industry-led, and industry-funded organization, and they still are today. Contrary to popular belief, NERC as ERO is still funded by the industry, thereby creating potential for conflict of interest. It was a secret to no one involved that the objective in drafting the Critical Infrastructure Protection (CIP) Standards was for the industry, through NERC, to put something in place to its liking before the Federal Government did so in its behalf. Thus, the CIP Standards were developed by a trade association.

Because NERC employs an American National Standards Institute (ANSI)-approved standards development process, it is required to follow certain rules including balloting of its standards to obtain approval from constituent industry member organizations. Consequently, as the CIP Standards went through the balloting process, they became less inclusive, more ambiguous, and created more exemptions to applicability. It should also be noted that prior to industry acceptance of the final version, the CIP Standards went though three rounds of drafting and subsequent industry comment of approximately 1000 pages each (with some redundancy), and the NERC Drafting Team could accept or reject recommendations unilaterally as they deemed appropriate, with but modest explanation as to rationale. NERC and many utility representatives recognized the limitations of this effort, but felt anything more rigorous in terms of requirements would not be acceptable to enough utility organizations to pass ballot.

As the NERC CIP Standards moved to their final revision, the focus was shifted entirely to bulk power grid reliability in and of itself, rather than on societal welfare and safety from a homeland security or economic perspective. The reliable operation of a small substation that supports a major oil or gas pipeline in a remote locale is not salient to grid stability, but failure of same could very well have profound adverse consequences for the health of the US economy. Likewise, under the CIP Standards, the importance of continuity of electric power to municipal water works, manufacturing plants, refineries, hospitals, and military installations, etc., is not a factor requiring consideration in determining the importance (or "Criticality") of the electric system assets which serve them.

Perhaps the biggest issue with the CIP Standards as a set is CIP–002, which establishes the scope of applicability for all of the other CIP Standards: identification of "Critical Assets." These are individual pieces of electric system equipment such as electric generating units, substation transformers and digital protective relays,

[4] National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS–200-final-march.pdf

and though not explicitly stated, presumably though not explicitly the control system hosts, related servers, and operator consoles as well. Per CIP–002, deciding exactly which electric system assets are critical to reliable operation of the bulk electric system is left up to each individual organization to determine for itself, using a "risk based assessment methodology" of its own choosing or design. It is only the network-computing control systems components used to operate these specific Critical Assets—thereby deemed "Critical Cyber Assets"—that must be protected under the CIP Standards. For all other non-Critical electric and control system assets, the CIP Standards simply do not apply and may be ignored. As CIP–002 is currently written, allowing an organization to choose its own methodology permits the documented results from the flip of the coin as a perfectly valid and compliant approach to self-determination of Critical Assets. FERC has expressed consternation with this "flexibility" in its Notice of Public Rulemaking (NOPR) comments, and in its Final Rule will in all likelihood remand this Standard back to the NERC Standards process for re-conception. Unfortunately, the NERC standards development process takes a great deal of time, and our enemies are not constrained to only take advantage of our vulnerabilities after our schedule for securing them has run its course. The industry has been in the process of developing cyber security standards for over four years, and yet the matter remains unconcluded.

As noted, the CIP Standards apply only to those electric system components self-identified by asset owners themselves to be critical to their ability to maintain reliability for that part of the bulk electric grid falling under the aegis of each. The process does not embrace intra-region, inter-region, or a national viewpoint of the grid as a system, but rather only parochial considerations, each in isolation to the others. Additionally, there is no requirement to take into consideration the potential for multiple contingency threat scenarios that can involve more than one sphere of interest, such as interdependency of critical natural gas pumping stations and the greater electric power system. What's more, because utilities are interconnected, they often share equipment where the utilities conjoin (e.g., "dual ported Remote Terminal Units-RTUs"), to say nothing about network-to-network data router interconnections. Accordingly, because utilities will apply the CIP Standards in a non-uniform fashion, one utility's less rigorous application of the CIP requirements will make it a "weak link" relative to its neighbor utility, to the detriment of the cyber security of both organizations and any others to which there are further data network interconnections. Also note that all major electric sector control systems in North America communicate over the common "NERCnet", further exacerbating the situation. Worse yet, these days most control networks are also interconnected with their corporate IT networks, which themselves are connected to the Internet. A chain is only as strong as its weakest link.

Technically, the CIP Standards were conceived primarily from the frame of reference of protecting control center host systems and operator consoles, rather than field and plant floor controls equipment ("Other Facilities") at work in substations, switchyards, and power plants. The data systems in use within control centers generally utilize current computing and networking technology, requiring protective measures akin to those used in mainstream business and Internet computing. Conversely, most field PCS (e.g., substation equipment) and power plant DCS controller equipment still in use today employ technology that generally is obsolete and has little in the way of built-in cyber defenses, with little potential for upgrade or augmentation. But since the CIP Standards are intended to apply for both data center and intelligent field assets, they had to be written in a way that would be relevant for advanced current and future computing technologies, while at the same time accommodating what is essentially 'ancient' field and plant controls equipment. The result is milquetoast one-size fits all standards that are not rigorous enough for current and future cyber security challenges on the one hand, and by and large are overkill for the older field and plant cyber assets still in use. What's more, major gaps in CIP Standards' effectiveness are created by a number of explicit exclusions from applicability—in essence, loopholes.

Ironically, some of the most important contributors to grid reliability, nuclear power plants, are excluded from the scope of consideration as to criticality. While the Nuclear Regulatory Commission (NRC) has robust physical security standards for nuclear plants, the interconnection of nuclear power plant cyber control assets with those used to manage the bulk electric grid currently is not addressed in either NERC or NRC Standards. Also, while physical security requirements are specified by NRC for nuclear power plants, a little appreciated subtlety is that the CIP Standards specify physical security requirements for Critical Cyber Assets only. There is no existing NERC standard governing physical security of the Critical Assets themselves, or any other grid assets for that matter.

Since electric distribution systems have been excluded from CIP Standards' scope, so too are the controls used to operate them. This is true even though distribution assets are in operation within many transmission substations. Regardless of this, while many distribution systems employ no control system at all, the ones that do are electronically interconnected with transmission control systems, thereby creating a direct pathway into the networked-controls infrastructure of the greater bulk electric grid. Independent System Operator (ISO) and Regional Transmission Operator (RTO) energy management systems (EMS) are intrinsically data networks, interconnected one with another via NERCnet. Also via NERCnet, each is also interconnected with "downstream" control systems operated by more localized distribution operators, including cooperatives and municipal utilities. With control systems of all ownership becoming increasingly interconnected to one another, while also being interconnected with general-purpose corporate data networks and the Internet, control system exposure to cyber threats is greatly increased. Accordingly, the frame of reference concerning standards for control system cyber security supporting grid reliability purposes must be expanded to account for at least those operational control systems that need to be directly interconnected. This means expanding the scope of the standards to include smaller control area systems which routinely exchange data—and potentially viruses, worms, or other possibly compromised data—with ISO/RTO systems directly. Smaller control area systems can be attractive points of entry and through-navigation paths employed in common hacker "island hopping" technique. By analogy, at least some of the 9/11 terrorists entered the air transit system through feeder airports on that fateful day.

Another exception to applicability of the CIP Standards are control systems' data communication infrastructure per se. Currently, the electric industry has a huge investment in serial communications that will not be replaced and/or upgraded to routable communications such as Internet Protocol (IP) for many years. These serial communication systems have been demonstrated by the National Laboratories to be cyber vulnerable, e.g., through induction coil passive wiretapping or war dialing, and there have been instances where serial communications have been compromised. However, legacy protocol serial communications are excluded from the CIP Standards' scope simply because they employ non-routable protocols.

A further dubious exclusion from the scope of CIP Standards' applicability involves the Open Access Same-Time Information System (OASIS). These distributed market trading systems are excluded from CIP scope, even though they are routinely connected to energy management systems (EMS) and/or SCADA reliability systems on one side, and the Internet on the other. There is no existing regulation currently governing the cyber security of market systems, which many large systems operators will tell, at least privately, are paramount to their ability to dispatch their reliability responsibilities. In fact, aside from OASIS systems becoming entirely unavailable, an operations manager for a large transmission organization recently offered in confidence that "the thing that scares [him] most in terms of maintaining reliability is spoofed [OASIS] schedules and tags" through cyber means.

Finally, while some electric industry organizations are using ambiguities within the CIP Standards to minimize the number of Critical Cyber Assets to which the Standards must be applied, without realizing it they may be greatly increasing their liability in other ways. At the ISA Expo2007 in Houston,[5] a panel session was held on October 2, 2007, covering NERC CIP implementation. The NERC representative in attendance explicitly stated that a utility would be CIP-compliant merely by establishing cyber security policies of some kind, even if they are poorly conceived or effectively inadequate to need. During the CIP Standards drafting process a less vocal but substantial number of electric industry representatives complained about the absence of "adequacy metrics" pertaining to the Standards' requirements in general across the board, which was not remedied prior to their balloted approval by the industry. This demonstrates how conception of the CIP Standards has missed the mark of thoughtfully effecting genuine cyber security, but rather has resulted in the framing of a compliance exercise in essence amounting to adherence to a checklist. This at once elevates the need for technically competent auditors who can review the checklists and ask the right questions, while at the same time there are very few auditors who have requisite experience in the context of control systems. What's more, during a panel session at the ISA Expo2005 in Chicago, one utility industry representative presented the following slide: "In the Electric Sector, the Business Case for CIP & Reliability initiatives in today's landscape must be based on the surety that your company will be financially impacted if it is found to be non-

[5] Panel Session on NERC Compliance, ISAExpo2007, Houston, TX, October 2, 2007.

compliant."[6] That is, if the amount of the fine would be less than the cost to become secure, the utility would pay the fine.

Case Histories Which Reveal NERC CIP Standards' Inadequacies

Contacts throughout industry have shared with me the details and adverse affects of more than 90 confirmed control system cyber security incidents to date. This information has been shared with me by individuals from the affected organizations, and from government sources such as the Nuclear Regulatory Commission (NRC), the DOE National Laboratories, the National Transportation Safety Board (NTSB), and the National Institute of Standards and Technology (NIST). Note use of the term "incident", not "attack", as most of these events have been unintentional. The incidents are international in scope (North America, Europe, and Asia) and span several industrial infrastructures including electric power, water, oil/gas, chemical, and manufacturing. With respect to the electric power industry, cyber incidents have occurred in transmission, distribution, and generation including fossil, hydro, and nuclear power plants. Impacts, whether intentional or unintentional, range from trivial to significant environmental discharges, serious equipment damage, and even death. Figure 2 shows the result of a Bellingham, WA, pipe rupture,[7] which an investigation concluded was not caused by an intentional act. Figure 3 is a picture from the Idaho National Laboratory (INL) demonstration of the ability to intentionally destroy an electric generator by simulating a cyber attack.[8]

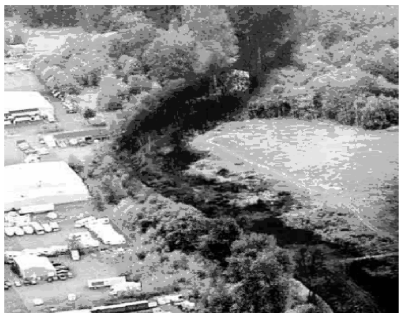

Figure 2 Bellingham, WA Gasoline Pipeline Rupture

Figure 3 INL Cyber Demonstration

The deficiencies in the NERC CIP can be demonstrated by the exercise of applying them to historical cyber events. In each historical case discussed below, adherence to CIP Standards' requirements would have failed to address the underlying causes. I have chosen events that are all publicly documented by government (US and Australian) reports. I have also included references to the Final Report of the 2003 Northeast Blackout.[9] The reason for including this reference example is because there were several cyber issues associated with the Northeast Blackout including co-temporal release of the Blaster worm and the First Energy SCADA system alarm problem. These issues resulted in 13 (of the 46) recommendations contained in the Northeast Blackout Report being cyber-related. The Northeast Outage Final Report was issued approximately two years before the NERC CIP Standards were approved. Not including the Blackout Report's recommendations is inexcusable.

Case (1) June 20, 2003 "SQL Slammer Worm Lessons Learned. . .".[10]

The control network at issued employed a frame relay data network service that interfaces with both the utility's host control system on one side of the network, and field components on the other. This network service, vended by a large telecommunications carrier, supported many diverse business organizations simultaneously. As is common, this network service utilized a high speed Asynchronous Transfer Mode (ATM) core network backbone at the center of the frame relay network. With the

[6] Thomas Flowers, "The Business Case for Being Auditably Compliant", ISAExpo2005, Chicago, IL, October 25, 2005.

[7] "Pipeline Accident Report Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999", National Transmission Safety Board Report NTSB/PAR–02/02 PB2002–916502.

[8] http://news.yahoo.com/s/ap/20070927/ap_on_go_ca_st_pe/hacking_the_grid_13

[9] Final Report of the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, https://reports.energy.gov/BlackoutFinal-Web.pdf

[10] SQL Slammer Worm Lessons Learned for Consideration by the Electric Sector, June 20, 2003, nerc.com.

release and rapid spread of the Slammer worm across businesses of all kinds serviced by the frame network, the core ATM infrastructure became choked by the worm's multiplying replication and propagation. This resulted in blockage of SCADA traffic between the utility controls host and remote controls equipment in field substations. Note that NERCnet is a shared frame relay network.

Issues: The telecom network was in essence shut down by Slammer worm traffic. The Final Report on the Northeast Blackout recommends the development of a capability to detect wireless and remote wire line intrusion and surveillance, and this report was issued prior to the adoption of the NERC CIP Standards. NERC should have heeded this recommendation, but inexplicably, the CIP Standards exclude availability requirements for telecom networking, which is intrinsic to control system operations. As will be discussed later, the NIST SP800–53 standard does not allow a scope exclusion concerning telecommunications network availability—the CIP Standards do.

Case (2) Tempe, Arizona Area Outage of June 29, 2007. [11]

The outage lasted 46 minutes and affected 98,700 customers, representing 399 Megawatts (MW) of load. It was caused by the unexplained activation of the distribution load shedding program in the energy management system (EMS) at the Salt River Project (SRP), the utility affected. A total of 141 distribution circuit breakers were opened by the EMS unexpectedly.

Issues: Most of the automation used in electric transmission and distribution systems is used to manage the distribution function. Distribution systems can be directly connected to transmission systems, and distribution system failures can be precursors to cascading outages resulting from runaway load shedding. However, the NERC CIP excludes distribution automation from scope, because they are not deemed to be part of the bulk electric system per se (i.e., the grid). NIST SP800–53 does not allow exclusion from scope of distribution automation assets.

Case (3) Australian Wireless Network Hack [12]

A disgruntled former consultant to an Australian firm that used radio-controlled SCADA sewage processing equipment packed his car with stolen radio equipment and attached it to a computer. He drove around the area on at least 46 occasions from February 28 to April 23, 2000, issuing radio commands to open discharge valves, resulting in sewage spills. This attack became the first widely known example of someone maliciously breaking into a control system.

Issues: Aware of this event, the task force that issued The Final Report of the Northeast Blackout recommended the development of capabilities to detect wireless and remote wire line intrusion and surveillance. The Blackout Report and the Australian sewage attack report were issued prior to the issuance of the NERC CIPs. Inexplicably, the NERC CIP Standards exclude non-routable protocols and do not explicitly address wireless communications. NIST SP800–53 does not have these scope exclusions concerning non-routable protocols, and addresses wireless communications explicitly.

Case (4) Nuclear Power Plant Cyber Incident [13]

On August 19, 2006, operators at Browns Ferry nuclear generating facility, had to manually scram (shut down) Unit 3 following a loss of both primary and secondary reactor water recirculation pumps. Plant procedures specified that the manual scram was required following the loss of recirculation flow. The NRC issued an Information Notice (IN) to alert licensees about recent operating experience related to the effects of potential interactions and unanticipated failures of Ethernet connected non-safety equipment on the safety and performance systems in use at nuclear power stations.

Issues: Nuclear plants represent approximately 20% of US electric power generation. Widespread shutdown of nuclear facilities would have significant adverse impact on the reliability of the bulk electric grid. The NRC is responsible for the safety of nuclear plants, that is, safe shutdown. NRC does not however "regulate" the continued operation of nuclear plants in relation to grid reliability, as witnessed in the NRC Information Notice. The NERC CIP Standards exclude nuclear power facilities from scope, while NIST SP800–53 does not allow such exclusions for nuclear plants.

---

[11] "Computer Problem Causes Brief Outage to as Many as 100,000 SRP Customers in Arizona", *Energy Assurance Daily,* Friday June 29, 2007, *http://www.oe.netl.doe.gov/docs/eads/ead062907.pdf*

[12] Supreme Court of Queensland r v Boden, Vitek 2002, CA Number 324 of 2001 DC Number 340 of 2001, *http://www.courts.qld.gov.au/qjudgment/QCA%202002/QCA02–164.pdf.*

[13] NRC Information Notice: 2007–15: Effects of Ethernet-Based, Non Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations, April 17, 2007.

Early Repercussions from Establishment of the CIP Standards

As noted above, each organization in the electric industry with responsibility for maintaining the reliability of the bulk electric system is free to adopt a risk based assessment methodology of its own choosing or design to determine which cyber controls apparatus must be protected. Discussion across the industry has born witness to an interesting phenomenon which has yet to be formally documented anywhere. It so happens that many of the largest electric utilities have determined in their risk assessments that they have no—zero—critical generation assets. In fact, within one of the largest regions in the US, the southeast, virtually none of the large operators have identified any of their generation assets—nuclear included—as being critical to reliability of the bulk electric system. The reason for this is offered forthrightly, that their systems have been designed to withstand "N–1 contingencies," meaning that they can withstand the loss of any single unit without adverse impact on reliability. What is not being considered is the potential for simultaneous multiple contingencies. With the greater controls infrastructure being as cyber-interconnected as observed earlier, it is by no means beyond the realm of possibility of just such an occurrence taking place. Without digression into potential permutations, while Slammer and Blaster worms were propagated via email, and email is generally not used in operational control systems, an analogous threat vector could be sculpted for widespread attack on the greater assemblage of control systems used to operate the grid. What if a Trojan Horse planted in numerous generation control systems should awaken at the appointed hour and simultaneously trip a whole collection of plants in a region offline at once? The effect would look very much like the Northeast Blackout. Very possible scenarios such as this are being discounted out of hand by people in positions of authority who really do not understand cyber security.

Second, we are also witnessing an unfortunate and unexpected phenomenon concerning the CIP Standards that leaves us at cross purposes with other needed electric system management improvements. Many of the more recent utility controls automation upgrades have been motivated by the goal of improving electric system reliability, but at the same time to also aid reduction in operation and maintenance costs. Many of these new systems enhancements are predicated upon the use of modern digital networking technologies (e.g., employing routable protocols such as IP), and in so doing these assets explicitly fall within scope of NERC CIP Standards' compliance. Consequently, because of concerns about potentially being "caught by the CIP Standards" in a state of noncompliance thereby resulting in potentially large fines, a number of utilities have started to disconnect, or have ceased implementation of, these modern networked-systems improvements—motivated explicitly by the goal of CIP Standards compliance-requirements avoidance. This tactic results in leaving certain existing cyber vulnerabilities unaddressed through exploitation of loopholes in the CIP Standards, as now written. At the same time, new "time and distance compression" operating efficiencies that can be garnered through use of modern networked remote control and telemetry are thereby lost by this step backward. The potential for improved operational efficiency could at least temporarily contain if not indeed reduce gross operating costs, which in turn holds the line on electric rates experienced by society. So, it appears that the industry is at cross-purposes in its response to the need to both secure and modernize the existing control systems infrastructure. This ironic industry response to the CIP Standards serves neither purpose in any discernable positive way.

An Alternative to the NERC CIP Standards

The NIST "Security Risk Management Framework" (hereafter referred to as "Framework") has been developed by the Department of Commerce, and its use is mandatory for all federal agencies under the Federal Information Security Management Act (FISMA).[14] It is devoid of conflict of interest and has been broadly and publicly vetted. There is nothing 'onerous' about the NIST Framework, as it applies specifically for systems that *do not* have national security significance, and recently it has been augmented to address the unique needs of industrial control systems. In a study performed by MITRE Corporation for NIST, a line-by-line comparison of controls and countermeasures within NIST SP800–53[15] and the NERC CIP Stand-

[14] The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. §3541, *et seq.*)

[15] National Institute of Standards and Technology Special Publication 800–53, Revision 1, *Recommended Security Controls for Federal Information Systems,* December 2006.

ards[16] was undertaken. The results indicated the NERC CIP Standards were less rigorous than even the low-baseline security controls established in the NIST Framework. In the final analysis, if U.S. Fish and Wildlife must comply with the low-baseline NIST Framework, from the perspective of societal wellbeing and economic stability, in good conscience is it prudent to require less from the operators of the electric grid.

A recurrent theme in the FERC NOPR is the need for greater granularity and detailed specificity in the CIP Standards. Part of the problem is the manner in which the CIP Standards are written—broadly brushed and highly generalized; so it's easy to understand FERC's desire for more specificity. This desire is at least in part motivated by the need to conduct compliance audits. The high-level abstraction of the NERC CIP Standards requirements language can leave the auditor struggling with shades of grey in interpretation (especially those auditors that come from a mainstream IT background exclusively), to say nothing as to grey-area impact in appeals to findings of non-compliance. In contrast, NIST SP800–53 is far more granular and provides clear requirements that have much less room for misunderstanding. Furthermore, the companion NIST SP800–53A[17] provides guidelines for determining the effectiveness of cyber security controls; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security needs of the organization. Additionally, NIST has also produced a detailed guidance document for industrial control system (ICS) security, NIST SP800–82,[18] which provides instruction on securing ICSs while at the same time satisfying their unique performance, reliability, and safety requirements.

One of the major problems in control system cyber security is the culture clash between an organizations' mainstream IT department and that responsible for the operating critical infrastructure and related control systems. The NIST Framework, specifically NIST SP 800–53 extended for Industrial Control Systems (ICS), is the only document of which I am aware of that addresses both IT and control systems security in the same document. Consequently, it is my belief that this is a key tool that can help bridge the organizational divide between mainstream IT and control system operations functions; which in and of itself can help to untangle many of the existing control system cyber security issues.

Adoption of the NIST Framework for the electric sector will eliminate the requirement for redundant effort faced by a number of quasi-federal organizations such as the Tennessee Valley Authority (TVA) and the Bonneville Power Authority (BPA), who are now required to prepare different sets of documentation and endure dual audits for both FISMA and NERC CIP Standards compliance. Is this duplication a good use of ratepayer dollars?

The electric sector is arguably the most interdependent of all the critical infrastructures, and it's also the first of the private industrial sectors (health and financial excluded) to move toward establishment of cyber security standards. Without digression, it would appear wise for all of our industrial sectors to adopt a consistent set of methodologies for cyber security of distributed and process industrial control systems. The vulnerability demonstration shown by CNN (reference 5) provides a clear justification. The advisory notice about the demonstrated vulnerability was issued to the electric industry, including dams, and was also released to the chemical and water industries as they use similar systems and networks and thereby similar cyber vulnerabilities. Additionally, having consistent requirements across industries can minimize the potential for having to modify control systems to meet individual sector security requirements.

One way to move towards cross-sector convergence in cyber security ways and means is for all stakeholders to use the same terminology and to eliminate duplicative or overlapping sets of security standards' requirements. NIST offers a set of high-quality publications addressing most of the relevant managerial, administrative, operational, procedural, and technical considerations. Each of these publications, such as SP 800–53, have been put through a significant public vetting process by all sectors, including, to the extent possible, by authorities in the national secu-

---

[16] *MITRE Technical Report (MTR070050): Addressing Industrial Control Systems in NIST Special Publication 800–53;* http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-in-SP800–53__final__21Mar07.pdf

[17] National Institute of Standards and Technology Special Publication 800–53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Third Public Draft), June 2007.

[18] National Institute of Standards and Technology Special Publication 800–82 (2nd draft), Guide to Industrial Control Systems (ICS) Security, *http://csrc.nist.gov/publications/drafts/800–82/2nd-Draft-SP800–82-clean.pdf*

rity domain. NIST offers its documents to all organizations interested in using them as a basis for developing common Standards within the ICS community.

Summary Opinion

NERC is now FERC's Electric Reliability Organization (ERO) and as such should no longer be acting as an industry-representative organization. However, much evidence reveals NERC still exhibiting vestiges of its role as an industry advocate, at least in so far as concerns its attempts to minimize the urgency of the matter of cyber security. Rather than be attentive to and supportive of the FERC NOPR and move to assure its implementation, NERC has chosen to issue rebuttal comments.[19] What's more, the dubious act of NERC submitting a rebuttal to FERC is exacerbated by the poor technical quality of its comments. NERC has not had previous experience with control system cyber security, and I do not believe that NERC as constituted is capable of providing adequate oversight of cyber security of the grid.

For the reasons stated above, the existing NERC CIP Standards are not adequate for cyber-securing the electric grid. There are other approaches that can provide a higher level of security without incurring significant incremental cost. My principal recommendation is that the NIST Framework's requirements should be incorporated into standards for industry that are currently being developed by the ISA99 Standards Development Committee, Security for Industrial Automation and Control Systems.[20] As is NERC, ISA is an accredited member organization of the American National Standards Institute, and the ISA99 committee brings together security experts from across industry, government, and academia. DHS has already provided valuable support by allowing experts from NIST and the National Laboratories to contribute in this ISA99 initiative, and it is vital that this support continue. I recommend further that the NIST Framework requirements form the basis of compliance audits to be conducted by a new and related entity, the ISA Security Compliance Institute. Any resulting fines or other findings should be addressed by NERC. A single set of Standards for industrial automation and control systems is more cost effective than a patchwork of standards conceived independently by each industrial sector. This would provide the leading practitioners on control systems cyber security to bring their expertise to bear and provide comparable levels of protection across the interdependent critical infrastructures.

Recommendation to Congress

Congress should empower FERC with the authority and responsibility for development of control system cyber security requirements and compliance criteria similar to role of NRC in these matters. In so doing, Congress should also provide FERC with the authority to separate ERO functions so that NERC is responsible for traditional electric system reliability Standards, and have a separate organization be responsible for the cyber security aspects of critical infrastructure protection. Finally, Congress should take action so that the ERO function is funded by the government, not by industry as is now the case, to better ensure that conflicts of interest do not interfere with doing what is right and necessary, and not just what is convenient.

Mr. LANGEVIN. Mr. Weiss, I want to thank you for your testimony. You had some very salient points in there, and I agree with your testimony.

I want to again thank all the witnesses for their testimony here today. And I now recognize myself for the purpose of questions. Let's get right to it.

Mr. Whiteley, as you are aware, we are very concerned about the aurora mitigation efforts ongoing in the electric sector. In a briefing with staff on Friday, DHS described a survey that NERC sent out in August 2007 to determine how many owners and operators were implementing the mitigation efforts.

Can you describe the survey and tell us its findings?

Mr. WHITELEY. The survey was the follow-up to the guidance that was issued earlier in the spring, and we have determined that approximately, at this point, 75 percent of the transmission grid

[19] NERC Comments on the FERC NOPR dated October 5, 2007, Comments on the North American Electric Reliability Corporation on the Notice of Proposed Rulemaking for Mandatory Reliability Standards for Critical Infrastructure Protection, nerc.com

[20] ISA99, Security for Industrial Automation and Control Systems

has either taken appropriate actions or is in the process of implementing those actions. And we continue to follow up with the remaining 25 percent of the grid that either has not reported or that hasn't started to take action to find out what the status is.

So in terms of ongoing work, we continue to follow up; to eventually reach a 100 percent reporting is our goal.

Mr. LANGEVIN. Why don't you have 100 percent compliance at this point? What is the remaining 25 percent? Why are they dragging their feet?

Mr. WHITELEY. Well, I don't have—I don't have information on whether they are dragging their feet or whether we just have not received the report. We are in the process of following up with them at the present time to determine just exactly that.

Mr. LANGEVIN. On that 75 percent you say is in compliance, this is not just anecdotal. You are talking about, these are 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 have asked, and they have explained what has been done. So we have direct information.

Mr. LANGEVIN. Well, I don't have as high a degree of confidence, and I have to say I am a bit skeptical that the entire electric sector is well on its way to having mitigated the problem and implemented strategies.

Mr. McClelland, would FERC determine an investigation to consider whether the level to which electric sector owners and operators have implemented these mitigation efforts?

Mr. MCCLELLAND. Yes. Yes. We agree that in order to determine whether or not there have been sufficient mitigation measures employed, it would be very important—in fact, essential—to have information that would validate what those mitigation measures were and who has conducted those mitigation measures.

Mr. LANGEVIN. Thank you.

Mr. McClelland and Mr. Whiteley, under today's regime that is, frankly, the option of the cyber standards, if a cyber exploit of the aurora vulnerability is imminent, how will the electric sector, ISAC or the Department of Homeland Security ensure the immediate implementation of mitigation efforts?

And doesn't the fact that this is an advisory document hamper the mitigation?

Mr. WHITELEY. NERC has issued it as an advisory because it falls outside of our present authority in terms of standards that have already been approved. Had they been approved standards, then we would have additional mechanisms to follow up with the industry. And so to the extent we could, we have issued the advisory, explained it, and we are following up.

Mr. MCCLELLAND. The Commission issued an order on September 20 to clarify, that required action alerts, as issued by NERC in this circumstance, are not required because they are not based on an approved reliability standard, the standard that has been through the open and inclusive process required by EPAct and then approved—subsequently approved by the Commission. However,

the Commission encourages—we applaud NERC and encourage these types of advisories to be put into place.

We have also now directed that—following a required action alert, the Commission has directed that within 30 days of the compliance date on such an alert, the Commission will receive a report from the ERO that will detail who has complied, who has not complied with what the level of compliance is, so that the Commission can evaluate whether further action—and that would include action to call for a reliability standard—is warranted.

Mr. LANGEVIN. Thank you.

Mr. Weiss, do you care to comment on any of the questions and, in particular, if, in fact, there was a need to move quickly as a result of actionable intelligence, some knowledge that there is a vulnerability that existed, A, does the current structure lend itself to closing loopholes quickly? And what is the best strategy or the best entity to make sure that if we have a situation that arises, that we can move quickly to close gaps, close vulnerabilities?

Mr. WEISS. I would like to address one other point, and that is, aurora is obviously a very critical vulnerability. It is the not only one; there are several others out there, probably of equal significance. And one of the things that I am very concerned about is that people focus so much on aurora that they don't look at other things.

I had a phone call from a friend from the oil/gas industry when they got that ISAC advisory. Their first question to me was, what about the other vulnerabilities? So the first thing I really want to get across is, we are not trying to address one and only one issue. What we are trying to address is the cyber vulnerability of the grid, and for that matter, the interconnections to the grid.

The second point is that what I have found personally over time is that there is a tendency for private industry to be very reticent to provide information to the government. Several years ago we prepared a scoping study. We did this under a DOE contract. It was Carnegie Mellon and my previous employer. It was a scoping study for setting up a cert for control systems, and one of the most important aspects on that was that we felt that that initial entity, where the information goes in, should not be a government entity. It should be somewhere that it could be sanitized and then sent off further to actually have the work done.

But the other point I want to get across, because I think this gets missed, is what I said to begin with. All of these industries use exactly the same equipment; that same, identical programmable logic controller that is used in a power plant or a substation is used in a steel mill, in a chemical plant, in a water plant, et cetera. So if they have problems or cyber issues, we need to know that.

One of the things I see that is missing, you could call it an ISAC, call it what you will, but there should be something that is focused on the control systems because that is what we are looking at. That is what cuts across.

Mr. LANGEVIN. Thank you, Mr. Weiss.

My time has expired. The Chair now recognizes the Ranking Member for 5µminutes.

Mr. MCCAUL. I thank you, Mr. Chairman.

You know, since 9/11 we have been very focused on physical threats. But in my view, not enough attention has been paid to vir-

tual threats and cyber threats, and yet we have known about these threats out there.

I think aurora kind of highlighted it and brought it even more so to our attention, not only to the panelists, but to Members of Congress when we had that briefing. We have a responsibility in a bipartisan way to do everything we can to protect the American people.

First and foremost, when you look at 25 nations that have cyber warfare programs out there, it causes me great concern. And Mr. Weiss, you mentioned other vulnerabilities. My question was going to be—and I do want to ask a question about NIST, if I can, as well. But as I said to the prior panel, some credit deserves to be made to Idaho National Lab and DHS for actually proactively finding a vulnerability, then fixing it, then mitigating it.

Mr. WEISS. Absolutely.

Mr. MCCAUL. But there are other vulnerabilities.

To the extent you can comment on those, Mr. Weiss, can you tell us what those are? And what do we need to be doing at the Federal level in the government to address those in the most practical way?

Mr. WEISS. Again, following up on what you just said, the Idaho National Lab and, for that matter, the other national labs have been doing this type of research for several years. Aurora, because it actually showed damage to equipment, is the first one that, if you will, really made a splash. But they have shown that you could damage equipment, that you can open valves, that you can open and close breakers. They have been showing that for the past 3µor 4µyears; it just hasn't gotten the attention it has needed.

Part of the issue that we have is in the control systems world, we have designed our systems for performance, and we have never assumed anybody would intentionally want to do harm. And so when I talk to people, it is the people that, if you will, own these systems that are the most knowledgeable, and if they thought about it, could cause the greatest harm. They are the people we need at the table because they could come up with, if you will, the worst cases and the things we really need to address.

Mr. MCCAUL. Of course, any country that has that capability also could use it against us.

Mr. WEISS. Sure.

Mr. MCCAUL. And has a mitigation strategy with respect to aurora helped protect us from some of these other vulnerabilities in these other areas?

Mr. WEISS. It can because part of what aurora did was look at a remote access vulnerability. That covers more than just aurora. So in that sense, it has done, incrementally, good. There are other things out there, there are other vulnerabilities that are totally independent, if you will, of the aurora vulnerability.

Mr. MCCAUL. That was sort of in my thoughts as well.

We sent a letter, a bipartisan letter, basically stating that we believe that the reliability of the Nation's bulk power system, BPS, would be better protected by a cybersecurity standard that incorporates additional security measures of the National Institute of Standards and Technology under the special publication 800–53.

Where are you three on this?

Mr. WEISS. Well, I have to be a bit careful because I was part of the process. What I can tell you is what we did.

We had a member from the NERC drafting team, myself, somebody from MITRE and several people from NIST where we went and we spent 2, 3 days going through, line by line, the comparison between the NERC CIPs and 800–53; and in addition to that, looking at 800–53 to make sure we are extended to cover control systems.

What NIST then did is, it held several meetings with Federal agencies that were bound by Federal law to use that. So they also got feedback coming in from the end-users.

I believe personally that the—like I say, I am biased—I believe, far and away, that is the best document that is out there. And it does one other thing I would like to make a point of.

One of the biggest problems we have today is a conflict between the IT organization and the control systems organizations, that is, throughout any industry or any company. The NIST document is about the only one that can address it because it is the only document that essentially was IT to start with. So IT is there, and it has now been extended to cover control systems. So we have one document that both organizations can share or have to share.

Mr. MCCAUL. And Mr. Whiteley?

Mr. WHITELEY. Well, certainly I would suggest that the CIP standards that we filed with the Commission are simply a starting point. And I think I have referenced that in my testimony. That it is a good starting point, and our intention is to make them better as time goes on.

Certainly, the evidence that NIST standards may be more applicable today to control systems than they were when these were originally drafted and that there is additional guidance from the cybersecurity community, it would be very appropriate for us to put them back through our standards process and make appropriate revisions.

And, in fact, I can tell you that in our normal cycle of revising our standards, the cybersecurity standards are already in our work plan within the next 3µyears for their first round of revisions, and they haven't even been approved yet. So we know they will get better; they have to get better over time.

Mr. MCCAUL. Mr. McClelland.

Mr. MCCLELLAND. I should begin by explaining, or at least clarifying, the Commission's authority. The Commission can approve a proposed—the Commission can't author a reliability standard; it can only approve or remand a reliability standard. Simultaneous with the approval, the Commission can call for immediate modifications to the standard.

The comments we received from Congress ask us to consider the NIST standards instead of the CIP standards the Commission had proposed in its Notice of Proposed Rulemaking. Understanding the Commission could not substitute the standards for the CIP standards, the Commission proposed to evaluate NERC on its performance by NERC's evaluation of the NIST standards.

There are entities, such as TVA, that will be under both NIST and CIP standards. The best elements of the NIST standards can and should be incorporated into the CIP standards. If the ERO

doesn't initiate that motion on its own, the Commission can and will initiate that motion.

I should also say that the CIP standards in their current state, the Commission is concerned. There are exclusions for reasonable business judgment. There are also exclusions for technical feasibility. An example would be if a piece of equipment is not capable of accepting a multicharacter password, a longer password with multicharacters, one might be able to claim under the current CIP standards that it is not technically feasible and be excused from that requirement.

So the Commission has expressed these concerns and is proposing to call for immediate modifications to the CIP standards. So on that basis, the CIP standards in their current form, the Commission feels needs improvement.

Mr. MCCAUL. Okay. Thank you very much.

Thank you, Mr. Chairman.

Mr. LANGEVIN. I thank the gentleman. And just as a follow up to Mr. McCaul's questions, a comment with respect to the vulnerability discovered in control systems, the aurora issue in particular.

I just wanted to mention how important Mike Assanty and Barry Coonley, Idaho National Labs, were to this effort, very critical to this effort. Talk about two guys thinking outside the box and discovered this problem. They did a—as far as I am concerned, a great service to the Nation and should be applauded for their hard work. And I received their brief back in January, as did the Department of Homeland Security, and then we got the committee briefing to this as well. And again, it did a great service to the country on this issue.

With that, the Chair now recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. Weiss, I mentioned earlier, when you were in the audience, it is nice to see you in a room instead of on a plane like we usually do. And I am glad that you were able to come out and share your thoughts, which are very helpful.

In the first panel, one of my colleagues asked how much more it would cost if the NIST standards were adopted instead of NERC. Do you have an opinion on what that cost would be, what the increment would be?

Mr. WEISS. The issue—it is a two-part answer. If the NERC CIPs were to cover as comprehensive a scope as the NIST standard, there would be no incremental cost.

The incremental cost is because, with the NERC's CIP standards, utilities can exclude——

Ms. LOFGREN. Right.

Mr. WEISS. —all kinds of equipment.

Ms. LOFGREN. Well, let's assume—I mean, the defects have been outlined by GAO and yourself in terms of scope. So let's use that as the baseline.

Mr. WEISS. Yeah. Then the answer, there should be really no difference, because what you are talking about is doing a cybersecurity assessment. And if you meet what would be a good, comprehensive cybersecurity assessment, it should be with either one. So there really shouldn't be any incremental cost.

Ms. LOFGREN. I have a question, and I guess it is for FERC because we have struggled now with this whole cybersecurity exposure issue for a considerable period of time; and I must say that despite sustained interest, I am not yet convinced that we have made the progress that we should have.

And the question is, who is going to have the responsibility to insist? And especially—you know, it is one thing for the Federal Government, that is not necessarily in a lead position technologically, to come into the tech sector and say, you have got to do this, because we probably don't know what we are talking about.

But it is quite a different thing to insist that at least industries that are not the tech industry use what is available and what is identified.

And we heard earlier today that our assistant secretary doesn't have the authority really to insist; and you are saying you don't have the ability really to insist. I have a sense of urgency about this, and I don't feel that sense of urgency from the testimony.

So the question is, you know, maybe one structure would be—and we are going to have—Mr. Garcia is going to get back to us. But when you have an assessment here such as we have now from NIST, and you know, I think they are widely acknowledged as a pretty reputable and efficient organization—you know, shouldn't we have the cybersecurity division have the ability to go to the regulator—for example, yourself in this case—and say, this has got to be done in this time frame for the national security?

Mr. MCCLELLAND. The Commission does have the ability to compel the return of a reliability standard within a predetermined period of time. It can be within days, if such urgency exists.

The difficulty when it involves national security issues, which I mentioned in the opening statement, is that the process is open and inclusive. It is participatory.

So folks are convened. They vote for a standard. They return the standard.

Ms. LOFGREN. I understand.

Mr. MCCLELLAND. The Commission then solicits comments. The Commission goes through Notice of a Proposed Rulemaking, considers the comments and then issues a final rule.

The cybersecurity provisions, however, were part of the Energy Policy Act, and they are the Commission's responsibility. With that in mind, the Commission now is actively reviewing its options in light of its authority and in light of recent developments.

Ms. LOFGREN. Well, I guess you know I just feel some sense of frustration because, as Mr. Weiss has outlined—and we don't want to go into all the details here; I mean, some of these vulnerabilities have been well known for some time. And if you take a look at the interconnection and cascading catastrophe that we are open to—and we haven't done anything about it; we haven't done anything about it in 4 or 5 years. And I just can't understand why.

And, you know, it is not something the Congress can enact because the vulnerabilities change as the technology does to some extent, although the stuff that we never fixed remains vulnerable.

You know, it has really got to be done administratively, and yet here we are just as bare as we ever were. And I just feel—you know, how do we instill a sense of urgency here?

Mr. MCCLELLAND. The aurora issue has heightened the sense of urgency. And, again, the Commission can compel a reliability standard. But it cannot compel action of users, owners and operators without a reliability—or it is not clear that the Commission can compel action of users, owners and operators without a reliability standard to base it on.

The process itself is open and inclusive. So, there again, I understand your concern, and there is a tension between an open and inclusive process.

Ms. LOFGREN. Well, I wonder if—I know my time is up, Mr. Chairman—but if you could get back to us on any suggestions that you would make for something like this. Because you know, we are all for openness, we are all for a process, and there is a role for that. But I don't particularly think that the energy sector is necessarily, you know, the leading edge on cybersecurity.

And we have a roadmap. And aurora was spectacular. I want to give credit to people who took action.

But there are things that Mr. Weiss has said, incidents and things that haven't even been reported, that if you look at the implications could be as dire or worse. They are out there, and they have not been attended to, and I don't see any plan to attend to them.

Mr. MCCLELLAND. We will be delighted to work with your staff on that information. Thank you.

Ms. LOFGREN. Thank you very much.

Mr. LANGEVIN. I thank the gentlelady.

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

Mr. GREEN. Thank you, Mr. Chairman. I thank you and the ranking member for convening this meeting.

I suppose I should say, in a sense, thank God for CNN, because CNN has made what was clear to some transpicuously clear to others. They brought great popularity to this issue. And I suppose at some point we have to ask ourselves, is there anything in that CNN report that we take issue with?

Dr. Weiss, is there anything in that report that you take issue with?

Mr. WEISS. No, there isn't. I thought it was well done.

The other thing I thought was well done is, the real details of the vulnerability were really not made public to those that we don't want to know about them.

Mr. GREEN. Yes, sir.

Does anyone take issue with any aspect of the CNN report.

Mr. WHITELEY. I certainly don't take issue with the CNN report on its face.

I just will point out that NERC has responsibly developed and filed with the Commission for approval CIP standards that will expand the cybersecurity protection of critical assets, as was exposed in the aurora videos.

Mr. GREEN. And Mr. McClelland?

Mr. MCCLELLAND. No, sir.

Mr. GREEN. Mr. McClelland, am I pronouncing that correctly, sir?

Mr. MCCLELLAND. It is McClelland.

Mr. GREEN. All right. Mr. McClelland, you indicated that it may take you a while to determine whether you need additional authority, or "new authority" I think is a term that you used. Is this correct?

Mr. MCCLELLAND. We are in the process of making those decisions now. We are evaluating our options under our authority in 215.

Mr. GREEN. Yes, sir.

Mr. MCCLELLAND. I don't know that I would say "a while," Representative, but we are evaluating.

Mr. GREEN. In Texas, we call this "fixin' to do" something. And about how long will you be fixing to do this?

The CNN report causes my constituents to have a great degree of consternation. So about how long do you think it will take before you can announce whether you need new authority? And if indeed you do, what new authority do you need?

Mr. MCCLELLAND. This is a difficult answer to provide, but I will put it forward.

As a staff member of the Commission, I cannot reveal pending Commission actions. I can say matters are under consideration. I can say they are important to the Commission. And I can say we are working diligently on them. But I cannot say that the Commission will take action within some period of time.

Mr. GREEN. Well, that is understandable.

I must tell you, I am appreciative that you did not use the words, "all deliberate speed"—for obvious reasons, hopefully.

Let me go to the next question. You said that you need more engineers.

Mr. MCCLELLAND. Yes, sir.

Mr. GREEN. You did not say how many more. So how many?

Mr. MCCLELLAND. The Commission has asked for an additional—a supplemental request in the 2008 budget for $9 million. The $9 million would be allocated towards 55 full-time employees. The majority of those employees would be engineers and bulk power system experts.

There are also auditors and some lawyers in the allocations.

Mr. GREEN. This will give you the number that you will need? Or will this give you a number that will benefit you?

Mr. MCCLELLAND. The Commission's authority changed substantially with EPAct 2005. For the first time, the Commission had direct authority over the reliability of the bulk power system.

That said, we are discovering—or we are now verifying, we are documenting needs for personnel.

Mr. GREEN. I have to ask you—let me just say this, sometimes when persons finish, I don't know whether they said "yes" or "no."

Mr. MCCLELLAND. I understand.

Mr. GREEN. May I just ask you again? And you would kindly give me a "yes" or "no"?

Will this give you the number that you need? Or will this give you a number that will be of benefit to you?

Mr. MCCLELLAND. It will be a number of benefit, subject to further review.

Mr. GREEN. Well, we will be honored to know the number that you will need, because if there is a need, I think we want to make sure that the need is met. Because this is critical.

Final question, Dr. Weiss—and may I call you Doctor?

Mr. WEISS. It is actually Mister.

Mr. GREEN. You look like a Doctor, so you are promoted today.

Dr. Weiss has indicated that ERO should be funded by the government. Is that what you said, Dr. Weiss?

Mr. WEISS. Yes. Yes.

Mr. GREEN. All right.

Let me ask you, friends, does anyone differ with Dr. Weiss on his basic premise that the ERO should be funded by the government?

Mr. WHITELEY. NERC's position is that the present funding mechanism, which is to take NERC's expenses and divide them equally amongst all users of electricity in the United States on a net-energy-for-load basis is reasonable and appropriate.

Mr. MCCLELLAND. I agree that at this time the Commission couldn't support the proposition that the ERO should be funded by the government. So I agree that the current funding mechanism is acceptable.

Mr. GREEN. If I may, Mr. Chairman—Dr. Weiss, you will have the last word from me, anyway.

Give the rationale for having the government fund it, please.

Mr. WEISS. For the simple fact that if the industry funds them, they are an industry-driven organization.

My concern, when you look at this—I mean, just the fact that NERC sent detailed rebuttal comments to the FERC NOPR, my view is that the ERO should be like in the nuclear world where you have INPO, the Institute for Nuclear Power Operations, that it should be an organization looking out for the public good, not for the industry good. So if it were funded by the government, not by industry, it would not be beholden to have to come up with recommendations that meet industry needs.

That is where I was coming from.

Mr. GREEN. Thank you, Mr. Chairman. I owe you 1 minute and 21 seconds.

Mr. LANGEVIN. I am calculating now. The Chair now recognizes the gentleman from New Jersey, Mr. Pascrell, for 5 minutes.

Mr. PASCRELL. Mr. Chairman, if there is any history here, and you know history tells tales about the Federal Energy Regulatory Commission. I know, Mr. McClelland, you are not on board too long, but my relationship with FERC has not been a good one. I had to drag 10 Congressmen from both sides of the aisle down there to stop an impending move 4 years ago, 5 years ago, which was successful, plus we all joined together in this. And FERC could not define what its responsibilities were.

If you remember at the end of the 90s and the early part of this century, FERC was trying to disassociate itself from any responsibility it had in the marketplace with energy problems. So this is not hyperbole here. I am not making this stuff up. There was quite a clash and conflict in the Congress' ability to have oversight of FERC, is something that we need to take a look at another time.

So when I hear the answers to the questions and when I read carefully your testimony, there is a lot of if's in here, and I don't

know when these things are going to be accomplished. And I agree with the gentlelady from California that I don't see or hear any sense of urgency.

This is critical, I think you would agree. You have a great background, so I hope you will bring some sensibility to what I consider an organization that has been dysfunctional for many years. And I don't want to go into the people who were put on there, because you don't want to hear that now.

Mr. Weiss, your testimony is quite interesting here. You know that NERC and FERC have been talking to each other, they have had a good relationship. We hope what will come out of that is pretty quickly some standards that we can agree on.

And I am sure, Mr. Mcclelland, that you couldn't answer the question for the gentleman from Texas, but you are going to go back to your superiors, get an answer to that question and give it to the committee if it is at all possible. I mean for you to tell us that you can't tell this committee when you are going to come forth with action. We didn't even ask you what the action was. You know, I find that to be very interesting. Boy, if that isn't political jargon down in Washington, D.C., I don't know what is. That is unacceptable to this chairman.

Mr. Weiss, I want to ask you this, as the NERC CIP standards, those infrastructure standards that we have talked about here today, you said as they moved to their final revision the focus was shifted entirely to bulk power grid reliability.

Mr. WEISS. Yes.

Mr. PASCRELL. In and of itself.

Mr. WEISS. Yes.

Mr. PASCRELL. Rather than on societal welfare. That is a powerful statement there. That is my words.

Mr. WEISS. Yes.

Mr. PASCRELL. In safety from a Homeland Security or economic perspective, the reliable operation—I think this is an example you give of a small substation that supports a major oil or gas pipeline in a remote local is not salient to grid stability, but failure of same could very well have profound adverse consequences for the health of the United States economy. Would you explain that?

Mr. WEISS. Yes.

Mr. PASCRELL. That a pretty potent statement you made.

Mr. WEISS. In fact, that was one of the two examples I could bring. But the point is for the bulk power grid the loss of a particular power plant or a particular substation will have no impact, if you will, on that local power grid. But if that particular substation or that particular power plant is providing the power to a natural gas pumping station, I know of one, for example, that provides about 60 percent of the natural gas to the entire northeastern United States. But that plant is in a sense meaningless to the local grid.

Mr. PASCRELL. Right.

Mr. WEISS. But if you lose that pumping station, you have lost all your natural gas.

Mr. PASCRELL. Right.

Mr. WEISS. So what is happening is in version 3 of the NERC CIPs, version 4 was the one that was finally accepted. In version

3 it had, I believe, either three or four criterion. One was bulk electric, the other was economy, and there was also health and safety. All of those were explicitly in version 3 of the NERC CIPs and then also removed as it went to version 4.

Mr. PASCRELL. Why?

Mr. WEISS. I can't explain that.

Mr. PASCRELL. Well, who removed this?

Gentlemen? Mr. Whiteley, who removed them and why?

Mr. WHITELEY. My understanding is that the changes that are made through the standard drafting process are made by the standard drafting team, which is comprised of the industry experts in the area that is being developed into a standard. And it was their judgment to make the revisions, whatever they were in to from version 3 to version 4, and eventually now that standard, recognizing that the authority that NERC has is limited to the bulk power system and that is a very——

Mr. PASCRELL. Your power is limited and FERC's power is limited, and we are talking about societal welfare, we are talking about the health of our community, the safety of the community, and you take all of those out before the final report. That to me makes no sense and we can't find out who took it out.

Can I ask one more question?

Thank you. Why wasn't the blackout report included in the final report, as you point out, Mr. Weiss, when we were dealing with NERC and CIP standards? Why was that taken out, Mr. Weiss?

Mr. WEISS. I don't know.

Mr. PASCRELL. That wasn't in there either. Give us some options why was it taken out? Come on, let's get to the meat and potatoes here. Why was it taken out? Who took it out? Give us some ideas of why.

Mr. WEISS. I can only tell you I was not on the drafting team. The comments that I put out, that ISA put out, were not accepted. That is all I can say.

Mr. PASCRELL. Well, we know why they weren't accepted.

Mr. Chairman, I think I have heard some interesting things this afternoon, and I think that this committee with your leadership and Michael's leadership and Mr. McCaul from Texas' leadership, I think we can get to the bottom of this. I am telling you, Mr. Chairman, nothing is going to get done if we leave it to chance. FERC is not a responsible public entity. It will not be until it is pushed by this Congress.

Thank you, Mr. Chairman.

Mr. LANGEVIN. I thank the gentleman for his questions and his comments, and I can assure you and the other members of the committee that the ranking member and I will continue, we are very close to this, and this is not the last hearing of its kind on the issue of cyber security. Whether it is Aurora or other security vulnerabilities, this is one of many where I plan to exercise intense oversight. And I thank the gentleman for his passion. As usual, it is great to have you back on the committee.

The Chair now recognizes Mr. Etheridge for 5.

Mr. ETHERIDGE. Thank you, Mr. Chairman, I am going to follow some of that same line for just a minute in a little different way.

VerDate Nov 24 2008 13:19 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00072 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-78\48973.TXT HSEC PsN: DIANE

In 1996, power was out across a wide range of western States because, as I remember, a squirrel got burned out on a transformer at a very crucial time. And then in 1998 there were two power failures. An ice storm took out power in eastern Canada and the United States. New Zealand lost power, as I remember, for a couple of months due to a transmission line failure.

2003, a blackout covered much of northeastern United States, and that was caused by failure of a transmission line, as I remember, in Cleveland. It sort of cascaded across a whole host of areas. And the interconnectivity of the nature of the grid means that a single point can have a significant impact.

So let me ask my question this way. Some of the testimony of folks here is that the possibility of a coordinated attack on multiple control systems can be a devastating event. Can we all agree with that?

Mr. MCCLELLAND. Yes.

Mr. WHITELEY. [Nonverbal response.]

Mr. WEISS. [Nonverbal response.]

Mr. ETHERIDGE. Would a massive effort be required to have a large impact.

Mr. WHITELEY. Massive effort and large impact. It would be a significant effort to attack all of those cyber assets simultaneously. Is it hypothetically possible? I presume so.

Mr. ETHERIDGE. Well, I raise that question because if a squirrel can have that kind of impact, a squirrel is not very high tech. I mean I am not trying to be funny; I am being very deadly serious about this issue.

Mr. WHITELEY. And if I can respond on the blackouts or outages that you have talked about, in each of those cases there is a single failure that leads back to other failures of the system. And that is precisely why the standards that we put forward, and many of which are now actually mandatory and enforceable, address issues like vegetation management so that the trees don't grow into the lines. And when there are single points of failure that they don't cascade——

Mr. ETHERIDGE. Okay.

Mr. WHITELEY. So we are addressing them in our existing standards.

Mr. ETHERIDGE. Okay, I understand that. Well, how likely is it that a single cyber attack on a control system could take out a regional power system that then would have a major impact?

Mr. WEISS. Let me try and answer it this way, a cyber event can be targeting multiple systems at one time. So part of what I am asking, I am not trying to be too much of an engineer, but the issue is you are talking about targeting multiple entities, and it is also a function of when you do it. If you do it during the summer when the system is at its highest stress, and systems are out, it won't take that many more systems to create a larger failure. When the system isn't stressed as much, it would take more.

Just so you know, 4 years ago I gave a presentation at the Georgia Tech Protective Relay Conference. It was kind of a precursor to Aurora. It was essentially laying out a scenario that I ran by Sandia, Idaho, and PNNL as well as several other utilities, how simply using cyber alone you could bring the grid down for a sig-

nificant time, strictly on the transmission and distribution side. Fairly simple. Can you do it? Yes.

Mr. ETHERIDGE. Well, that leads to the next question then, somewhat similar. You said you can, but I guess my question is are control systems within the distribution grid that vulnerable to attack? And if so, what effect might that attack have and how catastrophic could it potentially be? I think that is important for us to have some sense of in this committee.

Mr. WHITELEY. I will just add from NERC's standpoint distribution systems are outside of our purview. However, you are talking about very similar kinds of systems that utilities protect in a very similar kind of manner. And if they are protecting their transmission assets, they are also protecting their distribution assets.

Mr. MCCLELLAND. I would like to add to that. I didn't understand the question to be distribution assets per se, but the wires associated with a bulk power system. Again to echo Mr. Weiss's comment, it would depend on the unit, how large is the generating unit that is being attacked or what is the combination of output from those generating units, what is the peak load on the system at the time, how sophisticated is the adversary.

There is a level of sophistication in order to be able to pull off a coordinated cyber attack against critical facilities in a critical time. And then to also say, perhaps take Mr. Whitely's comment and put that forward and put a twist on it, the level of cyber protection that one exercises is critical. The harder it is to penetrate someone's assets, there are easier targets around the corner.

So if the basic level of cyber protection is elevated, if the CIP standards are in place and the requirements are passed as mandatory and enforced or with real penalties behind those, one would expect the level of compliance to rise and make it more difficult but not impossible for a sophisticated adversary to carry out an attack against the bulk power system. So the threat is real.

Mr. WEISS. Can I add one other point?

Mr. ETHERIDGE. Please.

Mr. WEISS. It is the reason why I have been talking about distribution. Distribution is normally outside the purview, but there are two issues here. One is it is generally where money is being spent to upgrade the systems. And so they are going from the old, if you will, cyber dumb to very cyber alive systems.

The second point is those distribution systems electronically talk to transmission. In the past when you dealt with reliability you generally dealt with each one individually. The point about cyber is they talk to each other. That is what is so different here, the silos don't work anymore. So that is why market systems all of a sudden become an issue. They talk to SCADA systems. It is why telecom is important. It is why small facilities are important. It is, if you will, what happened on 9/11. The hijackers that came into Boston that boarded the plane did not board it from Boston, they boarded it from a smaller airport. If you don't take care of the smaller, the bigger is going to be a vehicle.

Mr. ETHERIDGE. Thank you, Mr. Chairman. I appreciate your indulgence. I yield back.

Mr. LANGEVIN. I thank the gentleman and, in consultation with the ranking member, we are going to ask each one question before we conclude.

And with respect to the distribution system, this is a timely question, can the panel answer this, under a future regime after the NERC standards are adopted, NERC will be able to regulate companies who don't comply with approved cyber standards, but as we pointed out in the committee's comments, NERC's definitions will exclude a lot of critical assets.

The way I read the NERC definition, the assets at issue in the Aurora vulnerability would not be considered critical assets. In other words, you have major vulnerability out there, but NERC isn't going to able to regulate the mitigation efforts of the industry even after the standards are passed.

Can the panel provide feedback on my interpretation?

Mr. WHITELEY. Perhaps I can start and maybe clarify my earlier comment, that it is certainly NERC's intention to reach through to any part of any system that has to do ultimately with reliability of the bulk power system. And if that means that something that is in an individual residence somehow is connected to the system that would threaten the bulk power system, then certainly we would use all of our authorities that we have to reach through and assure reliability and protection of those assets.

So from the standpoint of distribution or not, yes, if indeed the case is there, what the situation is is the line is drawn between distribution and transmission and that is where essentially the system stops the issue that may come up from the distribution system. But if indeed there is a problem on the distribution system, it would be our intention to use whatever authority we have to reach those issues, those problems, because they affect the bulk power system and that is within our purview.

Mr. LANGEVIN. But even if you wanted to, is NERC going to have the ability to actually have some teeth in that regulation or is it some other entity that has to impose it?

Mr. WHITELEY. In our view, if it impacts the reliability of the bulk power system, then we can reach it.

Mr. LANGEVIN. Other members of the panel?

Mr. MCCLELLAND. I agree to your point about critical assets. Again this was a major point in the Commission's notice for proposed rulemaking. The Commission thought and expresses and proposes therefore to direct NERC to develop a risk-based assessment to provide guidelines to industry to help standardize or at least put commonality in the definition of critical based assets.

In addition, the Commission has proposed to direct NERC that all critical assets be submitted on a regional basis. In other words, the folks within a reliability coordinator's area or regional entities area would have to determine what the critical assets were, submit it to that entity, and then those lists would be subject to the Commission's review.

So we share your concern concerning the determination of critical assets and propose to tighten the definition of critical assets significantly.

Mr. LANGEVIN. Thanks. Mr. Weiss, any final thought?

Mr. WEISS. [Nonverbal response.]

Mr. LANGEVIN. Thank you. The Chair now yields to the ranking member.

Mr. MCCAUL. Thank you, Mr. Chairman. A two-part question to the panel as a whole, the Information Sharing Analysis Centers, or ISACs, coordination with the private sector. I think it really pivots on the ability of the private sector wanting to share the information. Do you believe that under current law there are enough protections for private industry to do so? I mean recognizing that a company is not going to want to share the fact that they are vulnerable. They have a fiduciary duty to their shareholders that could obviously impact the company. Under current law, are there enough protections in place so that they will freely share that information?

And then the second part of my question is with respect to the Department of Defense we have a cyber warfare program. It seems to me there is great expertise in the U.S. military in terms of how somebody else could penetrate us; in addition, how we would better work hopefully with the DOD to better protect our critical infrastructure. Is that currently happening? I know I am throwing out two questions at you, but if could you tackle those.

Mr. WHITELEY. Well, the answer to the first question is at least it has been our experience that we are not having, we, NERC, are not having trouble receiving information from users, owners and operators when we ask the questions of how they are complying with standards that are in place or gaining information on our assessments so that we do overall reliability, all the way through into the alerts that have been put out. So far the history has been that we have not run into a significant problem along those lines.

On the second part, I am not directly aware whether or not we have engaged DOD in any kind of liaison or not. We can certainly get back to you on that and explain what level.

Mr. MCCAUL. Mr. Weiss may have more expertise on that issue.

Mr. WEISS. Let me try and answer both of the questions you asked. The first one I would actually modify a little bit, is there an incentive for industry to share that information? And one of the things that is happening is there has been very little, and that is why there has been very little of that information shared. Like I say, my database I have got, you know, 90 cases. There are not 90 cases, these are just control systems. None of these are IT. You don't have 90 cases in the ES, ISAC or any of the other ISACs. Part of it is there needs to be the expertise with the ISACs to deal with control systems and generally they are not there.

Like I said, the other thing is the incentive, why would an entity want to provide that information, even if they had it, because the other point is that a lot of these events are not even identified or known to be cyber. It is one thing for the light to go out, it is another for someone to realize it was cyber for why it occurred. Let me start with that.

The second thing, dealing with DOD, I have had a little bit of dealings, I have given a lecture at the naval post-grad school in Monterey. It was kind of interesting because they hadn't really been focusing on protecting cyber assets, they were looking at attacking the cyber assets. There is a big difference between protection and defense. What we need here is the defense.

And the other point I want to make is our systems in the commercial world, be they electric, chemicals, you name it, are different than DOD. I came from that after having come from nuclear. If you have got cyber safety-related equipment, that is very much more expensive, very different than is used elsewhere. So part of this is how do we get DOD working with us, and we kind of have in the sense that right now there is an individual who used to be on the DOD side who is now on the regulatory side.

Mr. MCCAUL. It seems to me you are relying a lot on Sandia and Idaho National Lab. We have a cyber warfare program that knows how to attack, and it seems to me they would know best, you know, in learning where to penetrate than equally where how we can defend. This is in my view.

Mr. WEISS. The only reason, again, I don't mean to be technical about this, but the systems that are used in the commercial-industrial world are different than IT systems and they are different than DOD systems. What DOD is used to in terms of trying to mitigate what they would do we don't have. And honestly if we tried to put them in, it would probably hurt us very, very deeply in terms of how these systems can perform. So it is not as straightforward as most people would like it to be.

Mr. MCCAUL. That is insightful. Mr. McClelland?

Mr. MCCLELLAND. The current process is open and inclusive. In order to compel entities to abide by reliability standards they have to be developed in an open, inclusive process. There is a conflict with national security issues. So if there is an issue such as Aurora, there is a concern if the mitigation measures are disclosed too fully and the information is disclosed publicly would you have done more harm than good. If we received mitigation plans, we send an agency mitigation plan for specifics in order that they can audit or they can determine compliance with a standard, will that information then be subject to public disclosure? That is a real concern and it is the intention of the Federal Power Act. Section 215 has worked very well for us to establish an ERO, to approve and critique reliability standards and check some or pen some in some cases and also to certify the regional entities to assist the ERO. When it comes to national security issues, this is an important subject. It is critical and it is under review, and we will move forward on this issue.

Mr. MCCAUL. I thank you, Mr. Chairman.

Mr. LANGEVIN. I thank the gentleman. Does the gentleman from New Jersey have any final questions?

Mr. PASCRELL. Yes, sir.

I want to thank the gentlemen for their patience this afternoon. I have a question that I hope you all would respond to. I want to talk about the 2003 northeast blackout. That blackout was a massive power outage that occurred through parts of the northeast and the midwestern United States and Ontario, Canada in August of 2003, August the 14th. It was the largest blackout in North American history. It affected 10 million people, 10 million people in the Province of Ontario, about one-third of the population of Canada, 40 million people in eight States, which is about one-seventh of the total population. This is pretty big. In the end the outage-related financial losses were estimated at a staggering $6 billion.

My question to all the witnesses is this, really two questions. Have we learned all the lessons about our vulnerability from that blackout? And part B, do the proposed NERC regulations properly take into account those lessons?

Why don't we start with Mr. Weiss and go to Mr. Whiteley and to Mr. McClelland?

Mr. WEISS. The NERC or, excuse me, the northeast blackout report, 13 of the 46 recommendations in that report were cyber. At least a couple of them were explicitly excluded from the NERC CIPs.

Mr. PASCRELL. Right.

Mr. WEISS. Wire line, et cetera. I cannot tell you why. I can tell you we certainly knew about it. I can also tell you the day of the northeast outage was also contemporary with it was the Blaster worm and that there was or were other facilities not in the northeast that had cyber events that day. You won't find that in the northeast blackout report because they weren't in the northeast.

So the issue is have we learned? I don't believe so.

Mr. PASCRELL. Thank you. Mr. Whiteley?

Mr. WHITELEY. I will address both parts. First, I would respectfully disagree with Mr. Weiss' connotation that the northeast blackout report recommendations on cyber security were not included in the CIP standards. I would be happy to get back with you on our analysis of those CIP standards and the fact that they addressed every one of the blackout recommendations.

As to the other standards that we have in place, each one of the standards, if followed on that day, would have resulted in nothing more than a single line outage in northeast Ohio and not a cascading outage. So I think the evidence is clear that our reliability standards, as they have been passed, once the industry follows them and we believe the industry is following them to the greatest extent, will result in a more reliable system than we had back in 2003, and yes, we have learned a lot from the 2003 blackout and we have taken a lot of action since that time.

Mr. PASCRELL. Thank you. Mr. McClelland.

Mr. MCCLELLAND. If you mean by the question are we finished or is it impossible for another blackout like this to happen, will it not be prevented? The answer is no. The standards are based on a continuing improvement process. The Commission's responsibility is to review those standards and call for modifications or reject the standards where the standards are not adequate.

As an example, NERC submitted 107 reliable standards to the Commission for approval. If things were perfect and everything was done we would have accepted 107 standards. The Commission approved 83 of those standards and called for major or significant modifications to 56 of the 83 standards we approved.

In addition, prior to June 18th, 2007—the standards became mandatory and enforceable on June 18th, 2007. Prior to that time there was a period of self-reporting where entities would say, I am not in compliance with these standards, I have got some problems, some or most of those problems may be characterized as potentially having low impact to the bulk power system, but some would have a high impact to the bulk power system and be on a parallel with the incident that caused the 2003 blackout.

The Commission is aware that over 4,000 self-reported violations have been reported to NERC, and the Commission is expecting mitigation plans to be submitted to correct those self-reported violations. The process is not done, blackouts can still occur. There has been substantial and significant progress by the industry to try to prevent another occurrence, but much work remains to be done.

Mr. PASCRELL. Thank you. Thank you, Mr. Chairman.

Mr. LANGEVIN. I thank the gentlemen. I want to thank the panel for their testimony and the answers you provided to the questions. I thought this was very productive. I thought your answers were very insightful. It has certainly given us a lot to think about. Clearly, there is much work to be done and we look forward to continued oversight in this area and continued efforts of working with you, but you have been very helpful and I do appreciate your testimony.

Again, I thank the witnesses for the valuable testimony and the members for the questions. The members of the subcommittee may have additional questions for the witnesses, and we ask that you respond as expeditiously in writing to those questions.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 5:30 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 13:19 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00079 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-78\48973.TXT HSEC PsN: DIANE

Appendix I: Letter from David Whiteley

COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY,
AND SCIENCE AND TECHNOLOGY
Washington, DC, December 12, 2007

Hon. JAMES R. LANGEVIN:
Chairman, Committee on Homeland Security, U.S. House of Representatives, Washington, D.C. 20515

Dear MR . CHAIRMAN: In the questions for the record you submitted to NERC following the Subcommittee's October 17, hearing, you 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?" I am writing to correct any misimpression that my November 20 response may have given regarding the timing of the written survey.

My answer to your question did not make clear that the survey of owners and operators regarding the implementation of mitigation measures was sent in October 2007, not in august 2007 as indicated in your question. The response provided a narrative discussion of the results of the October survey. As you requested, a copy of the survey itself, dated October 19, 2007, was included with my response.

I recognize that the way the response was written may inadvertently appear to confirm that the survey was sent in August. Enclosed is an amended copy of the response to Question No. 1 that clarifies the timing of the written survey. I would be grateful if this material could be substituted for my November 20 response to No. 1 in the written hearing record.

I apologize for any inconvenience this may have caused.

Sincerely.

DAVID A. WHITELEY,
Executive Vice President

APPENDIX II: Additional Questions and Responses

QUESTIONS FROM THE HONORABLE JAMES R. LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

RESPONSES FROM MR. GREG GARCIA

Question 1.: What percentage of electric sector owners and operators do you believe implemented the Aurora recommendations issued by NERC?

Response: The Electric Sector Information Sharing and Analysis Center (ES–ISAC) distributed the advisory to 3,000 electric utilities. As part of individual corporate risk management and critical infrastructure protection planning efforts, Electric Sector owners and operators consider known vulnerabilities and identify and implement mitigation activities to address them. It is the responsibility of owners and operators to implement the recommendations issued by the North American Electric Reliability Corporation. The Department of Homeland Security (DHS) is working with the Electric Sector, the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) to raise awareness and promote implementation of the recommendations. DHS is also working with DOE and FERC to determine what actions the private sector has implemented.

Question 2.: If a cyber exploit of the Aurora vulnerability is imminent, how will the Electric Sector ISAC or the Department of Homeland Security ensure the immediate implementation of mitigation efforts?

Response: Under the National Infrastructure Protection Plan (NIPP) Partnership Framework, public—and private-sector security partners collaborate on national critical infrastructure protection. The Department of Homeland Security (DHS) currently has several mechanisms in place to communicate with vendors, owners, and operators to facilitate information sharing about exploits and vulnerabilities, as well as incident management and appropriate mitigation efforts. For example, the United States Computer Emergency Readiness Team National Cyber Alert System facilitates information sharing about vulnerabilities to a broad audience; the Control Systems Cyber Security Vendors' Forum meets monthly to discuss emerging issues affecting control systems security; and DHS works directly with the control systems stakeholder community to exchange information by leveraging the Protected Critical Infrastructure Information program, which safeguards sensitive information shared by industry with the government.

In the case of the Aurora vulnerability, DHS worked with the private sector through the NIPP Framework to alert the control systems community. Federal agency partners worked with industry technical experts to assess the vulnerability and to develop sector-specific mitigation plans. The jointly developed mitigation guidance allowed owners and operators within the affected sectors to take deliberate and decisive actions to reduce significantly the risk associated with this vulnerability.

Question 3.: How many program managers have been in charge of the Control Systems Security Program in the last 3 years? What was the FY 2007 budget? Who is in charge of this program, and what grade is that person?

Response: Four individuals have served as the National Cyber Security Division (NCSD) Control Systems Security Program Director since May 2004. The Program Director position, within Cybersecurity and Communications at NPPD, is currently vacant and posted at the GS–15 level. In the interim, Cheri McGuire, GS–15, is serving as the Acting Control Systems Security Program Director.

The FY07 budget for the NCSD Control Systems Security Program was $9.3 million.

How has your office developed a process to formalize and improve information sharing regarding control system vulnerabilities with critical infrastructure owners and operators?

Response: The Department of Homeland Security (DHS) coordinates efforts among Federal, State, and local governments, as well as control systems owners, operators, and vendors, to improve control systems security within and across all critical infrastructure sectors by reducing cyber security vulnerabilities. DHS has developed a process to formalize the sharing of sensitive information related to control systems vulnerabilities. This process describes the information flow from vulnerability discovery to validation, public and private coordination, and outreach and awareness, and also identifies the deliverables and outcomes expected at each step in the process.

The process includes existing entities across the public and private sectors, such as the Federal Control Systems Security Working Group, the Process Control Systems Forum, Sector Specific Agencies, Government Coordinating Councils and Sector Coordinating Councils, the United States Computer Emergency Readiness Team (US–CERT), and Information Sharing and Analysis Centers. It also builds on established DHS practices and procedures for the identification, validation, coordination, and communication of vulnerabilities across the critical infrastructure and key resources (CI–KR) spectrum.

As part of this process, DHS uses three primary mechanisms to communicate vulnerability information about control systems to various stakeholders:

1. US–CERT shares information about vulnerabilities via several products. These products include Vulnerability Notes, which are released on a regular basis, and the Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems, which includes more detailed analyses of cyber vulnerabilities that may impact control systems.
2. DHS partners with vendors, owners, and operators to perform vulnerability assessments of selected systems to identify cyber vulnerabilities based on emerging exploits and works with industry to develop mitigation strategies. DHS also works with control systems vendors, owners, and operators as they share sensitive information through the Protected Critical Infrastructure Information program so that private-sector vulnerability data may be appropriately safeguarded.
3. DHS facilitates information sharing among control systems vendors through its sponsorship of the Control Systems Cyber Security Vendors' Forum established in 2006. The Forum holds monthly meetings at which control systems vendors share information and discuss emerging issues affecting control systems security. The Forum has served as a basis for building a trusted information sharing community and comprises more than 90 percent of the vendors who manufacture and provide support services to the CI–KR control systems market in the U.S.

Are all government-owned assets compliant with NIST 800–53 as applied to control systems?

Response: Under the Federal Information Security Management Act, all Federal agencies must meet minimum security requirements for information and information systems in accordance with National Institute of Standards and Technology (NIST) Special Publication 800–53, *Recommended Security Controls for Federal Information Systems,* as amended. NIST 800–53 is currently undergoing revisions to include security guidelines specific to control systems. Federal agencies have up to one year from the date of final publication to fully comply. DHS is working closely with NIST on these revisions.

Question 4.: According to the GAO, DHS has 13 different initiatives focused on securing control systems. The Department of Energy, the Federal Energy Regulatory Commission (FERC), and the National Institute of Standards and Technology (NIST) also have initiatives in this field. In 2004, the GAO recommended DHS create an overall strategy to coordinate various control systems activities across federal agencies and the private sector. **Please provide a copy of this strategy.**

Response: To reduce cyber risks to control systems within and across all critical infrastructure sectors, the Department of Homeland Security (DHS) coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors. Coordinating efforts to secure control systems is paramount to an effective protective posture for all critical infrastructure and key resources.

DHS is working with its partners to baseline activities to serve as the foundation for developing a comprehensive strategy that will encompass the public and private

sectors, set a vision to secure control systems, describe roles and responsibilities, and identify future requirements for resources and actions.

The Department has developed a timeline to complete this action building on work that has already been completed. In the first quarter of Fiscal Year 2008, a draft of the Federal sector portion of the strategy will be released for review by government stakeholders. In cooperation with the Partnership for Critical Infrastructure Security, the private industry component will be integrated into the strategy, with a draft available for review in the third quarter of FY 2008. After the review and comment period is completed, a final comprehensive strategy will be released in the first quarter of FY 2009.

Question 5.: How is the Science and Technology control systems program—Project LOGIIC—being used to help mitigate vulnerabilities in the control systems of the oil and gas sector?

Response: LOGIIC is a collaborative forum for government and industry to focus on cyber security issues for the oil and gas industry. Infrastructure owner and operator needs determine projects, which are supported by both government and independent experts. Projects examine needs and solutions for correlating and analyzing abnormal events to provide indications and warnings of cyber security threats. LOGIIC enables informed response to threats by taking corrective action. LOGIIC's goal is to achieve the ability to correlate abnormal events from the process control network and its interfaces to the business network with alerts from sources on the business network (intrusion detection systems, firewalls, etc.).

LOGIIC is helping to mitigate vulnerabilities by identifying and adapting new types of security sensors for process control networks, adapting a best-of-breed correlation engine to this environment, and integrating and demonstrating the technology suite in a test bed environment.

Question 6.: Did the Multi-State Information Sharing and Analysis Center (MS–ISAC) receive any more un-obligated funds for FY 2008?

Response: Yes, the Multi-State Information Sharing and Analysis Center (MS–ISAC) received funding using the available Fiscal Year 2007 carryover funds in the amount of approximately $1.4 million.

The MS–ISAC procurement was not awarded by the end of FY 2007 (September 30, 2007). DHS initiated a replacement procurement action that used both the committed $974,849.72 of FY 2007 funds and an additional $465,976.03 of FY 2007 carryover funds that had not been obligated by the close of FY 2007. FY 2007 carryover funds for cyber security are available for obligation until September 30, 2008, as stipulated in the DHS Appropriations Act of 2007 (H.R. 5441).

QUESTIONS FROM THE HONORABLE MICHAEL MCCAUL, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

Question 7.: I understand there is a hardware device that can be used in conjunction with other proposed mitigations that is currently being developed by engineers out at Idaho National Labs. I have been told that currently only one vendor is marketing a hardware fix despite there being multiple vendors that sell this sort of equipment. **What in your opinion is preventing other vendors from moving forward with this mitigation device? Similarly has the department engaged in any discussion of the use of its authorities granted under the Defense Production Act to ensure that those government customers that need these devices are accommodated?**

Response: Battelle Energy Alliance (BEA), the contractor responsible for operating the Department of Energy (DOE) Idaho National Laboratory (INL) and owner of INL intellectual property, has filed an application with the US Patent and Trademark Office for a method to mitigate the Aurora vulnerability. Multiple vendors have expressed interest in licensing the technology from INL. The technology transfer process conforms to standards for all DOE National Laboratories.

Regarding the Defense Production Act (DPA), the Department of Homeland Security has assessed the use of the DPA as a potential avenue for ensuring that certain technologies are developed and produced to meet national defense needs, including critical infrastructure protection needs; however, at this time the technology necessary to mitigate the threat related to control systems security is available to customers. A shortage in supply would drive further exploration of the use of the DPA.

Installing a hardware device with technology licensed from the BEA-pending patent can provide critical infrastructure and key resource asset owners and operators with endpoint security. The sector-specific mitigation plans, however, are based on

industry best practices and contribute to comprehensive risk reduction from cyber security vulnerabilities to control systems.

Question 8.: In Mr. Roxey's testimony he mentioned the need for technical experts to be engaged from the very start. Since the engineers at Idaho National Labs discovered this vulnerability have they been involved in developing the mitigations and briefing the private sector?

Response: Yes. Technical experts, including experts from the National Laboratories, supported efforts undertaken by the Sector Coordinating Councils, Information Sharing and Analysis Centers, and the Sector Specific Agencies to develop mitigation plans and provided briefings to critical infrastructure and key resource owners and operators on the control systems vulnerability. The Department of Energy National Laboratories, including the Idaho National Laboratory, provide subject-matter expertise to the Department of Homeland Security to improve control systems security.

Question 9.: What is the action plan to minimize overlapping efforts at DHS?

Response: The Department of Homeland Security coordinates efforts among a variety of stakeholders from both the public and private sectors to secure control systems. To prioritize activities and minimize overlapping of efforts, the Department is working with its partners to baseline activities to serve as the foundation for developing a comprehensive strategy that will encompass the public and private sectors, set a vision to secure control systems, describe roles and responsibilities, and identify future requirements for resources and actions.

Question 10.: What is being done to utilize private sector companies that have significant process control and SCADA cyber security experience to assist in the area of critical infrastructure cyber security protection?

Response: Recognizing the expertise the private sector has to offer, the Department of Homeland Security (DHS) sponsors a number of groups to foster close collaboration and information sharing among the control systems stakeholder community. The Cross Sector Cyber Security Working Group (CSCSWG), which was established in May 2007 by DHS and the Partnership for Critical Infrastructure Security, brings together government and private-sector cyber security experts to address systemic cyber risk collaboratively across the critical infrastructure and key resource sectors. The CSCSWG facilitates the sharing of information across the sectors about cyber security issues, such as common vulnerabilities and protective measures, as well as the policy implications of cross-sector cyber dependencies and interdependencies. Public and private sector representatives from all 17 sectors participate in the CSCSWG.

The Process Control Systems Forum (PCSF) is one of three standing groups under the CSCSWG that provide monthly updates on their work so that CSCSWG members can benefit from or engage in activities as appropriate. The PCSF was established to accelerate the design, development, and deployment of more secure control systems. It is the Department's primary vehicle for engaging with the private sector on control systems security and includes a variety of stakeholders including government, academia, owners and operators, systems integrators, and vendors. More than 200 people attended the PCSF's most recent annual meeting, at which the control systems stakeholder community gathered to discuss cyber security challenges and issues, deliver training resources, and provide technical subject matter expertise.

PCSF's Control Systems Cyber Security Vendors' Forum facilitates communication in a trusted environment between industrial automation and equipment suppliers and control system service providers. The Forum consists of 50 members from 27 domestic and international companies comprising 90 percent of the market share providing service to all 17 critical infrastructure sectors. Recent collaboration occurred earlier this year when members of the Vendors' Forum worked together to address the potential effects on control systems caused by the date change in the Daylight Saving Time (DST) standard. The change in DST impacted control systems in more than 19 countries. The control systems community recognized the importance of this issue and worked with the U.S. Computer Emergency Readiness Team (US–CERT) to develop a Technical Information Paper, "Daylight Saving Time Changes for 2007." This guidance to industry on mitigation measures was downloaded from the US–CERT website more than 500 times between April and July 2007.

DHS is also working with the Multi-State Information Sharing and Analysis Center (MS–ISAC), the SANS Institute, the Department of Energy Idaho National Laboratory, and representatives from government and industry on the SCADA Procurement Project. The Procurement Project seeks to develop common procurement lan-

guage that owners and regulators can incorporate into contracting mechanisms to ensure the control systems they are buying or maintaining have the best available security. The long-term goal is to raise the level of control systems security through the application of robust procurement requirements. The Procurement Project has received very positive feedback from users, and the document has averaged more than 450 downloads per month from the MS–ISAC website where it was posted in January 2007.

DHS will continue to work closely with public—and private-sector security partners through the CSCSWG and PCSF to coordinate our activities and develop a National Strategy to Secure Control Systems.

Question 11.: What is being done to coordinate a standard control system cyber security policy across each of the 17 Sector Specific Plans (SSP) defined by DHS?

Response: Under the National Infrastructure Protection Plan Risk Management Framework, all sectors must address the physical, cyber, and human elements of infrastructure in their preparedness and protection efforts. Securing control systems is part of the sectors' efforts to secure their cyber infrastructure. In support of the cross-sector cyber responsibility, the National Cyber Security Division is working closely with the Office of Infrastructure Protection (IP), the Sector Specific Agencies (SSAs), and other security partners to develop guidance and approaches to reduce cyber risk and integrate cyber security into the critical infrastructure and key resource (CI–KR) sectors' protection and preparedness efforts.

During the Sector-Specific Plan (SSP) development process, the Department of Homeland Security (DHS) provided cyber expertise to the sectors, including reviews of draft SSPs and participation in sector-specific cyber security meetings. Specifically, as sectors were developing their SSPs, DHS developed and provided information to SSAs on resources for cyber security practices and protective programs that are applicable across all sectors, as well as some that are more focused on individual sectors, to help identify cyber security-related protective programs. For each protective program, a brief description with the specific activities they supported within the preparedness spectrum was provided. DHS also developed information on cyber research and development (R&D) requirements and priorities to help SSAs identify cyber-related R&D priorities. DHS provided a description of Federal organizations that support cyber R&D and several references to R&D documents that outline specific cyber security initiatives. DHS also offered to work directly with any sector that requested assistance and worked with responding sectors to develop and review cyber security content for the SSPs. These resources identified control systems cyber security where appropriate.

DHS also developed a comprehensive SSP Cyber Guidance Checklist, which provided sectors with a framework for integrating cyber security throughout each section of their SSPs. The checklist complemented DHS' 2006 CI–KR Protection SSP Guidance developed by OIP and was intended to provide a starting point for SSAs as they integrated cyber into their SSPs. The checklist included an outline and guidance for the development of cyber content for the SSPs. DHS shared the checklist in IP-sponsored technical assistance sessions with SSAs to provide expertise and answer questions regarding the inclusion of cyber security in the SSPs. DHS personnel also met individually with those SSA representatives who expressed an interest in determining approaches for incorporating cyber security into their SSPs and sector risk management efforts.

DHS will continue to work with the SSAs as the 17 CI–KR SSPs are updated in the future and will provide additional guidance on cyber security-related goals, security partners, risk assessment approaches, protective programs, R&D priorities, and measures. These materials will continue to include control systems security and will help to ensure that sectors address control systems security in a consistent manner across the 17 CI–KR SSPs.

Question 12.: Are there any plans to increase the reach of the cyber security language in DHS 6 CFR Part 27, Section 550 for the chemical industry? If so what is anticipated and if not, why not?

Response: The Department of Homeland Security (DHS) does not intend to change any of the regulatory language contained in the Chemical Facility Anti-Terrorism Standard (6 CFR Part 27) regarding cyber security. Section 27.230(a)(8) makes cyber security a performance standard for high-risk chemical facilities. DHS is in the process of developing guidance to help high-risk chemical facilities identify and implement cyber security measures that may be appropriate given their unique circumstances and levels of risk. This guidance document, which is currently under development, will provide guidance on all of the risk-based performance standards established in 6 CFR Part 27. Some of the cyber security areas that will be ad-

dressed in the guidance document include cyber security policy, access control, personnel security, awareness and training, monitoring and incident response, disaster recovery and business continuity, system development and acquisition, configuration management, and audits.

Question 13.: What is the DHS going to do in order to drive collaboration and cooperation between the public sector and private sector?

Response: The National Infrastructure Protection Plan (NIPP) Partnership Framework supports the establishment and maintenance of Sector Coordinating Councils (SCCs) that enable private-sector owners and operators to interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal sector policy coordination and planning entities. Sectors also rely on Information Sharing and Analysis Centers (ISACs), which provide operational and tactical capabilities for information sharing and, in some cases, support for incident response activities. The ISACs, as well as other information sharing mechanisms, provide a means for the government and private sector to exchange information. In addition to the SCCs, the NIPP Partnership Framework enables sectors to establish and maintain Government Coordinating Councils (GCCs) comprising representatives across various levels of government (i.e., Federal, State, local, or tribal) so sector-specific strategies, activities, policy, and communications can be coordinated. SCCs and GCCs meet jointly to discuss sector activities, shape priorities for the future, and collaboratively develop and review critical infrastructure protection planning documentation.

The Cross Sector Cyber Security Working Group (CSCSWG) facilitates collaboration and coordination between government and private sector security partners with cyber security expertise from each of the 17 critical infrastructure and key resource (CI–KR) sectors on cross-cutting cyber issues. The CSCSWG, which held its inaugural meeting on May 30, 2007, meets monthly and includes more than 90 representatives from the SCCs and GCCs of the 17 CI–KR sectors.

The Department of Homeland Security coordinates efforts among government and private-sector members of the control systems community to improve security within and across all critical infrastructure sectors by reducing cyber security vulnerabilities. This coordination includes enhancing public-private partnerships through the Process Control Systems Forum and the Partnership for Critical Infrastructure Security, as well as using a process to formalize the sharing of sensitive information related to control systems vulnerabilities.

QUESTIONS FROM THE HONORABLE PAUL BROUN, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Question 14.: How is the Department facilitating long term mitigation efforts with vendors of control systems? What sort of contact does the Department have with the manufacturers of these devices?

Response: Assessing technologies is one of the Department's core long-term efforts and assists in identifying vulnerabilities, developing mitigation strategies, and sharing information to reduce risk to the Nation's critical infrastructure and key resources. The Department performs vulnerability assessments of selected vendor systems to identify cyber vulnerabilities based on emerging exploitations. This effort is accomplished by leveraging the infrastructure and test beds of Department of Energy National Laboratories, vendor facilities, and other existing end user facilities.

To date, the Department has completed eight control systems vulnerability assessments in cooperation with control systems vendors who provide the hardware, software, and training necessary to run the control system. Based largely on the results of these assessments, vendors have developed system patches, reconfigured system architectures, and built enhanced systems. The results of the vendor assessments have also helped inform other Federal control systems efforts, such as developing a self assessment tool for industry owners and operators to further reduce cyber risk associated with control systems. In addition, the Department has provided owners and operators with strategies for mitigating existing system security risks.

The Department sponsors the Process Control Systems Forum (PCSF), a public-private partnership which leverages the experience, capabilities, and contributions of international stakeholders from government; academia; industry users, owner/operators, and systems integrators; and the vendor community through meetings and working groups to develop and adopt common architectures, protocols, and practices. The PCSF's Control Systems Cyber Security Vendors' Forum facilitates communication in a trusted environment between industrial automation and equipment suppliers and control system service providers. The Vendors' Forum comprises 50 active members from 27 global manufacturers representing 90 percent of the control systems marketplace.

VerDate Nov 24 2008 13:19 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00088 Fmt 6601 Sfmt 6621 H:\DOCS\110-HRGS\110-78\48973.TXT HSEC PsN: DIANE

QUESTION FROM THE HONORABLE JAMES R. LANGEVIN, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY AND SCIENCE

RESPONSE FROM JOSEPH MCCLELLAND

Question 1.: It is my understanding that many security managers in the industry were interested in submitting comments to the FERC rulemaking on critical infrastructure protection, but felt that they could not do so for fear of retribution by their own management. **Is this a problem, and if so, what is FERC doing to allow for anonymous comments for future rulemakings?**

Response: In a rulemaking proceeding, the Commission's *ex parte* rules do not apply. Thus, a person wishing to remain anonymous could informally talk to Commission staff about his or her concerns without having to formally intervene and identify his or her name. Staff could pursue the concerns raised to the extent warranted. However, the Commission's Rules of Procedure require that a filing submitted to the Commission identify the name of the person making the filing. I believe that is appropriate as the public process of a rulemaking should include the willingness of formal commenters to identify their name in their comments.

QUESTIONS FROM THE HONORABLE MICHAEL T. MCCAUL, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY , AND SCIENCE

Question 2.: Why does the Notice of Proposed Rulemaking posted by NERC ignore for now the major infrastructure dependencies on the bulk power system? Should not every responsible entity be held to the same standards for securing critical assets?

Response: Section 215 of the Federal Power Act (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 need to maintain transmission system reliability. The Commission's authority under FPA section 215 does not extend to other infrastructure such as natural gas pipelines, oil pipelines, or railways, although such infrastructure can have a significant impact on the bulk power system.

Question 3.: As director of reliability do you support strengthening security and the SCADA control systems? With regard to the comments that FERC has received thus far on the CIP standards how do you see the regulations being promulgated?

Response: Yes, I do support strengthening security and control systems. Historically, control systems have been built with a focus on operations, with little or no focus on security, as many infrastructures have not been viewed as targets in the past. At the same time, these control systems are migrating towards the standard IT platforms and internet communications, making them even more vulnerable to attack by increasing the connectivity to the outside world. Pursuant to its authority and responsibilities, the Commission is in the process of analyzing public comments and evaluating the Notice of Proposed Rulemaking (NOPR) in light of those comments. The comments of the House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology are among those being considered. The NOPR proposed dozens of significant modifications to the CIP standards to make them stronger and more effective, thereby increasing security of SCADA control systems. They addressed, among other things, increased oversight of the implementation of the CIP standards, controls on the discretion exercised by responsible entities, and increased penalty levels for failure to comply with the CIP standards. I can assure you that the final rule will be based on a careful consideration of all comments submitted.

Question 4: Please describe what authority FERC currently has in the area of cyber security. Do you think the Commission should have the authority to modify a NERC standard?

Response: Pursuant to section 215(d) of the FPA, the Commission is authorized to approve a reliability standard developed by the North American Electric Reliability Corporation or NERC, the Commission-certified electric reliability organization. Section 215 of the FPA defines "reliability standard" to include "requirements for the operation of existing bulk-power system facilities, including cybersecurity protection. . ." Thus, section 215 explicitly allows for the development of reliability standards that relate to cyber security. Pursuant to section 215(d)(3) of the FPA, the Commission has authority to order compliance with a reliability standard and may impose penalties for non-compliance.

VerDate Nov 24 2008 13:19 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00089 Fmt 6601 Sfmt 6621 H:\DOCS\110-HRGS\110-78\48973.TXT HSEC PsN: DIANE

As you are aware, NERC submitted to the Commission eight proposed reliability standards, referred to as the "CIP" standards, which would require certain users, owners and operators of the nation's bulk power system to comply with specific requirements to safeguard critical cyber assets. In July 2007, the Commission issued a notice of proposed rulemaking that proposes to approve the proposed CIP standards. The NOPR also proposes to direct NERC to develop modifications to the proposed reliability standards to address specific concerns identified by the Commission. The Commission received public comment on the NOPR in October 2007 and intends to issue a final rule in a timely manner.

If the Commission, in the final rule, approves the reliability standards as proposed in the NOPR, they will become mandatory and enforceable. The Commission would then have authority to order compliance with the CIP standards and impose penalties for non-compliance with the cyber security requirements. It is important to understand that NERC has proposed an implementation plan that would require that entities begin compliance no earlier than mid-2009, with full compliance being achieved by the end of 2010. NERC represents that the long lead time is necessary to achieve compliance with many of the requirements of the proposed reliability standards; the NOPR proposed to approve NERC's implementation plan.

You also ask whether the Commission should have the authority to modify a NERC reliability standard. Section 215(d) of the FPA provides that the electric reliability organization, NERC, will develop proposed reliability standards and submit the standards to the Commission. The Commission has the options of approving or remanding a reliability standard. The Commission, however, does not have authority to develop a reliability standard on its own. Likewise, while section 215(d)(5) of the FPA authorizes the Commission to order the electric reliability organization to submit to the Commission a new or modified reliability standard to address a specific matter, the Commission does not have authority to independently authorize or modify a standard. While this is a significant limitation of the use of the section 215 process, The Commission has not yet reached the conclusion that legislation is needed at this time.

Question 5.: How will you oversee and ensure the security process goes forward? How will you work with the industry to ensure that security risks are addressed?

Response Once Commission-approved CIP standards are in place, Commission staff will participate in the audit of entities to determine the security posture of the industry. Commission staff also will work with NERC to continue to improve the CIP standards, requiring modifications to existing standards and new standards as appropriate. In addition, we will monitor and evaluate the number and types of assets that are being protected as critical assets. We will closely follow the standard development efforts that NIST and ISA are leading. In addition, the Commission proposed in the NOPR to require NERC to seek and consider comments from federal entities, such as Tennessee Valley Authority, that are subject to both the NIST standards and CIP standards to assist NERC in determining which elements of the NIST standards may be more advantageous to protect the Bulk Power System so that NERC may consider including such provisions into the CIP standards.

Question 6.: Does the Commission have enough resources to promote reliability and protection from cybersecurity threats?

Response: Based on our workload projections, the Commission is seeking to add more engineers and personnel with bulk power system experience, including cyber security and control system expertise. Thus, in June 2007, Chairman Kelliher wrote to the Chairmen and Ranking Members of the House and Senate Appropriations Committees, seeking an additional $9 million for our reliability work in fiscal year 2008. This would provide for an additional 55 Full-Time Equivalents (FTEs) to support the Commission's reliability program. These FTEs would consist primarily of electrical engineers, power system experts, auditors and lawyers. The Commission's Chairman also asked for authorization to hire electrical engineers non-competitively up to the GS–15 level, and to hire six additional executive senior level (SL) staff in support of its reliability program. As you may know, the Commission is a self-supporting agency and would recover the additional appropriations through fees and annual charges, as it does all of its costs, and will operate at no net cost to the taxpayer. I encourage you to support these requests by the Commission.

Question 7.: NERC said there has been 100% compliance with its action alert on cybersecurity. Does the Commission agree?

Response: The Commission has no information on whether there has been 100% compliance with NERC's action alert. To determine the level of compliance and the effectiveness of such compliance, the Commission intends to issue an order directing

submission of certain cyber security information from each generator owner and operator and transmission owner and operator in the United States registered by NERC. As a first step toward that end, the Commission, in an October 23, 2007 letter, informed the Office of Management and Budget (OMB) of the Commission's intended action, and requested OMB's emergency approval of the Commission's information collection request. This emergency approval, if granted, would expedite the OMB approval process, which in ordinary circumstances allows a sixty-day comment period on the proposed information collection before OMB approval. OMB has not acted on the Commission's request at this time.

NERC, following the Subcommittee's October 17, 2007 hearing, issued a survey regarding mitigation efforts, with responses due on November 2, 2007. Although 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 that NERC has received a complete set of responses to its data request. Thus, it is important for the Commission to issue an order seeking information that would supplement NERC's action and provide more detailed information on which to assess the status of mitigation efforts.

If the OMB authorizes the Commission to collect this information, the Commission intends to issue the order and direct the submission of this information to NERC. Following Commission review of the information, the Commission will determine whether further action is necessary or appropriate. For example, the Commission may consider adopting an order that requires, pursuant to section 215 of the FPA, the expedited development of a reliability standard to ensure that mitigation measures are promptly and effectively implemented. However, Commission review of this information may also indicate that no further action is necessary or appropriate.

Question 8.: How will FERC ensure the implementation of higher standards for cyber security? Will you investigate the mitigation efforts performed by owners and operators of the Aurora issue?

Response: Please see responses to questions 5 and 7.

QUESTIONS FROM THE HONORABLE PAUL BROUN, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Question 9.: Please describe what authority FERC currently has in the area of cyber security. Do you think the Commission should have the authority to modify a NERC standard? How will you oversee and ensure the security process goes forward? How will you work with the industry to ensure that security risks are addressed? Does the Commission have enough resources to promote reliability and protection from cybersecurity threats?

Response: Please see responses to questions 4, 5 and 7.

Question 10.: Can you describe the role that FERC is taking while working with the Department of Energy and the Department of Homeland Security?

Response: The Commission has been collaborating with both DHS and DOE as required by Homeland Security Presidential Directive/Hspd–7 (Critical Infrastructure Identification, Prioritization, and Protection) that established DHS as the lead in protecting the critical infrastructure of the United States and DOE as the Sector Specific Agency for electric power. In this regard, Commission staff have supported and participated in DOE and DHS security initiatives. For example, we participated in the DOE-led effort that produced the Roadmap to Secure Control Systems in the Energy Sector. We also participate in the electric sector Government Coordinating Council co-chaired by DOE and DHS personnel. We supported and participated in the efforts that developed the National Infrastructure Protection Plan and the Electric Sector Specific Plan. With DOE's cooperation, we have utilized the expertise found in the national laboratories to better understand control system cyber vulnerabilities. Commission staff participated in an interagency team, which included DHS and DOE, formed to address the Aurora vulnerability. Currently, we continue to cooperate with DOE and DHS and share information concerning threats. As the only agency with authority to approve mandatory reliability standards regarding the nation's electric grid, the Commission can direct the ERO to develop any needed standard in an expedited timeframe.

QUESTION FROM THE HONORABLE MICHAEL T. MCCAUL, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

RESPONSES FROM JOE WEISS

Question 1.: What are the principal differences between the ISA 99 standards and the NIST best practices found in Special Publication 800–53?

Response: Although the developmental processes were different for NIST 800–53 and the ISA 99 standards, the results are harmonious. There has been a significant amount of cross-pollination of people between the NIST and ISA standards which will provide for a seamless transition between the standards. Both ISA and NIST address multiple industries and have similar content in those areas where the development is essentially complete. It should be noted that neither ISA nor NIST include the exceptions and exclusions found in the NERC CIP cyber security standards. Specifically, NIST SP 800–53 security controls address the management, operational, and technical safeguards, countermeasures, and/or compensating measures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. ISA 99 Part 2 covers the management and operational requirements. NIST will be performing a mapping between ISA 99 Part 2 and the NIST SP 800–53 management and operational security controls. ISA 99 Part 4 will cover the technical requirements. NIST has provided SP 800–53 to the ISA 99 Part 4 Working Group for consideration in the development of the Part 4 standard. No significant differences are expected.

QUESTION FROM THE HONORABLE PAUL C. BROUN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Question 2.: What, in your opinion, is the most egregious element of the NERC CIP standards? If they had to change one particular element to be in line with your recommendations, what would it be?3

The most egregious element of the NERC CIP standards is the scope, particularly the limitations and vagueness in NERC CIP–002. To be in line with my recommendations, there would need to be two changes. The first change would be to eliminate the exclusions of telecom, market functions, electric distribution, non-routable protocols, and nuclear power plants. The systems and protocols that have been excluded by the NERC CIP process have vulnerabilities that could affect the reliability of the electric grid. The second change would be to require all systems that are electronically connected (e.g., digital or analog connection of information or control systems) to be considered critical. These changes would result in the utilities addressing all systems throughout the enterprise that could be pathways into or out of the control system networks. These changes are consistent with what is required for securing business Information Technology applications and would make the NERC CIPs more consistent with the NIST framework.

QUESTION FROM THE HONORABLE BENNIE G. THOMPSON, COMMITTEEE ON HOMELAND SECURITY

RESPONSE FROM DAVID A. WHITELEY

AMENDED DECEMBER 12, 2007

Question 1.: 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? Please provide the Committee with a copy of the survey and a narrative of the results.

Response: Survey responses were received from 133 entities. The respondents included generating plant owners, generating plant operators, transmission owners, transmission operators, and load-serving entities. The respondents ranged from very large, multistate investor-owned utilities to small municipal utilities. Responses were received from all eight reliability regions.

The results of the survey indicate 94% of the mitigation measures recommended in the June 21 ES–ISAC advisory are completed or are in progress. This 94% consists of 60% completed and 34% in progress. The remaining 6% are not being performed for a variety of reasons (not applicable due to nature of equipment, being done by another entity, could compromise reliability rather than help reliability).

The respondents indicated they are taking a prioritized approach to the mitigation measures in applying them to their facilities. All respondents with nuclear facilities

indicated they have completed the mitigation measures associated with those facilities and are working on other, smaller facilities on a prioritized basis.

A copy of survey is enclosed.[1]

Question 2.: If a cyber exploit of the Aurora vulnerability is imminent, how will the Electric Sector ISAC ensure the immediate implementation of mitigation efforts?

Response: The Electricity Sector (ES) ISAC would initiate the following notification steps:

- 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.
- Send e-mail notifications to the electric industry through distribution lists designed for notification purposes. The NERC regional entities, the reliability coordinators, and all Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) are included on the lists. Also included on the lists are government agencies (NRC, DOE, DHS, FERC, Public Safety Canada), other critical infrastructure sector ISACs, and industry trade associations.
- The notification would recommend that the industry promptly complete the immediate mitigation measures identified in the ES–ISAC Advisory. In the case of the June 21, 2007 ES–ISAC Advisory, those mitigation measures included:

1. Robust cyber access mechanisms
2. Disable remote configuration change capability
3. Disable automatic re-close function
4. Add time delay to close function
5. Disable remote close function

Following notification to the industry, the ES–ISAC would follow-up to monitor progress in implementing the immediate measures. The progress would be tabulated and reported to appropriate government agencies.

Question 3.: One of the NERC standards requires an entity to identify its "critical assets" and "critical cyber assets," with the goal of ensuring that these assets are adequately protected from any potential cyber incident. Under the NERC definition, would the assets at issue in the Aurora vulnerability be considered "critical assets"?

Response: Critical assets determined using the methodology from NERC standard CIP–002–1 would include generation assets which are subject to the Aurora vulnerability. These typically will be large generators and "blackstart" generators (i.e., those generators used to restart the bulk power system following a large blackout). However, not *all* generators are essential to the reliable operation of the bulk electric system, and therefore would not be included on a list of critical assets.

Question 4.: Are the NERC CIP standards consistent with the lessons learned document issued after the August 2003 blackout?

Response: Yes. The NERC CIP Standards are consistent with the recommendations in the August 2003 blackout report.[1] There were 13 recommendations (R32 through R44) in the "physical and cyber security" section of the recommendations list in the blackout report. Of these, all of the recommendations that could properly be addressed through Reliability Standards are addressed by requirements of the CIP standards, as shown in the table below. Recommendation 36 is not a standards issue, and recommendations 37 and 39 will require research before standards can be written to fully address the recommendation.

Recommendation	Relevant CIP Standard
32—Implement NERC IT Standards	CIP 002–009
33—IT Management Procedures	CIP 003, 007
34—Corporate Level IT Governance	CIP 003
35—Manage IT System Monitoring	CIP 005, 007, 008, 009

[1] See to committee file.

[1] Final Report on the August 14, 2003 "Blackout in the United States and Canada: Causes and Recommendations", U.S.-Canada Power System Outage Task Force, April 5, 2004. The recommendations regarding physical and cyber security appear at pages 163–169 of the Report, which is available at: *http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf.*

Recommendation	Relevant CIP Standard
36—US-Canada Risk Management Study	Government Study recommendation
37—IT Forensics and Diagnostics	CIP 004, 009 Research recommendation
38—Assess Risk and Vulnerability	CIP 002, 005, 007
39—Wireless and Remote Intrusion	CIP 005, Research recommendation
40—Control Access	CIP 006
41—Guidance for Background Checks	CIP 004
42—Confirm Role of NERC ES–ISAC	CIP 008
43—Establish Clear Authority	CIP 003
44—Prevent Information Disclosure	CIP 003

Not all the recommendations in the report address topics that are relevant to NERC standards development. Recommendation R36 deals with an intergovernmental action (initiation of a U.S.-Canada risk management study), not a performance standard requirement appropriate for incorporation into a Reliability Standard. Recommendation R41 is addressed in CIP 004, although there are significant legal and jurisdictional issues contained in its implementation that would need to be resolved outside the standards development process. The subject matter of that recommendation, moreover, is addressed by an existing NERC security guideline (scheduled for update in 2008). Recommendation R42 (confirmation of NERC ES–ISAC as the central point for sharing security information and analysis) is addressed in CIP 008. The recommendation also has been addressed outside NERC's standards process through the use of an incident reporting guideline. The guideline approach is better suited for this issue due to the frequent change in reporting procedures and protocols.

Question 5.: Do you agree with your NERC colleague Stan Johnson, who stated that this test "is not a realistic representation of how the power system would operate"?

Response: Yes. The test completed at Idaho National Lab (INL) and depicted in the video was a 30-second edited version of over three minutes of actual test. The generator in the test was a stand-alone diesel generator rated at 3.5 MW. While it is true that generators like the one in the test are connected to the grid in North America, they are not the backbone of the system and represent a very small portion of the total generating resources available. The true backbone of the system is large generators rated at 300 to 1,100 MW. These large generating units have more sophisticated protection systems that would most likely isolate the generators from the attack long before the effects (black smoke, repetitive shaking, parts falling off) shown in the video. The test at INL was conducted with the power system in an optimal configuration for an attacker to be successful. In the real power system, the power flows in a highly complex network make a successful attack much more difficult. The power flows on the network vary from day to day depending on what equipment is in-service or out-of-service. The direction and magnitude of the flows would have to be understood and taken advantage of by the attacker. While the test at INL helped demonstrate the feasibility of a cyber attack resulting in physical damage, a more comprehensive test would be very difficult, if not impossible to conduct.

Question 6.: Can NERC effectively conduct oversight over electric sector owners and operators, considering that NERC operates under dues received by these same companies?

Response: Yes. NERC does not operate under a system of dues, which suggests an element of voluntariness in the payments. Rather, Section 215 of the Federal Power Act, the regulations of the Federal Energy Regulatory Commission, and NERC's bylaws and rules were specifically written to preclude undue influence by electricity sector stakeholders. Within the United States, NERC is funded through assessments to load serving entities that are approved annually by FERC. Once approved, those assessments constitute a legally binding obligation to pay that is enforceable, ultimately, through federal law. FERC also approves NERC's budget each year, which specifies how funds raised by assessment will be used for NERC's var-

ious responsibilities, including enforcement. While electric sector owners and operators, along with all other electricity sector stakeholders, have the opportunity to express their views about NERC's annual budget and assessment, electricity sector stakeholders do not have decisional authority over NERC's budget or assessments. NERC's annual budget and assessments are approved, in the first instance, by NERC's independent board of trustees, and thereafter by FERC.

Question 7.: In his testimony, Mr. Weiss recommends that NERC incorporate the NIST Framework into its CIP standards. My understanding is that the NIST Framework is still a work in progress that is still subject to further amendment, and that it is intended to serve as model guidelines for federal government agencies, not mandatory standards applicable to the private sector with enforcement and penalty provisions. If this is true, please comment on whether the NIST Framework is actually an appropriate model for electric industry CIP standards that are required under the Federal Power Act (as amended by the Energy Policy Act of 2005) to be mandatory and enforceable? Please also comment on other reasons why the NIST Framework may not be an appropriate model for the NERC standards, including the lack of a formal stakeholder process required by Sec. 215 of the Federal Power Act, enacted by Congress in 2005 to govern the development of the NERC CIP standards.

Response: The NIST Framework[2] consists of a number of documents, including Federal Information Processing Standards (FIPS) 199 and 200 (standards) and NIST Special Publications (SP) 800–60, 800–53, 800–30, 800–18, 800–53A, and 800–37 (guidance and recommendations). As with other NIST SP800 documents, NIST SP800–53, Recommended Security Controls for Federal Information Systems, is self-described as "guidance documents and recommendations"[3] to be used in support of federal agencies' compliance activities with the mandatory Federal Information Processing Standards (FIPS) that implement the Federal Information Security Management Act (FISMA) of 2002.

The NIST guidance, as it exists in its approved format, was developed in support of FISMA for conventional IT security issues relating to conventional IT use of computers—the approved NIST guidance was not developed for industrial control systems. NIST is developing revised guidance for applicability to industrial control systems (ICS), but that has not been finalized. The revised guidance is in its 'final' public draft, with comments on the draft due on December 14, 2007. NIST plans on publishing the fully revised document within two weeks of the close of the comment period. As such, the revised ICS guidance does not yet formally exist, and therefore, could not today be included in any NERC CIP standards.

One major issue with the application of the NIST standards and guidance to the private sector deals with the assessment of impact, based on a significantly broader scope than the specific focus of the NERC Standards on the reliable operation of the bulk power system. The NIST standards and guidance process requires that *all* computer-based processes be considered, even those that have no bearing on reliable operations (and which are outside the scope of Section 215 of the FPA), including administrative functions and market functions. While these may have bearing on the business processes of the effected entities, they cannot be made mandatory under the auspices of reliability standards within the scope of Section 215.

Another issue with the application of the NIST standards and guidance is the level of technical detail included in the guidance, much of which does not directly relate to bulk power system reliability. The FIPS–199 concept of a "high water mark" for security classification requires, for example, that if any one component of a system requires a medium or high level of confidentiality, *all* components of that system must be implemented with a high confidentiality without regard to the resultant impact to operations, even if that result were detrimental to reliable operations. This will result in significantly more work required to achieve and maintain compliance with the standards, without any reliability-based benefit.

While there is a formal approval process for NIST *standards,* which require the approval of the Secretary of Commerce, there does not appear to be any formal documented process for creating, revising or approving NIST *guidance.* Further, the NIST (FIPS) standards allow the inclusion by reference of other documents (*e.g.,* SP800–53). These referenced documents do not have the same level of approval required as the formal text of the standards.

---

[2] See document references available from *http://www.csrc.nist.gov/groups/SMA/fisma/framework.html.*

[3] NIST Special Publication 800–53 rev 1, page iv, available at *http://www.csrc.nist.gov/publications/nistpubs/800–53-Rev1/800–53-rev1-final-clean-sz.pdf.*

In contrast, Section 215 of the FPA requires that "reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards" be provided by the Electric Reliability Organization certified by FERC (*i.e.,* NERC) in developing Reliability Standards. These requirements are incorporated in FERC's rules for certification of the ERO, and in the NERC rules of procedure as approved by FERC. The NERC process requires that "[a]ll mandatory requirements of a reliability standard shall be within an element of the standard,"[4] thereby ensuring that all mandatory and enforceable standards follow the same rigorous review and approval process approved by FERC as consistent with the statutory requirements. The NERC process allows the development of guidance, but cannot make those documents binding as mandatory and enforceable standards.

Question 8.: Concerns have been raised regarding the potential that one or more isolated cyber failures or attacks to electric distribution system assets could directly lead to more widespread failures or electric outages in the bulk power system. **Please explain if the standard radial design of electric distribution systems makes such a scenario unlikely, and if it in fact enhances the ability of electric utilities to isolate the impact of such events.**

Response: The distribution system is primarily a point-to-point system, with lines emanating in a radial pattern, from the local substation to the consumer. When a distribution line is taken out of service by a falling tree in an ice storm, for example, electricity no longer flows on that spoke and the consumers' lights go out. However, the problem is limited and localized. That is the nature of the distribution system—it is local and affects a limited area.

One or more isolated cyber attacks or failures on the distribution system will have a localized and limited effect. In addition, the isolation and protection requirements of the NERC CIP standards protect the bulk power system from intrusion reaching through the distribution system to bulk power system assets. For one or more isolated cyber failures or attacks to impact the bulk power system would require a very complex, coordinated, synchronized action. It would require a knowledgeable and determined attacker to exploit a vulnerability. While technically feasible, the likelihood is low of such a scenario successfully occurring.

Question 9.: My understanding is that the current ISA security standards and technical reports that Mr. Weiss recommends for incorporation in the NERC CIP standards are intended to be used as guidance, not to establish expectations for auditable compliance, and there are no measures or levels of noncompliance currently associated with ISA99. Levels of noncompliance would need to be created and approved before the standards could be used as mandatory and enforceable. **Do you think that such measures could be developed, if such measures are even possible, and how much time would it take to develop those measures?**

Response: Much like the status of the NIST guidance for industrial control systems, the ISA standards are still a work in progress. To date, only two "technical reports" which do not contain any requirements (*i.e.,* they are "informative" and not "normative" in nature) have been approved. Because these approved documents do not contain any "normative" requirements, quantifiable measures cannot be developed for them. The ISA standards themselves are being developed in at least four parts (or volumes), and of the four publicly documented parts, one deals with establishing terminology, concepts and models, and two deal with the establishment and operations of a security program. Only the fourth part deals with "Specific Security Requirements for Industrial Automation and Control Systems."

This fourth part has just been started, so it is impossible to determine how measures, levels of noncompliance, or violation risk factors (all of which are required elements of NERC standards, and are required for the compliance program activities) could be developed for any explicit requirements contained in that standard. It is unknown how long the process to develop those measures would require.

Question 10.: Appendix F of the NIST 800–53 standards lists at least 25 instances where an exception to compliance for Industrial Control Systems (ICS) may be taken when "the organization determines it is not feasible or advisable (e.g., adversely impacting performance, safety, reliability)". FERC has indicated that exemptions under "technically feasible" should be as limited as possible, yet it appears that incorporation of the NIST standards would allow for a very broad exemption under technical feasibility. Can you comment on this?

---

[4] NERC Reliability Standards Development Procedure, Version 6.1, available at *ftp://ftp.nerc.com/pub/sys/all__updl/oc/stp/RSDP__V6__1__12Mar07.pdf.*

Response: The NIST standards do not meet the Commission's expectations.

Question 11.: What would be the result if the electric industry was forced to implement the NIST best practices for control systems based upon SP 800–53?

Response: Any change now in cybersecurity requirements for the bulk power system would significantly retard progress toward more robust cybersecurity protections.

A requirement to adopt NIST "best practices" now would result in a suspension of the current efforts to implement the proposed NERC cybersecurity standards pending a review of the NIST standards. The result of the review would require new implementation plans and additional time.

The loss of industry compliance momentum and the delay in implementing mandatory bulk power system cybersecurity standards would be detrimental to the reliability of the bulk power system.

Question 12.: Are owners and operators of distribution facilities included within the NERC membership? If so, regardless of the authority extended in the Energy Policy Act, doesn't it make sense that distribution facilities be included in reliability considerations?

Response: Within the United States there are approximately 3,000 entities that own or operate distribution facilities. Approximately 375 of those entities are NERC members. NERC's authority to set and enforce reliability standards is not contingent on NERC membership, but extends to owners, operators and users of the bulk power system, whether or not they are a member of NERC. NERC can and does take account of the impact of distribution facilities on the reliability of the bulk power system. NERC can exercise jurisdiction over owners, operators, and users of the bulk power system.

Question 13.: How does NERC ensure that its members are making efforts to mitigate the Aurora vulnerability that we know exists within control systems?

Response: The Electricity Sector Information Sharing and Analysis Center (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 is working with the electricity sector entities to mitigate the vulnerabilities in the system by providing information about the vulnerability, recommending mitigation measures, and following up to monitor successful completion.

The ES–ISAC has worked closely with all segments and all levels in the industry to mitigate the vulnerabilities. Meetings have been held with representatives of all the major trade associations (EEI, APPA, NRECA), the CEOs of the largest companies, the Electricity Sector Coordinating Council, numerous operating level committees, and groups of technical experts.

Because the steps needed to mitigate the Aurora vulnerability are not reflected in approved reliability standards, NERC has no authority to compel those actions. Not all subjects are the appropriate topic for standards. The standards development process is by design a public and transparent one, and matters such as the Aurora vulnerability do not lend themselves to that public process. However, NERC believes the industry is demonstrating excellent judgment and cooperation in completing the implementation of the mitigation measures.

Question 14.: In your testimony you mention that NERC as the Electric Reliability Organization (ERO) was not given authority over facilities used for distribution of electric power. **Who has authority to enforce regulations over such facilities?**

Response: NERC as the electric reliability organization only has enforcement authority over the bulk power system. The definition of "bulk power system" in Section 215(a)(1) of the Federal Power Act expressly excludes facilities used for local distribution. Authority over facilities used for local distribution is generally reserved to the states, and the scope of that authority varies from state to state. State public utility commissions exercise such authority to the extent the utilities are within their jurisdiction. In a number of states, municipal utilities are not within the jurisdiction of state commissions.

Question 15.: NERC has proposed its own set of cybersecurity standards—will these standards make a difference, i.e. will they make us safer than we are today without these standards? Will there be more to do after these standards are accepted by FERC in their current form?

Response: The answer to both these questions is "yes." These standards represent a first step in a process of continually increasing the cybersecurity of the electricity industry. While some companies already meet or exceed the requirements of these standards, the vast majority of the industry is working very hard right now to meet both the letter and intent of the standards as they are written (and expected to be approved by FERC). Essentially every company has had to do some work in order to meet either the technical requirements, or provide sufficient documentation to prove during an audit that they have met the requirements. Many companies are analyzing their systems, and implementing policy-based and technical controls to significantly increase the cyber security posture, especially at their substations and power plants.

Since these standards represent a first step, there will be additional steps. Making the modifications proposed by FERC in the pending NOPR to approve the NERC Reliability Standards will be among the additional steps to be taken in this area. As the industry gains experience and confidence in implementing cybersecurity protections, and as the vendors of control systems begin to implement increased cybersecurity protections into their systems, the cybersecurity posture of the industry will increase, and additional standards can be written to ensure that all industry participants are continuing to "raise the bar" in their cybersecurity protections. NERC's rules, and a condition of accreditation by the American National Standards Institute, require that each standard be reviewed at least every five years. NERC anticipates completing the review and upgrade of all standards over a three-year period. The cybersecurity standards are scheduled for review in 2009 to asses them based on lessons learned to that point. NERC's standards development procedure provides a systematic approach to improving to the standards and documenting the basis for those improvements, and should serve as the mechanism for achieving those improvements.

The future revisions to the NERC cyber security standards will take place after the NIST guidance on security to Industrial Control Systems has been finalized, and it is likely that some of the recommendations in that guidance will be included in revised Reliability Standards. These recommendations will be analyzed and included (or not) based on their impact on the reliable operation of the bulk power system.

Question 16.: You mentioned in your testimony that the CIP standards were developed in a rigorous process. **How does NERC plan on operating if and when it must develop security standards much quicker than the rigorous standard process allows? Are there any contingency plans in place for when immediate action is necessary?**

Response: NERC operates according to its Rules of Procedure that have been approved by the Federal Energy Regulatory Commission. Section 300 of the Rules of Procedure discusses the reliability standards development processes. Rule 308 acknowledges that the current Reliability Standards Development Procedure (Version 6.1) includes a provision for approval of urgent action standards that can be completed within 60 days and emergency actions that may be further expedited. Further, Rule 309.3, Directives to Develop Standards Under Extraordinary Circumstances, stipulates the urgent approval action procedure may be utilized if necessary to meet a timetable for action required by governmental authorities or circumstances, respecting to the extent possible the provisions in the standards development process for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing reliability standards. After making a written finding that an extraordinary and immediate threat exists to bulk power system reliability or national security, the NERC independent Board of Trustees has discretion to substantially reduce the public notice and balloting periods, thus expediting the development timeframe.

When standards are implemented using the urgent action or emergency process, one of the following three actions must occur:

—If the urgent or emergency action standard is to be made permanent without substantive changes, then the standard must proceed through the regular standards development process within one year of the urgent or emergency action approval.

—If the urgent or emergency action standard is to be substantively revised or replaced by a new standard, then a request for the new or revised standard must be initiated as soon as practical after the urgent or emergency action ballot, and the standard must proceed through the regular standards development process as soon as practical within two years of the urgent or emergency action approval.

—The urgent or emergency action standard may be withdrawn through the regular standards development process within two years.

To address immediate threats, NERC can issue an "Essential Action" alert as proposed and currently pending before FERC in Rule 808.10 of NERC's Rules of Procedure. An "Essential Action" alert identifies specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the bulk power system to take to ensure the reliability of the bulk power system. Such alerts require NERC Board approval before issuance. These alerts are not mandatory, and NERC has no enforcement authority regarding these alerts, but NERC believes they can be a very useful tool in communicating to industry participants actions that are needed on an immediate basis to protect bulk system reliability.

AMENDMENT

Question 1. 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? Please provide the Committee with a copy of the survey and a narrative of the results.

Response: The written follow-up survey was distributed on October 19, 2007. Survey responses were received from 133 entities. The respondents included generating plant owners, generating plant operators, transmission owners, transmission operators, and load-serving entities. the respondents ranged from very large, multistate investor-owned utilities to small municipal utilities. Responses were received from all eight reliability regions.

The results of the survey indicate 94% of the mitigation measures recommended in the June 21 ES–ISAC advisory are completed or are in progress. This 94% consists of 60% completed and 34% in progress. The remaining 6% are not being performed for a variety of reasons (not applicable due to nature of equipment, being done by another entity, could compromise reliability rather than help reliability).

The respondents indicated they are taking a prioritized approach to the mitigation measures in applying them to their facilities. All respondents with nuclear facilities indicated they have completed the mitigation measures associated with those facilities and are working on other, smaller facilities on a prioritized basis.

Note: ES–ISAC, ELECTRICITY SECTOR, INFORMATION SHARING AND ANALYSIS CENTER, OPERATED BY NERC, "ESISAC Advisory Follow-up Survey", October 19, 2007, see committee file.

QUESTIONS FROM THE HONORABLE PAUL BROUN, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

RESPONSES SUBMITTED BY GREG WILSHUSEN

Responses from David A. Powner
Director, Information Technology Management Issues

Questions: In your review of the various programs in the federal government and the private sector to secure control systems, (1) do you identify any clear gaps in efforts? (2) As well are there any clearly duplicative programs working in parallel? (3) Are there initiatives that don't exist that should?

Responses: (1) We have identified gaps in programs in the federal government and private sector to secure control systems. As we reported in September 2007,[1] *The National Strategy to Secure Cyberspace*[2] directs the Department of Homeland Security, in coordination with the Department of Energy and other agencies, to work in partnership with private industry in increasing awareness of the importance of efforts to secure control systems, developing standards, and improving policies with respect to control systems security. However, we reported that the federal government does not yet have an overall strategy for guiding and coordinating control systems security efforts across the multiple agencies and sectors. In addition, more can be done to coordinate related control system activities within and across sectors and across the government. For example, while the Department of Energy has led the development of an industry road map to secure control systems for the energy sector, we have not seen evidence that other sectors, such as transportation, have developed such road maps. Another gap we reported is that the Department

[1] 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)..

[2] The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

of Homeland Security lacks a rapid, efficient process for disseminating sensitive information to private industry owners and operators of critical infrastructures.

(2) We reported that overlapping and possibly duplicative control systems security activities may exist. For example, there are multiple efforts underway to develop standards for control systems security. These include industry specific standards, such as the North American Electric Reliability Corporation standards and the American Gas Association standards, as well as more general standards, such as the ISA (formerly the Instrumentation, Systems, and Automation Society) standards and, within the federal government, the National Institute of Standards and Technology standards. Each has different levels of specificity, and the opportunity exists to better coordinate and harmonize these standards.

(3) With respect to your question on initiatives, actions could be taken to reduce or eliminate gaps and duplicative activities discussed above. For example, we previously recommended that the Department of Homeland Security develop a governmentwide strategy for securing control systems. As it moves forward with this effort, it should take the opportunity to identify and coordinate the activities described above and other control systems activities. In addition, industry experts spoke of the beneficial value of the activities of the national laboratories in working with control systems vendors and operators and the benefit of possibly expanding such activities.

In responding to these questions, we relied on previous audit work we preformed in developing our report on critical infrastructure control systems, as well as ongoing work examining security of control systems.