CYBERSECURITY FOR POWER SYSTEMS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON ENERGY &
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

October 21, 2015

Serial No. 114–43

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
97–762PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing 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 SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
F. JAMES SENSENBRENNER, JR., Wisconsin
DANA ROHRABACHER, California
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
BILL JOHNSON, Ohio
JOHN R. MOOLENAAR, Michigan
STEVE KNIGHT, California
BRIAN BABIN, Texas
BRUCE WESTERMAN, Arkansas
BARBARA COMSTOCK, Virginia
GARY PALMER, Alabama
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DARIN LaHOOD, Illinois

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
ALAN GRAYSON, Florida
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
KATHERINE M. CLARK, Massachusetts
DON S. BEYER, JR., Virginia
ED PERLMUTTER, Colorado
PAUL TONKO, New York
MARK TAKANO, California
BILL FOSTER, Illinois

SUBCOMMITTEE ON ENERGY

HON. RANDY K. WEBER, Texas, *Chair*

DANA ROHRABACHER, California
RANDY NEUGEBAUER, Texas
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
THOMAS MASSIE, Kentucky
STEPHAN KNIGHT, California
BARBARA COMSTOCK, Virginia
BARRY LOUDERMILK, Georgia
LAMAR S. SMITH, Texas

ALAN GRAYSON, Florida
ERIC SWALWELL, California
MARC A. VEASEY, Texas
DANIEL LIPINSKI, Illinois
KATHERINE M. CLARK, Massachusetts
ED PERLMUTTER, Colorado
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma
MICHAEL T. MCCAUL, Texas
RANDY HULTGREN, Illinois
JOHN R. MOOLENAAR, Michigan
BRUCE WESTERMAN, Arkansas
DAN NEWHOUSE, Washington
GARY PALMER, Alabama
RALPH LEE ABRAHAM, Louisiana
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
ELIZABETH H. ESTY, Connecticut
KATHERINE M. CLARK, Massachusetts
PAUL TONKO, New York
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
EDDIE BERNICE JOHNSON, Texas

CONTENTS

October 21, 2015

Opening Statements

Witnesses:

Appendix I: Answers to Post-Hearing Questions

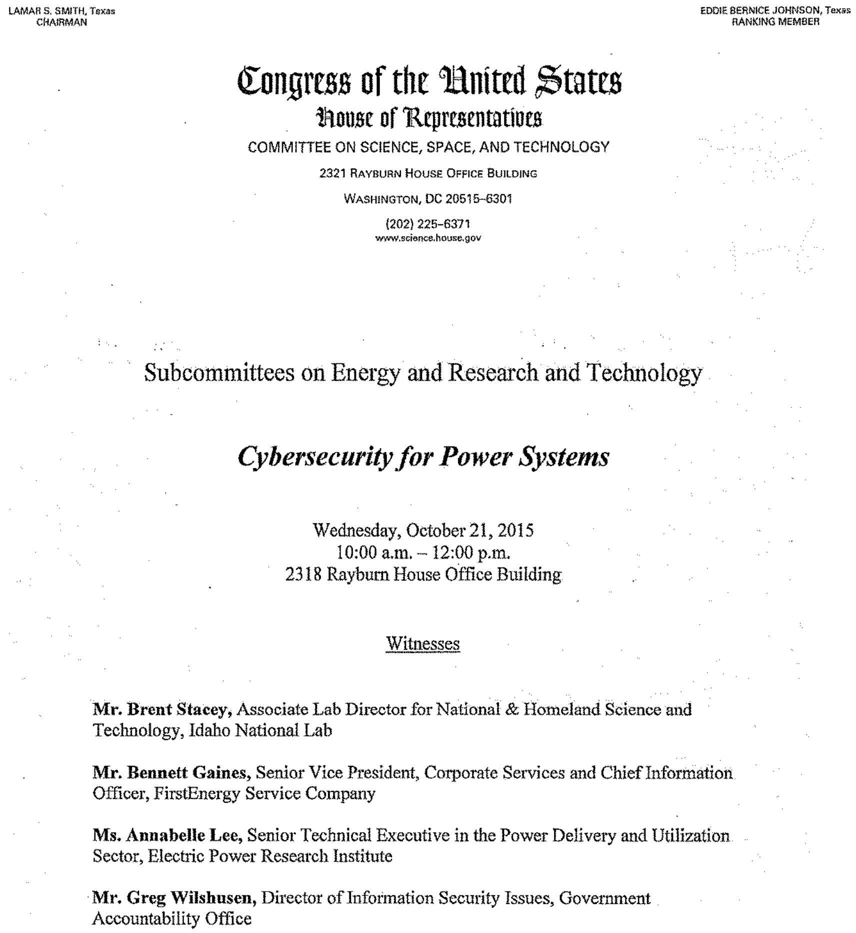
Appendix II: Additional Material for the Record

CYBERSECURITY FOR POWER SYSTEMS

WEDNESDAY, OCTOBER 21, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ENERGY &
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:04 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Randy Weber [Chairman of the Subcommittee on Energy] presiding.



LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittees on Energy and Research and Technology

Cybersecurity for Power Systems

Wednesday, October 21, 2015
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Mr. Brent Stacey, Associate Lab Director for National & Homeland Science and Technology, Idaho National Lab

Mr. Bennett Gaines, Senior Vice President, Corporate Services and Chief Information Officer, FirstEnergy Service Company

Ms. Annabelle Lee, Senior Technical Executive in the Power Delivery and Utilization Sector, Electric Power Research Institute

Mr. Greg Wilshusen, Director of Information Security Issues, Government Accountability Office

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON ENERGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

Cybersecurity for Power Systems

HEARING CHARTER

Wednesday, October 21, 2015
10:00 a.m. – 11:30 a.m.
2318 Rayburn House Office Building

PURPOSE

The Subcommittees on Energy and Research and Technology will hold a joint hearing titled *Cybersecurity for Power Systems* on Wednesday, October 21, 2015, starting at 10:00 a.m. in Room 2318 Rayburn House Office Building. The purpose of this hearing is to examine efforts by federal agencies, industry, and the Department of Energy national labs to mitigate cybersecurity threats to the U.S. power supply. Witnesses have been asked to outline operating techniques and technology that can be used to prevent system vulnerability to cyber-attacks in the electric sector. This hearing will explore solutions to mitigate cyber threats identified in a Committee hearing last September entitled *Examining Vulnerabilities of America's Power Supply.*[1]

WITNESSES

- **Mr. Brent Stacey,** Associate Lab Director for National & Homeland Science and Technology, Idaho National Lab
- **Mr. Bennett Gaines,** Senior Vice President, Corporate Services and Chief Information Officer, FirstEnergy Service Company
- **Ms. Annabelle Lee,** Senior Technical Executive in the Power Delivery and Utilization Sector, Electric Power Research Institute
- **Mr. Greg Wilshusen,** Director of Information Security Issues, Government Accountability Office

BACKGROUND

American critical energy infrastructure, including electrical power plants, transmission and distribution lines, oil and gas pipelines, and transformers and substations remain some of the most vulnerable critical infrastructure to cyber-attack. The Department of Homeland Security has designated the energy sector as one of 16 critical infrastructure sectors, largely due to the

[1] Information on the hearing available at: https://science.house.gov/legislation/hearings/examining-vulnerabilities-america-s-power-supply-0

"enabling function" energy contributes across all critical infrastructure sectors.[2] Maintaining the stability and security of the electric grid will require modernization of existing industrial control systems and increasing incorporation of two-way, internet connected systems to manage reliability as more distributed energy systems are introduced to the electric grid.[3]

As discussed during the Committee hearing last September, America's electric grid is being modernized through an increased use of "smart grid" technology and distributed energy sources. However, this modernization also increases the risk of cyber-attack.[4] While smart grid technology uses digital information and control technology to improve reliability, security, and efficiency of the electric grid, adding technology that increases the interconnectedness of industrial control and IT systems can increase its vulnerability to cyber-attack.[5]

System Vulnerabilities

One key area of vulnerability within the grid is the Supervisory Control and Data Acquisition (SCADA) system that has been in use since the 1970s. These legacy systems have historically consisted of remote terminal units often connected to mainframe computers via telephone lines or radio connections and were not connected to central IT networks. Over the years, electric grid modernization efforts have increasingly created more access points to these analog systems.[6] As these legacy systems were not designed with IT network vulnerabilities in mind, digital security features were not integrated into their industrial control systems.

The integration of distributed generation and digital operating systems in conventional power plants can also increase cybersecurity vulnerabilities for critical energy infrastructure. While distributed generation and micro-grids can increase grid resiliency in the event of a disruption, more access points for cyber-attacks are created as distributed energy sources and users (e.g., plug-in electric vehicles) are added to power grid.[7]

Another area of vulnerability for cyber-attack is the increasing integration of "smart grid" technology. In practice, the "smart grid" generally refers to a technology used to modernize utility electricity delivery systems using computer-based remote control and automation that incorporate two-way communication technology and computer processing that has been used for decades in other industries into functions on the electric grid.[8] While the vast majority of America's electric power grid today primarily delivers electricity in a one-way flow from

[2] Department of Homeland Security, *Critical Infrastructure Sectors*. Last updated August 26, 2015. Available at http://www.dhs.gov/critical-infrastructure-sectors

[3] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

[4] Bartol, Nadia, *Statement before the Subcommittee on Oversight and Subcommittee on Energy, Committee on Science, Space, and Technology*. Examining Vulnerabilities of America's Power Supply, July 30, 2015. Available at https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY21-WState-NBartol-20150910.pdf

[5] Department of Energy, Office of Electricity Delivery & Energy Reliability, *Smart Grid*. Available at: http://energy.gov/oe/services/technology-development/smart-grid

[6] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

[7] Ibid.

[8] Ibid.

generator to outlet, the number of interconnected smart grid devices is only expected to grow, with industry experts estimating that there could be as many as 50 billion interconnected smart devices in the world by 2020.[9] This increased use of smart grid technology adding automatic two-way communication between distribution and consumption sites creates cybersecurity vulnerabilities to the system as a whole.[10]

In addition, the security and privacy measures built into smart electricity meters could put American consumers' personal information at risk, as these systems send data about energy use wirelessly to electric distribution companies and control the flow of power to customers.[11] Components of the smart grid are also controlled by software, which may make these devices and functions subject to manipulation over the network.

Ongoing Threats

While there has been no reported cyber-attack that has resulted in widespread loss of power, there have been many attempted attacks. An investigation completed by USA Today earlier this year found that the United States power grid "faces physical or online attacks approximately 'once every four days.'"[12] In addition, it appears that these cyber threats could be highly sophisticated. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into industrial control systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[13] Increasing examples of cyber intrusions and malware (such as BlackEnergy, HAVEX, and Sandworm) on industrial control systems of critical infrastructure have also been reported. [14]

Federal Mitigation Efforts

Federal cybersecurity management, regulation, research, and development for energy systems is distributed between the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC) the Department of Energy, the Department of Homeland Security, and the National Institute for Standards and Technology (NIST). The Energy Independence and Security Act of 2007 (EISA) established federal support for the modernization of America's electric grid and required actions on cybersecurity by a number of federal agencies, including the National Institute of Standards and Technology (NIST), FERC, and DOE.[15]

[9] Bartol, Nadia, *Statement before the Subcommittee on Oversight and Subcommittee on Energy, Committee on Science, Space, and Technology*. Examining Vulnerabilities of America's Power Supply, July 30, 2015. Available at https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY21-WState-NBartol-20150910.pdf

[10] National Institute of Standards and Technology, *Smart Grid: A Beginner's Guide*. Available at: http://www.nist.gov/smartgrid/beginnersguide.cfm

[11] Campbell, Richard J., *The Smart Grid and Cybersecurity – Regulatory Policy and Issues*. Congressional Research Service, June 15, 2011. Available at: http://www.crs.gov/pdfloader/R41886

[12] Ibid.

[13] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System*. Congressional Research Service, June 10, 2015. Available at: http://www.crs.gov/pdfloader/R43989

[14] Ibid.

[15] Wilshusen, Gregory. *Challenges in Securing the Modernized Electricity Grid*. Testimony

Today, NIST has developed *Guidelines for Smart Grid Cybersecurity*, a comprehensive, voluntary framework for industry to follow in developing effective cybersecurity strategies. NIST also led the development of the "Framework for Improving Critical Infrastructure Cybersecurity," outlining industry methodologies, procedures, and processes to synchronize approaches to address cyber risks.[16] FERC, the federal regulatory agency, continues to approve industry cybersecurity standards developed and proposed by the private corporation NERC. NERC also manages the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which is designed to establish situational awareness, incident management, coordination, and communication capabilities across America's power grid operators through timely information sharing.[17]

The Department of Energy has established initiatives to facilitate development of industry tools for voluntary risk assessment and smart grid technology, and the Department of Energy National labs provide risk assessment, modeling, and technology development expertise, including the Cyber Security Test Bed at Idaho National Lab that allows industry to test control systems under the conditions of a cyber-attack.[18] The Department of Homeland Security operates the National Cybersecurity and Communications Integration Center (NCCIC) to facilitate information sharing between public and private entities to reduce vulnerabilities and improve mitigation and recovery response, as well as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), designed to strengthen industrial control systems in electric systems.[19]

Due in part to the number of agencies involved in the process, federal and state cyber threat mitigation efforts are often burdened by different and unclear regulatory authorities, lack of monitoring to ensure industry standards are met, slow communication between agencies, and effective information sharing between industry and relevant federal entities. These challenges have been repeatedly identified by the Government Accountability Office (GAO).[20]

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. February 28, 2012. Available at http://gao.gov/assets/590/588913.pdf

[16] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* . February 12, 2014, available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[17] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System.* Congressional Research Service, June 10, 2015. Available at: http://www.crs.gov/pdfloader/R43989

[18] Idaho National Laboratory. *INL Cyber Security Research: Defending the Network Against Hackers.* Department of Energy. Available at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-INL_Cyber_Security_Research.pdf

[19] Campbell, Richard J., *Cybersecurity Issues for the Bulk Power System.* Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

[20] Wilshusen, Gregory. *Challenges in Securing the Modernized Electricity Grid.* Testimony
Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. February 28, 2012. Available at http://gao.gov/assets/590/588913.pdf

Additional References:

1. McMillian, Robert. "Cyber Risk Isn't Always in the Computer: Vulnerable industrial systems that support data centers can open a back door to hackers" Wall Street Journal. Sept. 24, 2015. Available at http://www.wsj.com/articles/cyber-risk-isnt-always-in-the-computer-1443125108.

2. Reilly, Steve. "Bracing for a big power grid attack: 'One is too many'" USA Today. March 24, 2015. Available at http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/

Chairman WEBER. Good morning, and welcome to today's joint Energy and Research and Technology Subcommittee hearing examining cyber threats to American energy systems.

Today, we will hear from an expert panel on the growing threat of cyber attacks to the nation's electric grid. Our witnesses today will also provide insight into how industry and the federal government are working together, or maybe in some instances not working together, to anticipate cyber threats, and improve the reliability and resiliency of our electric grid against those cyber attacks.

The reliability of America's power grid is one of our greatest economic strengths. I like to say, the things that make America great are the things that America makes, and how do we do that? With an affordable, reliable, dependable electricity supply.

In my home State of Texas, reliable and affordable power serves a population that is increasing by more than 1,000 people a day, and it provides power to the energy-intensive industries that drive consumption. Texas is by far the nation's largest consumer of electricity. Keeping the Texas power grid reliable and secure is key to continuing this economic growth.

But as we established in a hearing on broad threats to the power supply earlier this year, utilities face significant threats to that same reliable delivery of power. Our electric grid is particularly vulnerable to growing cybersecurity threats as the grid is modernized, as distributed energy, electric vehicles, and modernized digital operating systems create more access points for cyber attacks. And while the nation's industrial control systems for the grid are analog systems designed to last for decades, digital IT systems must constantly adapt to combat evolving cyber threats.

Small-scale cyber and physical attacks to our electric grid are estimated to occur once every four days, and in over 300 cases of significant cyber and physical attacks since 2011, suspects have never been identified. Now, let me repeat that. In over 300 cases of significant cyber and physical attacks since 2011, no suspects have been identified.

We often think of cybersecurity and other threats to the power grid at a macro scale, but these types of attacks can occur even at a local level. In 2011, the Pedernales Electric Co-op, a non-profit co-op that serves approximately 200,000 customers north of San Antonio, was struck by a cyberattack. While the attack thankfully did not disrupt power to consumers, it is a stark reminder that threats to the grid are real, and they are not going to go away anytime soon.

Our nation's power supply cannot be protected overnight, particularly as utilities struggle to adapt technology to manage a growing number of cybersecurity threats. Cyber threats to the power grid will continue to evolve, particularly as more interconnected smart technologies are incorporated into the electric grid. We call those smart meters back in Texas. And as protective technology improves, so does the capability and creativity of those who are conducting those cyber attacks, unfortunately.

While we cannot predict every method of attack, the federal government can and should play a role in assisting industry with developing new technology and security safeguards. Accordingly, research and development efforts at the Department of Energy are focused on providing industry with comprehensive tools to conduct internal analysis to identify and address cybersecurity weaknesses so that the industry can take the lead in addressing these same vulnerabilities.

That is why testing facilities and cooperative research, like the Cyber Security Test Bed at Idaho National Lab, are valuable tools to combat cyber threats. At INL, industry can test control systems technology in real world conditions, reducing response time and risk for future attacks.

I'd like to say in advance I want to thank the witnesses for testifying before the Committee today. I look forward to a discussion about cyber threats to our critical infrastructure, and how the federal government can provide industry with the tools and technology necessary to fight the next generation of cyber attacks.

[The prepared statement of Chairman Weber follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON ENERGY CHAIRMAN RANDY K. WEBER

Good morning and welcome to today's joint Energy and Research and Technology Subcommittee hearing examining cyber threats to American energy systems. Today, we will hear from an expert panel on the growing threat of cyber-attacks to the nation's electric grid.

Our witnesses today will also provide insight into how industry and the federal government are working together to anticipate cyber threats, and improve the reliability and resiliency of our electric grid against cyber-attacks.

The reliability of America's power grid is one of our greatest economic strengths. In my home state of Texas, reliable and affordable power serves a population that is increasing by more than 1,000 people per day, and provides power to the energy intensive industries that drive consumption. Texas is by far the nation's largest consumer of electricity. Keeping the Texas power grid reliable and secure is key to continuing this economic growth.

But as we established in a hearing on broad threats to the power supply earlier this year, utilities face significant threats to the reliability of power delivery. Our electric grid is particularly vulnerable to growing cybersecurity threats as the grid is modernized, as distributed energy, electric vehicles, and modernized digital operating systems create more access points for cyber-attacks.

And while the nation's industrial control systems for the grid are analogue systems designed to last for decades, digital IT systems must constantly adapt to combat evolving cyber threats.

Small scale cyber and physical attacks to our electric grid are estimated to occur once every four days. And in over 300 cases of significant cyber and physical attacks since 2011, suspects have never been identified.

We often think of cybersecurity and other threats to the power grid at a macro scale, but these types of attacks can occur even at the local level. In 2011, the Pedernales Electric Co-op, a non-profit co-op that serves approximately 200,000 customers north of San Antonio, was struck by a cyberattack. While the attack thankfully did not disrupt power to consumers, it is a stark reminder that threats to the grid are real, and are not going away.

Our nation's power supply cannot be protected overnight, particularly as utilities struggle to adapt technology to manage a growing number of cybersecurity threats. Cyber threats to the power grid will continue to evolve, particularly as more interconnected smart technologies are incorporated into the electric grid.

And as protective technology improves, so does the capability and creativity of those conducting attacks.

While we cannot predict every method of attack, the federal government can and should play a role in assisting industry with developing new technology and security safeguards.

Accordingly, research and development efforts at the Department of Energy are focused on providing industry with comprehensive tools to conduct internal analysis to identify and address cybersecurity weaknesses so that industry can take the lead in addressing these vulnerabilities.

That's why testing facilities and cooperative research, like the Cyber Security Test Bed at Idaho National Lab, are valuable tools to combat cyber threats. At INL, industry can test control systems technology in real world conditions, reducing response time and risk for future attacks.

I want to thank our witnesses for testifying before the Committee today. I look forward to a discussion about cyber threats to our critical infrastructure, and how the federal government can provide industry with the tools and technology necessary to fight the next generation of cyber-attacks.

Chairman WEBER. I now recognize Ms. Bonamici.

Ms. BONAMICI. Thank you very much, Chairman Weber, for holding this hearing, and thank you to our witnesses for participating.

As many of you know, October is National Cyber Security Awareness Month, so it's a fitting time for this hearing today.

We're all familiar with the increasing frequency of cyber attacks that compromise personal and business information. At the World Economic Summit earlier this year, cyber threats made the top 10 list of the most likely global risks. Lloyd's of London estimates that cyber attacks can cost businesses as much as $400 billion a year.

What we're focusing on today is a different kind of cybersecurity. It's about securing the electric grid so that a cyber attack doesn't affect grid operations, which could halt our daily lives and threaten our economic security. These attacks often gain entry through an information technology system, but, instead of taking corporate data, they directly target system operations that can cause havoc and chaos.

In February of this year, an elite group of hackers broke through an electric utility's firewall and gained access to their substation controls in just 22 minutes. Luckily the attack was a drill initiated at the request of the utility to test their system. But this example demonstrates what's possible.

The energy sector continues to report more cyber attacks to the Department of Homeland Security, more than any other critical infrastructure sector. In just one month the PJM Interconnection, which coordinates electricity transactions in 13 states and in D.C., experienced 4,090 documented cyber attempts to attack their system. That's more than five and a half attacks on their electrical market system per hour.

So far, no publically reported cyber events have resulted in an electricity outage in the United States but the sophistication of attacks on industrial controls systems is increasing.

Utilities across our country are advancing energy efficiency through smart grids and programs like feed-in tariff systems. As we discuss ways to keep the grid safe, we also must be mindful of doing so without inhibiting innovation.

Google, Wells Fargo, and Aetna are exploring ways to leverage employee behavior as a tool, instead of a vulnerability, to build a more secure system. From understanding how people swipe their phones, to the patterns they use when typing on a keyboard or walking, a better understanding of behavioral biometrics is opening the door to developing more cyber-secure components and processes. The more we understand about human and social behavior, the stronger our toolbox. Rather than resting the success of our cybersecurity efforts on programs that require changes in human behavior, we might have better success if we change our technology and processes to fit the behavior of people. And the more we understand the behavior of threat actors, the better we can design protections.

So in addition to building a better technology-based firewall, we need to invest in developing a better human firewall. Our weakest link and our most resilient asset to meet the dynamic changing needs of the cyber arms race is us.

I thank each of our witnesses for being here today, and I look forward to hearing what each of you has to say, and thank you for sharing your expertise.

Thank you, Mr. Chairman. I yield back the remainder of my time.

[The prepared statement of Ms. Bonamici follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON ENVIRONMENT MINORITY RANKING MEMBER SUZANNE BONAMICI

Thank you, Chairman Weber and Chairwoman Comstock, for holding this hearing, and thank you to our witnesses for participating. As many of you know, October is National Cyber Security Awareness Month, so it's a fitting time for this hearing.

We are all familiar with the increasing frequency of cyber attacks that compromise personal and business information.

At the World Economic Summit earlier this year, cyber threats made the top 10 list of most likely global risks. Lloyd's of London estimates that cyber attacks can cost businesses as much as $400 billion a year.

What we are focusing on today, however, is a different kind of cyber security. It's about securing the electric grid so a cyber attack doesn't affect grid operations, which could halt our daily lives and threaten our economic security. These attacks often gain entry through an information technology system, but, instead of taking corporate data they directly target system operations that can cause havoc and chaos.

In February of this year, an elite group of hackers broke through an electric utility's firewall and gained access to their substation controls in 22 minutes. Luckily the attack was a drill initiated at the request of the utility to test their system. But this example demonstrates what's possible.

The energy sector continues to report more cyber attacks to the Department of Homeland Security than any other critical infrastructure sector. In just one month the PJM Interconnection, which coordinates electricity transactions in 13 states and DC, experienced 4,090 documented cyber attempts to attack their system. That's more than five and a half attacks on their electrical market system per hour.

So far no publically reported cyber events have resulted in an electricity outage in the U.S. But the sophistication of attacks on industrial controls systems is increasing.

Utilities across our country are advancing energy efficiency through smart grids and programs like feed-in tariff systems. As we discuss ways to keep the grid safe, we must be mindful of doing so without inhibiting innovation.

Google, Wells Fargo, and Aetna are exploring ways to leverage employee behavior as a tool, instead of a vulnerability, to build a more secure system. From understanding how people swipe their phones, to the patterns they use when typing on a keyboard or walking, a better understanding of behavioral biometrics is opening the door to developing more cyber-secure components and processes.

The more we understand about human and social behavior, the stronger our toolbox. Rather than resting the success of our cybersecurity efforts on programs that require changes in human behavior, we might have better success if we change our technology and processes to fit the behavior of people. And the more we understand the behavior of threat actors, the better we can design protections.

So in addition to building a better technology-based firewall, we need to invest in developing a better human firewall. Our weakest link and our most resilient asset to meet the dynamic changing needs of the cyber arms race is us.

I thank each of our witnesses for being here today, and I look forward to hearing what each of you has to say.

Thank you, Mr. Chairman, and I yield back my remaining time.

Chairman WEBER. I thank the gentlelady from Oregon.

Our first witness today is Mr. Brent Stacey, Associate Lab Director for National & Homeland Science and Technology at that Idaho National Laboratory. Mr. Stacey earned his bachelor's degree from Idaho State University.

Our next witness is Mr. Bennett Gaines, Senior Vice President of Corporate Services and Chief Information Officer for FirstEnergy Service Company. Mr. Gaines earned his bachelor's degree in social sciences from Baldwin Wallace College and his master's degree from the University of Phoenix.

Next, we have Ms. Annabelle Lee, Senior Technical Executive in the Power Delivery and Utilization Sector for the Electric Power Research Institute. Ms. Lee received her B.A. from Stanford University and her master's degree from Michigan State University.

And our final witness today is Mr. Greg Wilshusen—is it——

Mr. WILSHUSEN. Wilshusen.

Chairman WEBER. Wilshusen.

Mr. WILSHUSEN. Yes.

Chairman WEBER. Okay. So the rest of the Committee is duly notified. Wilshusen, Director of Information Security Issues for the Government Accountability Office. Mr. Wilshusen received his bachelor's degree in business administration from the University of Missouri and his master's degree in information management from George Washington University School of Engineering and Applied Sciences.

Welcome to all of you, and Mr. Stacey, you are recognized.

TESTIMONY OF MR. BRENT STACEY, ASSOCIATE LAB DIRECTOR FOR NATIONAL & HOMELAND SCIENCE AND TECHNOLOGY, IDAHO NATIONAL LAB

Mr. STACEY. Thank you, Chairmen Weber, Chairwoman Comstock, Ranking Member Grayson, Ranking Member Lipinski, and distinguished Members of the Committees. I want to thank you for holding this hearing and inviting testimony from Idaho National Laboratory, also known as INL.

INL is acutely aware of the important national challenges facing critical infrastructure, especially the infrastructure vital to securing our energy supply. For over a decade, INL has developed and built capabilities focused on the control systems employed by our nation's critical infrastructure. I'd like to highlight a few examples out of many which represent how INL teaming with others has contributed to the security of our infrastructure.

First, the 2006/2007 Department of Homeland Security's Aurora project test, destroying an electrical generator connected to INL's power grid, was significant in proving a cyber-physical vulnerability in the electric power system.

Second, for DOE Office of Electricity Distribution and Energy Reliability, as the lead laboratory along with Sandia National Laboratory for the National Supervisory Control and Data Acquisition Test Bed, INL completed more than 100 assessments on vendor and asset owner control systems to identify and resolve cyber vulnerabilities. For DHS, INL provides control systems and critical infrastructure experts in support of DHS programs including Industrial Control System Cyber Emergency Response Team, or ICS–CERT.

INL remains committed to the complex national security challenges that face our nation. As we lean forward pushing the limits of science and engineering for control systems security, we see a number of trends that offer insight into the direction for future research and development. These insights include, one, the presumption that a control system is air-gapped is not an effective cybersecurity strategy. This has been demonstrated by over 600 assessments. Intrusion detection technology is not well developed for control system networks. The average length of time for detection of a malware intrusion is 4 months and typically identified by a third party. As the complexity and interconnectedness of control systems increase, the probability increases for unintended system failures of high consequence independent of malicious intent. The dynamic threat is evolving faster than the cycle of measure and countermeasure, and far faster than the evolution of policy. And fifth, the demand for trained cyber defenders with control systems knowledge vastly exceeds the supply.

In a world in which we are rapidly migrating to the Internet of Everything, these insights, and others, highlight a seemingly unmanageable, exponentially increasing burden of vulnerabilities, attack surfaces and interdependencies.

INL views this burdensome and dynamic cyber-physical landscape, at its most basic level, as a three-tier pyramid of defense. The base level is hygiene: the foundation of our nation's efforts composed of the day-to-day measure and countermeasure battle. Elements of this level include important routine tasks such as standards compliance and patching. The hygiene level is and has been primarily the role of industry. The second level of the pyramid is advanced persistent threat composed of the more sophisticated criminal and nation-states' persistent campaigns. This requires a strategic partnership with industry and government. At this level, ICS–CERT provides critical surge response capacity and alerts. At the top of this pyramid are the high-impact low-frequency events: catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from. This level is primarily the responsibility of government.

At INL, we are focusing our future research on the top two levels, striving for a 2- to four-year research-to-deployment cycle. Our objective with this research is to achieve transformational innovations that improve the security of our power infrastructure by reducing complexity, implementing cyber-informed design, and integrating selected digital enhancements.

In conclusion, I'd like to thank the Committee members for this opportunity to share our insights into the capabilities, experiences, and vision for cybersecurity and the protection of our nation's power grid. Your interest in understanding cybersecurity threats with an emphasis on the reliability of our national power grid is commendable and gives me confidence that there is strong support from our legislators for research leading to innovative solutions.

One of my intentions today is to instill reciprocal confidence that INL, in concert with DOE and DOE laboratories, will continue to apply our intellectual talent and research to address these challenges.

In honoring the time allotted for my statement, I request that my full written statement be entered into the record. Thank you.

Chairman WEBER. Without objection, so ordered.

[The prepared statement of Mr. Stacey follows:]

STATEMENT OF
MR. BRENT J. STACEY, ASSOCIATE LABORATORY DIRECTOR
NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
SCIENCE SUBCOMMITTEE ON ENERGY
AND
SCIENCE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

OCTOBER 21, 2015

Written Testimony of Mr. Brent Stacey, Associate Laboratory Director
for National & Homeland Security – Idaho National Laboratory

Chairman Weber, Chairwoman Comstock, Ranking Member Grayson, Ranking Member Lipinski, and distinguished members of the Committees; I want to thank you for holding this hearing and inviting testimony from Idaho National Laboratory, also known as INL.

INL is acutely aware of the important national challenges facing critical infrastructure, especially the infrastructure vital to securing our energy supply. For over a decade, INL has developed and built capabilities focused on the control systems employed by our nation's critical infrastructure. This includes conducting research in the science and engineering of our electric power transmission and distribution systems. INL has the strong benefit of completing full-scale, real-world tests of technology solutions to validate and improve grid modeling and simulation.

I would like to highlight a few examples, out of many, which represent how INL has contributed to the security of our infrastructure:

1. The 2006 Department of Homeland Security's (DHS) Aurora project test, destroying an electrical generator connected to INL's power grid, was significant in proving a cyber-physical vulnerability in the electric power system.
2. For DOE Office of Electricity Distribution and Energy Reliability (DOE-OE): As the lead laboratory, along with Sandia National Laboratory, for the National Supervisory Control and Data Acquisition (SCADA) Test Bed, INL completed more than 100 assessments on vendor and asset owner control systems to identify and resolve cyber vulnerabilities.
3. For the Department of Defense: INL contributes research experimentation results and provides access to our full scale power grid test bed to characterize and improve models for understanding and mitigating the impacts of geomagnetic disturbance.
4. For DHS: INL provides control systems and critical infrastructure experts in support of DHS programs, including the Industrial Control System Cyber Emergency Response Team (ICS-CERT) Program and Regional Resilience Assessment Program (RRAP). This includes analysis of threat information, training of critical infrastructure owners and operators, assessing the security and resilience of infrastructure systems, and identification of infrastructure dependencies/interdependencies within a region.

INL has been and remains committed to the complex national security challenges that face our nation. As we lean forward pushing the limits of science and engineering for control systems security, we see a number of trends that offer insight into the direction for future research and development.

These insights include:

1) The presumption that a control system is "air-gapped" is not an effective cyber security strategy. This has been demonstrated by over 600 assessments.
2) Intrusion detection technology is not well developed for control system networks; the average length of time for detection of a malware intrusion is four months and typically identified by a third party.
3) As the complexity and "interconnectedness" of control systems increase, the probability increases for unintended system failures of high consequence - independent of malicious intent.
4) The dynamic threat is evolving faster than the cycle of measure and countermeasure, and far faster than the evolution of policy.
5) The demand for trained cyber defenders with control systems knowledge vastly exceeds the supply.

In a world in which we are rapidly migrating to the Internet of Everything, these insights, and others, highlight a seemingly unmanageable, exponentially increasing burden of vulnerabilities, attack surfaces and interdependencies.

INL views this burdensome and dynamic cyber-physical landscape, at its most basic level, as a three-tiered pyramid of defense. The base level is hygiene – the foundation of our nation's efforts, composed of the day-to-day measure and countermeasure battle. Elements of this level include important routine tasks such as standards compliance, patching, and password management. The hygiene level is and has been primarily the role of industry, with both vendors and asset owners participating. The second level of the pyramid is advanced persistent threat - composed of the more sophisticated criminal and nation state persistent campaigns. This level requires a strategic partnership with industry and government and, as such, it is important to note that these roles are still evolving. At this level, ICS-CERT provides critical surge response capacity and issues alerts of current vulnerabilities to the government and asset owners. At the top of this pyramid are the high impact low frequency events - catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from. This level is primarily the responsibility of the government. At INL, we are focusing our future research on the top two levels, striving for a two to four year research-to-deployment cycle. Our objective with this research is to achieve transformational innovations that improve the security of our power infrastructure by reducing complexity, implementing cyber-informed design, and integrating selected digital enhancements.

As the recognized leader in this field, it is our opinion that the risks and benefits of cyber exploitation of control systems require that the U.S. build and maintain a strategic, coordinated, technologically superior capability and capacity for control systems research, development, demonstration and deployment. To help catalyze the nation to meet this requirement, INL continues to invest in control systems innovation. Evidence of the high demand for this capability is demonstrated by the large variety of strategic partners – all agreeing that the nation has an immediate need for high performance research and response teams. Our focus is on experts, students, and trainees continuously mastering control systems cyber skills through learning, experimentation, operation, and competitive experiences. Of particular emphasis is the INL's focus on specialization in solutions based on cross functional teams (e.g. cyber, safety, operations, power, communications, etc.), 'out-of-band' innovations, and cyber-informed engineering designs. As an example, INL is pursuing a grand challenge to develop novel and deployable solutions to take a set of high value infrastructure assets off the table as targets. Using INL's significant power and communications infrastructure to analyze technology and infrastructure interdependencies, teams will explore the viability of: 1) insertion of analog attack surface disruption zones, such as custom analog circuits printed at low cost with 3D printer technology, inserted between the control network and the ultimate physical process system being targeted; and 2) pruning down unnecessarily complex systems to the bare minimum process requirements, thereby dramatically reducing the attack surface open to attackers.

In conclusion, I would like to thank the Committees' members for this opportunity to share our insight on the capabilities, experiences, and vision for cybersecurity and the protection of our nation's power grid. The dynamic evolution and technical complexity of the threats demand visionary, multifaceted science and leadership solutions. Your interest in understanding cybersecurity threats with an emphasis on the reliability of our national power grid is commendable and gives me confidence that there is strong support from our legislators for research leading to innovative solutions. One of my intentions today with this testimony is to instill reciprocal confidence that INL, in concert with DOE and other DOE laboratories, will continue to apply our intellectual talent and research to address these challenges. In honoring the time allotted for my statement, I request that my full written statement be entered into the record. Thank you.

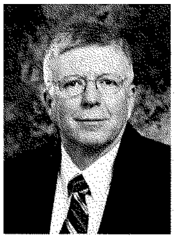
Written Testimony of Mr. Brent Stacey, Associate Laboratory Director
for National & Homeland Security – Idaho National Laboratory

SUMMARY

STATEMENT OF
MR. BRENT J. STACEY, ASSOCIATE LABORATORY DIRECTOR
NATIONAL & HOMELAND SECURITY
IDAHO NATIONAL LABORATORY
BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
SCIENCE SUBCOMMITTEE ON ENERGY
AND
SCIENCE SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

OCTOBER 21, 2015

As the recognized leader in this field, it is our opinion that the risks and benefits of cyber exploitation of control systems require that the U.S. build and maintain a strategic, coordinated, technologically superior capability and capacity for control systems research, development, demonstration and deployment. To help catalyze the nation to meet this requirement, INL continues to invest in control systems innovation. Evidence of the high demand for this capability is demonstrated by the large variety of strategic partners – all agreeing that the nation has an immediate need for high performance research and response teams. Our focus is on experts, students, and trainees continuously mastering control systems cyber skills through learning, experimentation, operation, and competitive experiences. Of particular emphasis is the INL's focus on specialization in solutions based on cross functional teams (e.g. cyber, safety, operations, power, communications, etc.), 'out-of-band' innovations, and cyber-informed engineering designs. As an example, INL is pursuing a grand challenge to develop novel and deployable solutions to take a set of high value infrastructure assets off the table as targets. Using INL's significant power and communications infrastructure to analyze technology and infrastructure interdependencies, teams will explore the viability of: 1) insertion of analog attack surface disruption zones, such as custom analog circuits printed at low cost with 3D printer technology, inserted between the control network and the ultimate physical process system being targeted; and 2) pruning down unnecessarily complex systems to the bare minimum process requirements, thereby dramatically reducing the attack surface open to attackers.



Brief Biography

Brent J. Stacey

Associate Laboratory Director
National & Homeland Security
Idaho National Laboratory

Contact Information

Idaho National Laboratory
P. O. Box 1625-MS 3750
Idaho Falls, ID 83415
(208) 526-7011
Brent.Stacey@inl.gov

Brent is responsible for Idaho National Laboratory's (INL) National and Homeland Security (N&HS) mission. INL's N&HS is a major center for national security technology development and demonstration, employing 500 scientists and engineers across $300M in programs. He is responsible for INL's Nuclear Nonproliferation, Critical Infrastructure Protection and Defense Systems missions. These missions include heavy manufacturing of armor, application of INL's unique infrastructure (grid, wireless testbed, explosives range, and a number of research facilities). These missions also support major programs for Department of Defense, Department of Homeland Security, and the Intelligence Community. Previously, Brent served as INL's Chief Information Officer leading an information management, classified and unclassified cyber security, high-performance/scientific computing transformation, and INL's records management and library. Brent also served as INL's director of Technology Deployment, fundamentally transforming INL's technology deployment and commercialization. Brent served a key role in INL's campus expansion through state-of-the-art infrastructure in new buildings and utility corridors.

Brent has over 30 years of experience in information technology and cyber security in electric utility and related government markets.

He has served as CEO, president, vice-president, and CIO for small- to mid-sized domestic and international companies.

Just prior to joining the INL as part of the new Battelle contract, Brent served as CIO for Argonne National Laboratory for three years.

Brent was recognized as Idaho's *Information Technology Executive of the Year* in 2002 for his leadership. He was a founder of SRV.net, one of the first Internet service providers in the Pacific Northwest, and was the first president and chief executive officer of the Idaho Regional Optical Network, a nonprofit organization chartered to advance science, research, education, health care and state government through access to very high-speed and cost-effective bandwidth. Brent was recently inducted into the CIO Hall of Fame and recognized as a Premier 100 IT leader in 2012.

Chairman WEBER. Mr. Gaines, you're up.

TESTIMONY OF MR. BENNETT GAINES, SENIOR VICE PRESIDENT, CORPORATE SERVICES AND CHIEF INFORMATION OFFICER, FIRSTENERGY SERVICE COMPANY

Mr. GAINES. Good morning, Chairman Weber and Members of the Committee. I am Bennett Gaines, Senior Vice President, Corporate Services, Chief Information Officer for FirstEnergy. Our 10 operating companies serve 6 million electrical customers in six states, and we control an interconnected network of power plants, transmission lines and distribution facilities. I am responsible for providing information technology services, ensuring the security of the company's physical and cyber assets.

Over the past few years, FirstEnergy has worked with the Department of Homeland Security, the Department of Energy, and Congress, sharing steps we are taking to address cyber threats as well as developing partnerships with the federal government in these efforts.

In 2013, FirstEnergy was one of only a handful of utilities that entered into a cooperative research and development agreement, or CRADA, with Homeland Security, a relationship that has proven valuable to both us and the federal government. In 2014, we began working directly with the Department of Energy as one of the first utilities to deploy the Cybersecurity Risk Information Sharing Program, or CRISP, tool. We strongly believe that sharing this information of critical information is essential and should be actively supported moving forward. The fact is, although the cybersecurity efforts of electric utilities have been effective in addressing threats to date, we need to continually strengthen and build on these efforts to ensure they are up to the task of meeting the future cyber-related challenges.

Operational and technical advances have created roader surfaces that are more vulnerable to attacks. Companies continue to integrate remote access, mobile devices that increase exposure. High-value targets such as Supervisory Controlled Data, Acquisition, or SCADA systems, further entice attackers to take advantage of an organization.

Cyber attacks are on the rise, and the behavior of cyberterrorists has become increasingly destructive. Many companies are doing an excellent job with prevention through layer defense, real-time alerting, operational monitoring, security awareness training, and other proven tactics. However, in light of today's threats and vulnerabilities, we need to focus more of our attention on getting ahead of the threats rather than simply reacting to the threats.

Toward that end, we need to take aggressive steps to mitigate vulnerabilities and minimize the damage and business losses that could result from potential compromises.

At FirstEnergy, we're evaluating cyber threats to our communications network by integrating more traditional data regarding physical access systems and the status of equipment and health and on our power systems. This process, called Threat Intelligence

Management, or TIM, provides a more comprehensive system-wide consistent picture that our Security Operations Center can use to improve our response to cyber attacks. While any information can be shared, it also must be aggregated, correlated, analyzed and distilled to be relevant and actionable. By supporting these essential functions, TIM helps us maintain a critical infrastructure that is both highly secure and resilient. The program analyzes a constant flow of information from every corner of the system to anticipate and detect threats. This data can be shared among government and industry partners to enhance awareness of threats and provide more warning information to better mitigate attacks.

Simply put, TIM offers a better platform for information sharing. The program not only helps us better identify and analyze threats and attacks, it also supports more effective information sharing and great collaboration among all stakeholders. This results in more threat indicators, improved security, greater resilience of critical infrastructure, and ultimately more effective collaboration between industry and government.

Finally, the TIM program provides enhanced visibility of the enterprise overall security posture. This is accomplished by coordinating the monitoring of cybersecurity, physical security, information technology, and operational technologies. Advanced analysis of these functions provide early warning of security incidents and rapid mitigation of vulnerabilities.

In closing, we must continually improve our cybersecurity systems and processes to stay ahead of the bad actors. To give you a greater sense of the size and scope of the problem, I simply point out that during my brief time here today, FirstEnergy probably has defended itself from at least four cyber attacks.

As you consider where to focus our efforts moving forward, I urge you to look towards greater research and funding in this area with a focus on aggregating, correlating, analyzing and distilling information in order to be relevant and actionable. I strongly believe that one of the best ways to achieve this goal is through an effective threat intelligence management program.

Thank you very much for the time.

[The prepared statement of Mr. Gaines follows:]

Written Testimony

Bennett L. Gaines
Senior Vice President, Corporate Services, and Chief Information Officer
FirstEnergy

Before the
Joint Subcommittees on Energy & Research and Technology
Committee on Science, Space, and Technology

United States House of Representatives

On

Cybersecurity for Power Systems

October 21, 2015

Summary

Information-sharing between the electric industry and the federal government is essential to maintaining a strong, effective and proactive approach to protecting our nation's vital communications networks from potential cyber-attacks.

Cyber-attacks to the electric sector are becoming more sophisticated and are constantly evolving as defensive security measures become increasingly predictable. According to *Under Cyber Attack – Ernst & Young's Global Information Security Survey, 2013*, 59 percent of respondents saw an increase in external threats in the previous 12 months. Despite a target's firewall, antivirus protection, email and passwords, determined and malicious actors will stop at nothing to compromise or attack an organization's cyber assets. It has been said that compromising a system is not a question of *if*, but *when*. Moreover, sophisticated cyber-attacks can evade detection, potentially for weeks or even months at a time.

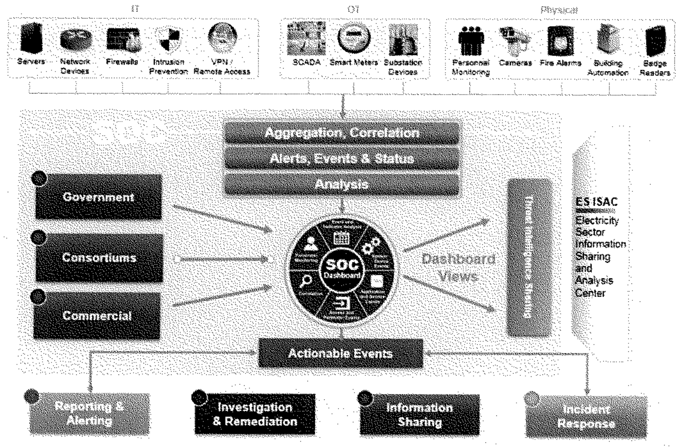
With every operational and technical advance that is made to improve productivity – including remote access, mobility and "bring your own device" policies – organizations also are broadening their attack surface and exposure. Additionally, electric utilities operate a complex, interconnected network of power plants, transmission lines and distribution facilities, and their management is distributed across each enterprise. High-value targets – such as Supervisory Control and Data Acquisition (SCADA) systems – further entice attackers to take advantage of an organization.

In response, many organizations are doing an excellent job with prevention through layered defenses, real-time alerting, operational monitoring and security awareness training and other proven tactics. In light of today's threats and vulnerabilities, however, we need to focus more of our attention on anticipating attacks rather than reacting to them. Leading organizations are expanding their efforts – and taking bolder steps – to combat cyber threats. Rather than waiting for the threats to come to them, they are prioritizing efforts that enhance visibility and enable a proactive response through monitoring and prompt detection.

Organizations may not be able to control when information security incidents occur, but they can control how they respond. The best way to reduce the adverse impact of an attack is to identify it and intervene as quickly as possible. To do this, we must increase our awareness of indicators, detect threats, and respond to incidents quickly and efficiently. We have an abundance of data to achieve this goal; however, this information often is acquired using diverse tools, stored in disconnected and isolated systems, and monitored by unrelated groups.

Solution

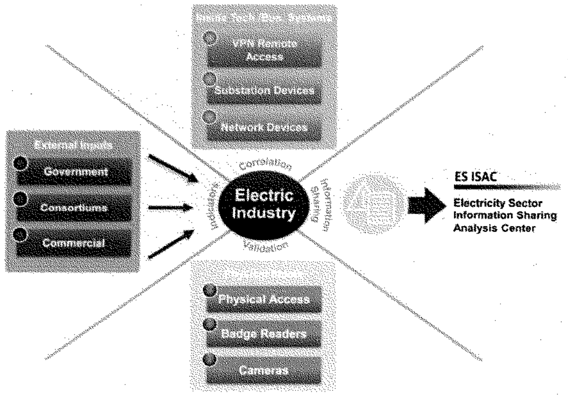
To combat cybersecurity attacks, a Threat Intelligence Management (TIM) program provides enhanced visibility of the enterprise's overall security plan by monitoring cybersecurity, physical security, information technology and operations technology. Advanced analysis of these functions is performed to provide an early-warning system for security incidents and rapid mitigation of vulnerabilities.



Analysis of the correlated data is conducted by security teams that augment real-time information from the Security Information and Event Management (SIEM) system and related tools. Teams develop requirements and identify indicators while designing the logic for additional use cases (a methodology used in system analysis to identify, clarify, and organize system requirements) to identify trends and emerging threats. The output is validated to ensure the use cases accurately identified threats and to determine the overall security posture of the organization, and this information can be shared with internal business units and external partners. It also could be shared with the federal government or sector-specific, information-sharing organizations as part of an overall threat intelligence collaborative. The benefits of this collaborative would include: identifying and communicating previously undetected Advanced Persistent Threats (APT); communicating precursors of upcoming attacks; providing indications of zero-day vulnerabilities (a gap in the software that is unknown to the vendor and exploited by a hacker); and developing and sharing mitigation strategies, use cases, firewalls and Intrusion Prevention System (IPS) rulesets.

Framework

As a practical matter, organizations can achieve the benefits of a TIM program by integrating global intelligence into their established security technologies and practices, and including these elements:



Planning: Organizations must decide the amount of protection they need to apply to their information assets on a granular level, department by department. This enables them to prioritize intelligence requirements, establish a strategic blueprint for protection, and outline intelligence workflows with both internal and external roles and responsibilities.

Collection: Typically, spending on internal intelligence collection and intrusion detection solutions is already significant. Augmenting it with external global intelligence networks and third-party data feeds such as botnets, Darknet, and peer-to-peer alternatives extends protection to cover emerging threats and preserves the value of legacy security investments. The intelligence infrastructure often includes a console or portal to make collected information available inside the organization.

Analysis: Intelligence analysis includes integration across multiple information sources, correlation to identify potential threats, and evaluation to determine the degree of risk each threat represents. This culminates in the identification of root causes and bad actors, with recommendations for defenses or countermeasures.

Dissemination: Dissemination typically involves cooperation among organizations and their external intelligence partners and includes early warning communications, customized action reports, and personal contact between internal security specialists and external intelligence analysts.

Adaptation and Enhancement: "Closing the loop" also is a shared responsibility in which intelligence partners develop event metrics and use cases to identify protection, detection, infrastructure and analysis.

A new generation of security data-mining tools uses innovative techniques to collect and analyze massive amounts of information: data from PCs, mobile devices and servers; data from internal networks, including the composition and content of network packets; and threat intelligence about attacks on other organizations and the tools and methods used. In addition to analyzing these traditional information sources, big data security tools also can obtain information from non-traditional sources such as building key card scanners, personnel records and even Microsoft Outlook calendars. This data may be used, for instance, to assess the legitimacy of remote log-ins by employees.

The heightened visibility provided by the big data capabilities of new security analytics platforms creates unprecedented opportunities to identify anomalies, uncover evidence of hidden threats or even predict specific, imminent attacks. More data creates a richer, more granular view as it presents the threat landscape in high definition. Security-related details can be seen in sharper focus, and irregularities can be found faster.

Security Indicators

Information from external sources, including governments, consortiums and commercial providers, is critical to threat intelligence. Established sources used today include Cyber Information Sharing and Collaboration Program (CISCP), which is a threat-awareness cooperative between the Department of Homeland Security (DHS), the United States Computer Emergency Readiness Team (US-CERT), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Private organizations include the Electricity Information Sharing and Analysis Center (E-ISAC), which represents the electric sector; commercial services that inform customers of vulnerabilities and patches via alerts; and most recently, CRISP, the cybersecurity risk information sharing program that uses automated sensors to detect malicious activity attempting to compromise networks.

Data from these sources is important to overall cybersecurity, as it provides additional alarms and events that the organization is experiencing now. Knowledge gained from other organizations witnessing these attacks and events enables them to quickly identify when such events occur on their system.

Department of Energy, Cybersecurity Risk Information Sharing Program (CRISP)

CRISP is a public-private partnership that permits the sharing of cyber threat information and production of situational awareness tools to identify, prioritize and coordinate the protection of the electrical sector's critical infrastructure. CRISP enables critical infrastructure owners and operators to voluntarily share, in near real-time, cyber threat data and analysis and receive mitigation measures from other participants.

CRISP began as a partnership between the Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE/OE), the North American Electric Reliability Corporation (NERC) Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Pacific Northwest National Laboratory (PNNL), Argonne National Laboratory (ANL), and participating companies. FirstEnergy is a participant, and more companies are being added.

Department of Homeland Security Enhanced Cybersecurity Services (ECS)

As the federal government's lead agency for coordinating the protection, prevention, mitigation and recovery from cyber incidents, DHS works with business owners and operators to strengthen their facilities and communities. To accomplish this, the DHS Enhanced Cybersecurity Services (ECS) program was expanded in February 2013 by Executive Order (Improving Critical Infrastructure Cybersecurity).

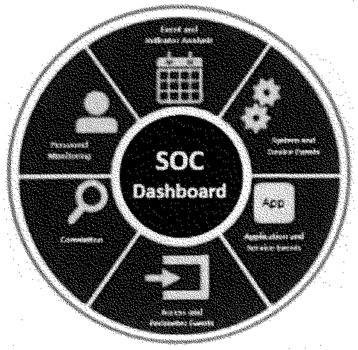
ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops indicators based on this information and shares them with qualified Commercial Service Providers (CSP), enabling them to better protect their customers who are critical infrastructure entities. ECS augments, but does not replace, existing cybersecurity capabilities.

North American Electric Reliability Corporation (NERC)

NERC was founded in 1968 by representatives of the electric utility industry for the purpose of developing and promoting voluntary compliance with rules and protocols for the reliable operation of the bulk power electric transmission systems of North America. NERC's mission is to improve the reliability and security of the bulk power system in the United States, Canada and part of Mexico. The organization aims to accomplish this not only by enforcing compliance with mandatory reliability standards, but also by acting as a catalyst for positive change – including shedding light on system weaknesses, helping industry participants operate and plan to the highest possible level, and communicating lessons learned throughout the industry.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The ICS-CERT partners with members of the control systems community to help develop and vet recommended practices, provide guidance in support of ICS-CERT incident response capability, and participate in leadership working groups to ensure the community's cyber security concerns are considered in our products and deliverables. The ICS-CERT facilitates discussions between the federal government and the control systems vendor community, establishing relationships that foster a collaborative environment in which to address common control systems cyber security issues. The ICS-CERT also is developing a suite of tools that will provide asset owners and operators with the ability to measure the security posture of their control systems environments and to identify the appropriate cyber security mitigation measures they should implement.



Security Operations Center

The Security Operations Center (SOC) is a concentrated set of sophisticated technologies and processes that provide enhanced visibility, correlation, real-time analysis and incident awareness of security events in the electric sector. The goal of the SOC is to provide a single pane of information spanning IT, OT, Physical and Cyber security. The SOC monitors and handles investigations with high efficiency and greater effectiveness than previously experienced in most organizations.

Building a well-informed Threat Intelligence Management program will result in more threat indicators, improved security, greater critical infrastructure resilience, and ultimately more industry and government collaboration. These efforts also support one of our nation's highest priorities: Presidential Policy Directive 21 identifies "critical infrastructure security and resilience" as the shared responsibility of "Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure."

Further, in Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity"), the Obama Administration emphasized the need for robust information-sharing among all critical infrastructure stakeholders. The Threat Information Management program brings us to the closest point to not only our own identification and analysis of threats and attacks, but also to a more functional and effective information-sharing process – and the knowledge-sharing output of this process will help foster greater collaboration among all stakeholders.

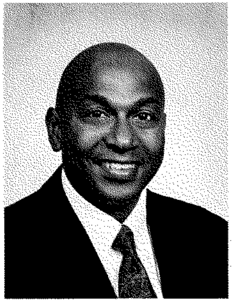
Finally, while any information can be shared, it must be aggregated, correlated, analyzed and distilled to be relevant and actionable. The goal is to ensure a secure critical infrastructure that is as resilient as it is protected from threats and attacks.

Bibliography:

- Under Cyber Attack: EY's Global Information Security Survey, 2013
- EMC – Storage Report, 2013
- Cybersecurity Risk Information Sharing Program (CRISP)
- Department of Homeland Security – Enhanced Cybersecurity Services (ECS)
- North American Electric Reliability Corporation (NERC)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Department of Homeland Security – CRADA - Cyber Information Sharing Collaboration Program (CISCP)
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
- Presidential Policy Directive 21
- Executive Order 13636 "Improving Critical Infrastructure Cybersecurity"

FirstEnergy®

76 South Main St.
Akron, OH 44308
www.firstenergycorp.com



Bennett L. Gaines

Senior Vice President, Corporate Services and
Chief Information Officer

Bennett L. Gaines is senior vice president, Corporate Services, and chief information officer for FirstEnergy Service Company, a subsidiary of FirstEnergy Corp. Gaines is responsible for the delivery of Information Technology (IT) services, including FirstEnergy's corporate IT strategy and governance process, as well as the company's communications and data network. He also is responsible for Corporate Security (physical and cyber), Flight Operations and Supply Chain. He was appointed to his current position in July 2012.

Gaines joined FirstEnergy in 2006 as vice president, Information Technology/Corporate Security and chief information officer. Earlier in his career, he was vice president and chief information officer at Cincinnati-based Cinergy Corp., where he was responsible for the delivery of IT services and telecommunications and network operations.

Before joining Cinergy in 2003, Gaines was managing director, Business Services, at Powergen plc in the United Kingdom. He was responsible for the strategy and delivery of IT and other shared services and managed IT activities. Prior to this position, he was corporate director, Supply Chain, for LG&E Energy Corp., a subsidiary of Powergen, based in Louisville, Ky. From 1998 to 2000, he was employed by EDS Corp. in Dallas, Texas.

Gaines earned a Bachelor of Arts degree from Baldwin-Wallace College and a Master of Arts degree from the University of Phoenix.

Chairman WEBER. Thank you, Mr. Gaines.

Ms. Lee, you're now recognized.

STATEMENT OF MS. ANNABELLE LEE, SENIOR TECHNICAL EXECUTIVE IN THE POWER DELIVERY AND UTILIZATION SECTOR, ELECTRIC POWER RESEARCH INSTITUTE

Ms. LEE. Good morning, Chairmen and Members of the Subcommittees.

The Electric Power Research Institute is an independent, nonprofit organization and conducts research and development relating to the generation, delivery, and use of electricity for the benefit of the public.

The nation's power system consists of both legacy and next-generation technologies. New grid technologies will operate in conjunction with legacy equipment that may be several decades old and provide new security controls.

Traditional information technology—IT—devices typically have a lifespan of 3 to five years, and historically, IT has included computer systems, applications, communications technology and software typical for a business or enterprise. In contrast, operational technology, or OT, devices, have a lifespan of up to 40 years or longer and have historically focused on physical equipment technology that is commonly used to operate the energy sector.

There's some basic differences between the security requirements for IT and OT systems. For example, the focus for IT systems is confidentiality of information such as customer energy usage and privacy information. The focus for OT systems is availability and integrity to ensure that the reliability of the grid is maintained even in the event of a cybersecurity incident.

With the increase in the use of digital devices and more advanced communications and IT, the overall attack surface has increased. These new devices include commercially available components as an alternative to proprietary solutions that are specific to the electric sector. Many of the commercially available solutions have known vulnerabilities that could be exploited when the solutions are installed in OT devices.

The electric sector is addressing these attacks with various mitigation strategies. Cybersecurity must be included in all phases of the system development lifecycle and address deliberate attacks launched by disgruntled employees and nation-states as well as non-malicious cybersecurity events, for example, user errors or incorrect documentation.

Risk assessment is a key planning tool for implementation of an effective cybersecurity program. EPRI, in conjunction with utilities, researchers, and vendors, developed a risk assessment methodology that is based on a typical IT methodology with impact and likelihood criteria that are specific to the electric sector. This work was performed as part of the National Electric Sector Cybersecurity Organization Resource, or NESCOR for short, project, DOE funded public-private partnership. Several utilities are implementing mitigation strategies at the enterprise level. One example is an Integrated Security Operations Center, or ISOC for short. An ISOC is designed to collect, integrate and analyze alarms and logs from traditionally siloed organizations, providing much greater situational awareness to the utility's security team.

Two documents specifically address the electric sector and provide mitigation strategies. Both documents are used worldwide. The first is the National Institute of Standards and Technology Interagency Report Guidelines for Smart Grid Cyber Security. The development was led by NIST with a team of roughly 150 volunteers. A second document is the Electricity Subsector Cybersecurity Capability Maturity Model, which allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity. Many utilities and EPRI map their R&D programs to the domain specified in this maturity model.

With the modernization of the electric grid, new technologies and devices have been deployed to meet our current and future electric sector needs. With this new functionality comes new threats including cybersecurity threats. To take advantage of the new technology, these threats must be addressed.

This concludes my statement.

[The prepared statement of Ms. Lee follows:]

Written Testimony

Hearing of the House Science, Space and Technology Committee
Subcommittees on Energy and Research & Technology

United States House of Representatives

Ms. Annabelle Lee
Senior Technical Executive – Cyber Security
Electric Power Research Institute

"Cybersecurity for Power Systems"

October 21, 2015

The Electric Power Research Institute (EPRI) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, non-profit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety, and the environment. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the U.S., and international participation extends to more than 30 countries.

Background

The nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, intelligent components to the electric grid that communicate in much more advanced ways (e.g., two-way communications and wired and wireless communications) than in the past. These new components will operate in conjunction with legacy equipment that may be several decades old, and provide no cyber security controls. Traditional information technology (IT) devices typically have a life span of three to five years. In contrast, operational technology (OT) devices have a life span of up to 40 years or longer. With the constantly changing IT and threat environments, addressing potential cyber security events is a challenge.

With the increase in the use of digital devices and more advanced communications and IT, the overall attack surface has increased. For example, substations are modernized with new equipment that is digital, rather than analog. These new devices include commercially-available operating systems, protocols, and applications as an alternative to proprietary solutions that are specific to the electric sector. Many of the commercially-available solutions have known vulnerabilities that could be exploited when the solutions are installed in OT system components. Potential impacts from a cyber event include: billing errors, brownouts/blackouts, personal injury or loss of life, operational strain during a disaster recovery situation, or physical damage to power equipment.

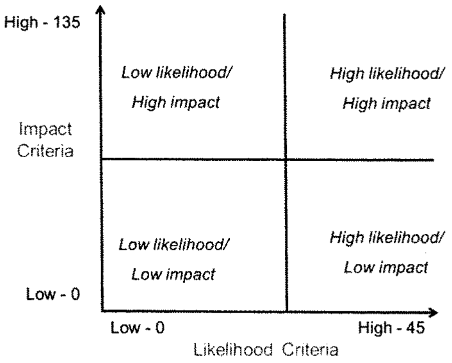
Another change is the convergence of IT and OT. Historically IT has included computer systems, applications, communications technology and software to store, retrieve, transmit and process data typically for a business or enterprise. OT has historically focused on physical equipment-oriented technology that is commonly used to operate the energy sector. Currently, multiple groups and operators often independently gather and analyze information from isolated and "stove-piped" systems that have been developed to provide security monitoring for physical, enterprise, and control system environments. As the threat landscape has evolved, there is a greater need to have a coordinated view of all aspects of an organization's security posture (i.e., situational awareness) and events (both unintentional, such as a component failure; and malicious) that may impact an organization's security posture, and responses to those events.

Risk Management

Cyber security is a priority for critical infrastructures, especially electric utilities. To adequately address cyber security risks, utilities need to understand that there are some basic differences between the security requirements for IT systems and the security requirements for OT systems. In general, the focus for IT systems is confidentiality of information; for example, customer energy usage and privacy information. The focus for OT systems is availability and integrity, to ensure that the reliability of the grid is maintained even in the event of a cyber security incident. OT systems also have performance requirements and any significant delay in sending and/or receiving data and commands could adversely impact the reliability of the grid. Some typical IT security controls such as cryptography and vulnerability scanning that have been implemented in OT systems could cause systems to fail. Because of these differences, utilities need to ensure that implemented security controls do not adversely impact the reliability of the grid.

To adequately address potential threat agents and vulnerabilities, cyber security must be included in all phases of the system development life cycle - from the design phase through implementation, operations and maintenance, and sunset. Cyber security must address deliberate attacks launched by disgruntled employees and nation-states as well as non-malicious cyber security events (e.g., user errors, incorrect documentation, etc.). Currently, the majority of cyber security events are non-malicious. Because organizations, including utilities, do not have unlimited resources, including personnel and funds, cyber security must be prioritized with the other components of enterprise risk. *Risk* is the potential for an unwanted impact resulting from an event. Enterprise risk addresses many types of risk such as investment, budgetary, program management, legal liability, safety, and inventory risk, in addition to cyber security. A cyber security risk management strategy should be a component within an organization's enterprise risk management strategy.

One phase within risk management is risk assessment. Risk assessment is a key planning tool for implementation of an effective cyber security program and involves identifying threats, vulnerabilities, and the potential impact and risk associated with the exploitation of those vulnerabilities. Risk assessments are performed on systems. Once the risk is determined, the organization needs to determine a course of action. This could be accept, avoid, mitigate, share, or transfer the risk. Risk assessments are not one-time activities. Rather, organizations should perform risk assessments on an ongoing basis throughout the system life cycle. The two criteria used in a risk assessment are impact and likelihood. EPRI, in conjunction with utilities, academia, researchers, and vendors developed a risk assessment methodology that is based on a typical IT methodology with impact and likelihood criteria that are specific to the electric sector. This work was performed as part of the National Electric Sector Cybersecurity Organization Resource (NESCOR) project – a DOE funded public-private partnership. Some of the NESCOR impact criteria include: system scale, safety concern, ecological concern, restoration costs, negative impact on generation capacity, and negative impact on the bulk transmission system. Some of the NESCOR likelihood criteria include: skill required, accessibility (physical), accessibility (logical), and attack vector. A score of 0, 1, 3, or 9 is determined for each criterion then a sum is calculated for impact and likelihood. The resulting score can be displayed on a graph, as shown below. The systems that fall in the upper right quadrant, high likelihood/high impact, are the highest priority for the organization as are the mitigation strategies for these systems.


High - 135
Impact Criteria
Low - 0
Low likelihood/ High impact
High likelihood/ High impact
Low likelihood/ Low impact
High likelihood/ Low impact
Low - 0
High - 45
Likelihood Criteria

Mitigation Strategies

Utilities, government agencies, academia, research organizations, and vendors are collaborating on many projects to develop tools and techniques to address cyber security threats and vulnerabilities. This collaboration is important to ensure that the unique cyber security requirements of the electric sector are addressed. Summarized below are several applicable cyber security research efforts.

To address current and emerging cyber security threats and vulnerabilities, several utilities are implementing mitigation strategies at the enterprise level. One example is an Integrated Security Operations Center (ISOC) that includes corporate systems, control systems, and physical security. Currently, multiple groups and operators independently gather and analyze information from datacenters, substations, networks, physical security and field equipment. Data is also collected and analyzed from external sources. Correlating this data to find suspicious activity can be extremely challenging and often only occurs long after an incident happens.

An ISOC is designed to collect, integrate, and analyze alarms and logs from these traditionally *siloed* organizations, providing much greater situational awareness to the utility's security team. Additionally, an ISOC allows utilities to transition to an intelligence-driven approach to incident management, which is much more effective for handling advanced threats.

Several requirements documents that specifically address the electric sector provide mitigation strategies. Two of these documents are highlighted below.

- The first document is the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, initially published in 2010. The development was led by NIST with a team of volunteers from the private sector, academia, research organizations, and government. Roughly 150 individuals volunteered their time to author this document. This is the first document that focused on the electric sector and it has been distributed and used worldwide.

- A second document is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity. The maturity model was developed as part of a White House initiative led by DOE in partnership with the Department of Homeland Security (DHS) and involved close collaboration with industry, other Federal agencies, and other stakeholders. This document is also used worldwide.

DOE has been the designated Sector Specific Agency (SSA) for the energy sector since 2003 and research and development (R&D) has been identified in the Sector Specific Plan (SSP) as a key source of innovation and productivity for the Energy Sector. Since more than 80 percent of the country's energy infrastructure is owned by the private sector, DOE has initiated several collaborative research efforts. Two are highlighted below:

- A key mission of DOE's Office of Electricity Delivery and Energy Reliability (OE) is to enhance the reliability and resilience of the nation's energy infrastructure. Cybersecurity of energy delivery systems is critical for protecting the energy infrastructure and the integral function that it serves in our lives. OE designed the Cybersecurity for Energy Delivery Systems (CEDS) program to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.

- DOE published a *Roadmap to Achieve Energy Delivery Systems Cybersecurity* in 2011 that provides a plan to improve the cybersecurity of the energy sector. The strategic framework within presents the vision of industry, vendors, academia, and government stakeholders for energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next decade. The vision within the roadmap states: *By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.* The roadmap is an update to the 2006 *Roadmap to Secure Control Systems in the Energy Sector.* The 2011 roadmap addresses gaps created by the changing energy sector landscape and advancing threat capabilities, and to emphasize a culture of security.

Many utilities and EPRI map their R&D programs to the strategies defined in the *Roadmap* and to the domains specified in the ES-C2M2. These common categories are used by utilities, academia, and research organizations in the public and private sectors as they define and prioritize their research agendas. This is particularly important with the constantly changing threat environment.

Another NESCOR project focused on the development of *failure scenarios* for the electric sector. A *cyber security failure scenario* is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Each scenario includes a title, short description, relevant vulnerabilities, impact, and potential mitigations. Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality,
- Failures due to data integrity attacks,
- Communications failures,

- Human error,
- Interference with the equipment lifecycle, and
- Natural disasters that impact cyber security posture.

Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence.

Included below is a sample failure scenario.

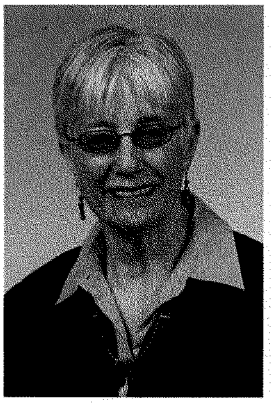
> **AMI.26 Advanced Metering Infrastructure (AMI) Prepaid Billing Cards are Compromised Resulting in Loss of Revenue**
>
> **Description:** The prepaid billing cards for AMI are compromised. Example compromises include tampering with cards to change the credit amount, erasing the logic that decrements the credit amount remaining, or forging cards.
>
> **Relevant Vulnerabilities:**
>
> - *System assumes data inputs and resulting calculations are accurate* on prepaid billing cards inserted into a meter,
> - *System permits unauthorized changes* to AMI billing information on prepaid billing cards.
>
> **Impact:**
>
> - Loss of revenue.
>
> **Potential Mitigations:**
>
> - *Design for security* in the payment system,
> - *Check software file integrity* (digital signatures or keyed hashes) on the prepaid billing card contents,
> - *Authenticate data source* i.e., prepaid billing cards for AMI billing,
> - *Perform security testing* as a part of system acceptance testing.

For utilities that do not have readily available cyber security staff, the failure scenarios may be used as part of the overall risk management process to begin addressing potential cyber security events. For all utilities, the failure scenarios may be used to train new personnel and for refresher training for all staff. Finally, the failure scenarios may be used as input to tabletop exercises. Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular situation. Many tabletop exercises can be conducted in a few hours.

The NESCOR failure scenarios have been used by researchers and utilities around the world.

Conclusion

With the modernization of the electric grid, new technologies and devices have been deployed to meet our current and future electric sector needs. These new intelligent components communicate in more advanced ways (e.g., two-way communication and wired and wireless communications) than in the past. Cyber security is important because the bi-directional flow of two-way communication and the control capabilities in the modernized grid enable an array of new functionalities and applications. With this new functionality comes new threats, including cyber security threats. To take advantage of the new technology, these threats must be addressed. Identified above are several mitigation strategies that may be used to address current and future cyber security threats and vulnerabilities. Some of these mitigation strategies will be implemented in the new advanced technology.



Annabelle Lee
Senior Technical Executive – Cyber Security
Power Delivery and Utilization

Annabelle is a Senior Technical Executive in the Power Delivery and Utilization Sector of EPRI. She is the program manager for two DOE projects and is the lead for the Information Assurance project set at EPRI, focusing on security risk management, metrics, and architectures. She also has expertise in applied cryptography. Annabelle's experience comprises 40 years of technical experience in IT system design and implementation and over 25 years of cyber security specification development and testing. Over her career she has authored or co-authored many documents on cyber security, cryptography, and testing. She began her career in private industry concentrating on IT systems specification, software testing and quality assurance.

From 1996 to 2010, Annabelle was a Senior Cyber Security Strategist at the National Institute of Standards and Technology (NIST). She led the Smart Grid Cyber Security Working Group (CSWG) at NIST. Annabelle established the CSWG, defined the work program, and defined the cyber security and privacy strategies for the Smart Grid. The CSWG published the NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security* in September 2010. The NISTIR is used worldwide.

Annabelle was detailed to the Department of Homeland Security (DHS) for four years. At DHS, Annabelle was the Director, Standards, Best Practices, and R&D Requirements Program and the Director of the Supply Chain Risk Management (SCRM) Program within the DHS National Cyber Security Division. At NIST, Annabelle was the Director of the Cryptographic Module Validation Program (CMVP). Annabelle was the technical lead for the development of Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules.*

From 1984 to 1996, Annabelle was a Lead Engineer in the Criminal Justice and Public Safety Division of the MITRE Corporation. She provided support to the FBI Criminal Justice Information Services (CJIS) Division. She was the task leader responsible for defining, specifying, and monitoring the implementation of the information security program for the CJIS systems. This included the National Crime Information Center 2000 and the Integrated Automated Fingerprint Identification System.

Prior to this, Annabelle worked in the private sector concentrating on IT systems specification, implementation, and testing. Annabelle has a BA from Stanford University and an MA from Michigan State University.

Chairman WEBER. Thank you, Ms. Lee.

Mr. Wilshusen, you are recognized for five minutes.

STATEMENT OF MR. GREG WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Weber, Representative Bonamici, and other Members of the Subcommittees, thank you for the opportunity to testify at today's hearing on efforts by federal agencies and industry to mitigate cybersecurity threats to the U.S. power systems.

As you know, the electric power industry is increasingly incorporating information and communications technologies into its existing infrastructure. The use of these technologies can provide many benefits such as greater efficiency and lower cost to consumers. However, if not implemented securely, modernized electricity grid systems will be vulnerable to attack and that could result in loss of electrical services essential to maintaining our national economy and security.

Today, I'll discuss actions taken and required to bolster cybersecurity of the nation's power systems. Before I begin, if I may, I'd like to recognize several members of my team who were instrumental in developing my statement and performing the work underpinning it. With me today is Mike Gilmore, an Assistant Director, and Brad Becker, who led this effort. In addition, Lee McCracken, John Ludwigson, and Scott Pettis also made significant contributions.

In 2011, we reported on a number of challenges that industry and government stakeholders faced in securing smart grid systems and networks against cyber threats. These challenges included taking a comprehensive approach to cybersecurity, ensuring that smart grid systems had built-in security measures, monitoring implementation of cybersecurity standards and guidelines, effectively sharing cybersecurity information, and establishing cybersecurity metrics.

Since then, FERC has acted to implement our recommendations to assess these and other challenges in its ongoing cybersecurity efforts. However, it did not implement our recommendation to coordinate with state regulators and other groups to periodically evaluate the extent to which utilities and manufacturers are following voluntary cybersecurity guidelines.

Other entities have acted to improve cybersecurity in the sector. For example, NERC has issued updates to its critical infrastructure protection standards for cybersecurity and has hosted an annual conference on grid security. In 2014, NIST updated its smart grid cybersecurity guidelines to address the threat of combined physical-cyber attacks. NIST also issued a framework for improving critical infrastructure protection and cybersecurity. The framework is intended to provide a flexible and risk-based approach for entities including those within the electricity subsector to protect their vital assets from cyber threats.

The Departments of Homeland Security and Energy have efforts underway to promote the adoption of the framework by critical infrastructure owners and operators. These departments have also developed cybersecurity risk management approaches and tools that are available for use by the electricity subsector.

Nevertheless, given the increasing use of information and communications technologies to operate the electricity grid and other areas, continued attention to these and other areas is required to help mitigate the risk these threats pose to the electricity grid.

In particular, assuring that security features are built into smart grid systems and that a comprehensive approach to cybersecurity is taken whereby utilities employ a defense in depth strategy based on sound risk management principles will be essential. Effectively sharing cyber threat vulnerability and incident information among federal, state and local governments as well as the private sector stakeholders in a timely manner is imperative to provide utilities with the information they need to protect their assets against cyber threats.

Additionally, an effective mechanism for monitoring the implementation and effectiveness of the cybersecurity policies, practices and controls over U.S. power systems is paramount to ensure the resiliency and security of the electricity grid.

To summarize, more needs to be done to meet the challenges facing the industry in enhancing security. Federal regulators and other stakeholders need to work closely with the private sector to address cybersecurity challenges as the generation, transmission and distribution of electricity come to rely more on emerging and interconnected technologies.

Chairman Weber and Members of the Subcommittee, this concludes my statement. I'd be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

GAO

United States Government Accountability Office

Testimony

Before the Subcommittees on Energy and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 10 a.m. ET
Wednesday, October 21, 2015

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity of the Nation's Electricity Grid Requires Continued Attention

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

October 21, 2015

GAO Highlights

Highlights of GAO-16-174T, a testimony before the Subcommittees on Energy and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

CRITICAL INFRASTRUCTURE PROTECTION

Cybersecurity of the Nation's Electricity Grid Requires Continued Attention

Why GAO Did This Study

The electric power industry—including transmission and distribution systems—increasingly uses information and communications technology systems to automate actions with the aim of improving the electric grid's reliability and efficiency. However, such "smart grid" technologies may be vulnerable to cyber-based attacks and other threats that could disrupt the nation's electricity infrastructure. Several federal entities have responsibilities for overseeing and helping to secure the electricity grid. Because of the proliferation of cyber threats, since 2003 GAO has designated protecting the systems supporting U.S. critical infrastructure (which includes the electricity grid) as a high-risk area.

GAO was asked to provide a statement on opportunities to improve cybersecurity for the electricity grid. In preparing this statement, GAO relied on previous work on efforts to address cybersecurity of the electric sector.

What GAO Recommends

In its 2011 report, GAO recommended that (1) NIST improve its cybersecurity standards, (2) FERC assess whether challenges identified by GAO should be addressed in ongoing cybersecurity efforts, and (3) FERC coordinate with other regulators to identify strategies for monitoring compliance with voluntary standards. The agencies agreed with the recommendations, but FERC has not taken steps to monitor compliance with voluntary standards.

View GAO-16-174T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO reported in 2011 that several entities—the North American Electric Reliability Corporation (NERC), the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE)—had taken steps to help secure the electric grid. These included developing cybersecurity standards and other guidance to reduce risks.

While these were important efforts, GAO at that time also identified a number of challenges to securing the electricity grid against cyber threats:

- *Monitoring implementation of cybersecurity standards*: GAO found that FERC had not developed an approach, coordinated with other regulatory entities, to monitor the extent to which the electricity industry was following voluntary smart grid standards, including cybersecurity standards.
- *Clarifying regulatory responsibilities:* The nature of smart grid technology can blur traditional lines between the portions of the grid that are subject to federal or state regulation. In addition, regulators may be challenged in responding quickly to evolving cybersecurity threats.
- *Taking a comprehensive approach to cybersecurity:* Entities in the electricity industry (e.g., utilities) often focused on complying with regulations rather than taking a holistic and effective approach to cybersecurity.
- *Ensuring that smart grid systems have built-in security features:* Smart grid devices (e.g., meters) did not always have key security features such as the ability to record activity on systems or networks, which is important for detecting and analyzing attacks.
- *Effectively sharing cybersecurity information:* The electricity industry did not have a forum for effectively sharing information on cybersecurity vulnerabilities, incidents, threats, and best practices.
- *Establishing cybersecurity metrics:* The electricity industry lacked sufficient metrics for determining the extent to which investments in cybersecurity improved the security of smart grid systems.

Since 2011, additional efforts have been taken to improve cybersecurity in the sector. For example, in 2013, NERC issued updated standards to address these and other cybersecurity challenges. NIST also updated its smart grid cybersecurity standards in 2014. It has also developed a cybersecurity framework for critical infrastructure, and DHS and DOE have efforts under way to promote its adoption. In addition, FERC assessed whether these and other challenges should be addressed in its ongoing cybersecurity efforts. However, FERC did not coordinate with other regulators to identify strategies for monitoring compliance with voluntary cybersecurity standards in the industry, as GAO had recommended. As a result, FERC does not know the extent to which such standards have been adopted or whether they are effective. Given the increasing use of information and communications technology in the electricity subsector and the evolving nature of cyber threats, continued attention can help mitigate the risk these threats pose to the electricity grid.

Chairman Weber, Chairwoman Comstock, Ranking Members Grayson and Lipinski, and Members of the Subcommittees:

Thank you for inviting me to testify at today's hearing on efforts by federal agencies, including the Department of Energy, and industry to mitigate cybersecurity threats to U.S. power systems. As you know, the electric power industry is increasingly incorporating information and communications technologies (ICT) and networks into its existing infrastructure (e.g., electricity networks including power lines and customer meters). This use of ICT can provide many benefits, such as greater efficiency and lower costs to consumers. Along with these anticipated benefits, however, cybersecurity and industry experts have expressed concern that, if not implemented securely, modernized electricity grid systems will be vulnerable to attacks that could result in widespread loss of electrical services essential to maintaining our national economy and security.

Since 2003 we have identified protecting systems supporting our nation's critical infrastructure (which includes the electricity grid) as a high-risk area, and we continue to do so in the most recent update to our high-risk list.[1]

In my testimony today, I will describe actions taken and opportunities remaining to secure the grid against cyber attacks. In preparing this statement we relied on our previous work in this area, including studies examining efforts to secure the electricity grid and the associated challenges and cybersecurity guidance.[2] We also considered actions taken by agencies in implementing the recommendations from our prior report on cybersecurity of the electricity grid. The prior reports cited

[1] GAO's biennial high-risk list identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a government-wide high-risk area since 1997, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Most recently, in the 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities. See, most recently, GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

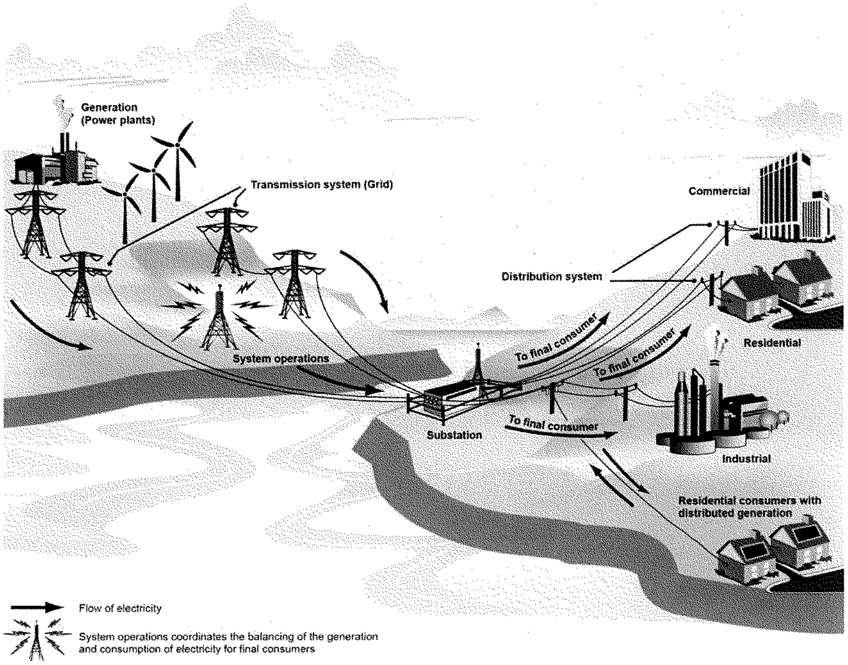
[2] GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO-12-92 (Washington, D.C.: Dec. 9, 2011), and *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, GAO-11-117 (Washington, D.C.: Jan. 12, 2011).

throughout this statement contain detailed discussions of the scope of the work and the methodology used to develop each of them. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The electricity industry, as shown in figure 1, is composed of four distinct functions: generation, transmission, distribution, and system operations. Once electricity is generated—whether by burning fossil fuels; through nuclear fission; or by harnessing wind, solar, geothermal, or hydro energy—it is generally sent through high-voltage, high-capacity transmission lines to local electricity distributors. Once there, electricity is transformed into a lower voltage and sent through local distribution lines for consumption by industrial plants, businesses, and residential consumers. Because electric energy is generated and consumed almost instantaneously, the operation of an electric power system requires that a system operator constantly balance the generation and consumption of power.

Figure 1: Functions of the Electricity Industry


Generation
(Power plants)
Transmission system (Grid)
Commercial
Distribution system
System operations
To final consumer
To final consumer
Residential
Substation
To final consumer
Industrial
Residential consumers with distributed generation
Flow of electricity
System operations coordinates the balancing of the generation and consumption of electricity for final consumers

Source: GAO. | GAO-16-174T

Utilities and others own and operate electricity assets, which may include generation plants, transmission lines, distribution lines, and substations—structures often seen in residential and commercial areas that contain technical equipment such as switches and transformers to ensure smooth, safe flow of current and regulate voltage. Utilities may be owned by investors, municipalities, and individuals (as in cooperative utilities). System operators—sometimes affiliated with a particular utility or sometimes independent and responsible for multiple utility areas—manage the electricity flows. These system operators manage and control the generation, transmission, and distribution of electric power using control systems—IT- and network-based systems that monitor and control sensitive processes and physical functions, including opening and closing circuit breakers.[3]

As we have previously reported, the effective functioning of the electricity industry is highly dependent on these control systems.[4] Nevertheless, for many years, aspects of the electricity network lacked (1) technologies—such as sensors—to allow system operators to monitor how much electricity was flowing on distribution lines, (2) communications networks to further integrate parts of the electricity grid with control centers, and (3) computerized control devices to automate system management and recovery.

Modernization of the Electricity Infrastructure

As the electricity industry has matured and technology has advanced, utilities have begun taking steps to update the electricity grid—the transmission and distribution systems—by integrating new technologies and additional IT systems and networks. Though utilities have regularly taken such steps in the past, industry and government stakeholders have begun to articulate a broader, more integrated vision for transforming the electricity grid into one that is more reliable and efficient; facilitates alternative forms of generation, including renewable energy; and gives consumers real-time information about fluctuating energy costs.

This vision—the smart grid—would increase the use of IT systems and networks and two-way communication to automate actions that system operators formerly had to make manually. Electricity grid modernization is an ongoing process, and initiatives have commonly involved installing advanced metering infrastructure (smart meters) on homes and commercial buildings that enable two-way communication between the utility and customer. Other initiatives include adding "smart" components to provide the system operator with more detailed data on the conditions

[3] Circuit breakers are devices used to open or close electric circuits. If a transmission or distribution line is in trouble, a circuit breaker can disconnect it from the rest of the system.

[4] 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).

of the transmission and distribution systems and better tools to observe the overall condition of the grid (referred to as "wide-area situational awareness"). These include advanced, smart switches on the distribution system to reroute electricity around a troubled line and high-resolution, time-synchronized monitors—called phasor measurement units—on the transmission system.

The use of smart grid systems may have a number of benefits, including improved reliability with fewer and shorter outages, downward pressure on electricity rates resulting from the ability to shift peak demand, an improved ability to more efficiently use alternative sources of energy, and an improved ability to detect and respond to potential attacks on the grid.

Regulation of the Electricity Industry

Both the federal government and state governments have authority for overseeing the electricity industry. For example, the Federal Energy Regulatory Commission (FERC) regulates rates for wholesale electricity sales and transmission of electricity in interstate commerce. This includes approving whether to allow utilities to recover the costs of investments they make to the transmission system, such as some smart grid investments. Meanwhile, local distribution and retail sales of electricity are generally subject to regulation by state public utility commissions.

State and federal authorities also play key roles in overseeing the reliability of the electric grid. State regulators generally have authority to oversee the reliability of the local distribution system. The North American Electric Reliability Corporation (NERC) is the federally designated U.S. Electric Reliability Organization, and is overseen by FERC. NERC has responsibility for conducting reliability assessments and developing and enforcing mandatory standards to ensure the reliability of the bulk power system—i.e., facilities and control systems necessary for operating the transmission network and certain generation facilities needed for reliability. NERC develops reliability standards collaboratively through a deliberative process involving utilities and others in the industry, which are then sent to FERC for approval. These standards include critical infrastructure protection standards for protecting electric utility-critical and cyber-critical assets. FERC has responsibility for reviewing and approving the reliability standards or directing NERC to modify them.

In addition, the Energy Independence and Security Act of 2007[5] established federal policy to support the modernization of the electricity

[5] Pub. L. No. 110-140 (Dec. 19, 2007).

grid and required actions by a number of federal agencies, including the National Institute of Standards and Technology (NIST), FERC, and the Department of Energy. With regard to cybersecurity, the act required NIST and FERC to take the following actions:

- NIST was to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems. As part of its efforts to accomplish this, NIST identified cybersecurity standards for these systems and the need to develop guidelines for organizations such as electric companies on how to securely implement smart grid systems. In January 2011,[6] we reported that NIST had identified 11 standards involving cybersecurity that support smart grid interoperability and had issued a first version of a cybersecurity guideline.[7] In February 2012, NIST issued the 2.0 version of the framework that, according to NIST documents, added 22 standards, specifications, and guidelines to the 75 standards NIST recommended as being applicable to the smart grid in the 1.0 version from January 2010.[8] In September 2014, NIST issued the first revision of the cybersecurity guidelines.[9]
- FERC was to adopt standards resulting from NIST's efforts that it deemed necessary to ensure smart grid functionality and interoperability. However, according to FERC officials, the statute did not provide specific additional authority to allow FERC to require utilities or manufacturers of smart grid technologies to follow these standards. As a result, any standards identified and developed through the NIST-led process are voluntary unless regulators use other authorities to indirectly compel utilities and manufacturers to follow them.

[6] GAO-11-117.

[7] NIST Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 1.0, January 2010 and NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010.

[8] NIST Special Publication 1108R2, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 2.0, February 2012.

[9] NIST Interagency Report 7628 Revision 1, *Guidelines for Smart Grid Cyber Security*, September 2014.

Cyber Threats and Vulnerabilities Facing the Electricity Grid

Like threats affecting other critical infrastructures, threats to the electricity industry and its transmission and distribution systems are evolving and growing and can come from a wide array of sources. Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, software coding errors, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled insiders, foreign nations engaged in espionage and information warfare, and terrorists.

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or pursuing a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. They make use of various techniques—or exploits—that may adversely affect federal information, computers, software, networks, and operations, such as a denial of service, which prevents or impairs the authorized use of networks, systems, or applications.

The potential impact of these threats is amplified by the connections between industrial control systems, supervisory control and data acquisition (or SCADA) systems, information systems, the Internet, and other infrastructures, which create opportunities for attackers to disrupt critical services, including electrical power. The increased reliance on IT systems and networks also exposes the electric grid to potential and known cybersecurity vulnerabilities. These include

- an increased number of entry points and paths that can be exploited;
- the introduction of new, unknown vulnerabilities resulting from an increased use of new system and network technologies;
- wider access to systems and networks due to increased connectivity; and
- an increased amount of customer information being collected and transmitted, which creates a tempting target for potential attackers.

We and others have also reported that smart grid and related systems have known cyber vulnerabilities. For example, cybersecurity experts have demonstrated that certain smart meters can be successfully attacked, possibly resulting in disruption to the electricity grid. In addition, we have reported that control systems used in industrial settings such as electricity generation have vulnerabilities that could result in serious damages and disruption if exploited.[10] Further, in 2007, the Department of Homeland Security, in cooperation with the Department of Energy, ran a test that demonstrated that a vulnerability commonly referred to as "Aurora" had the potential to allow unauthorized users to remotely control, misuse, and cause damage to a small commercial electric generator. Moreover, in 2008, the Central Intelligence Agency reported that malicious activities against IT systems and networks have caused disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multicity power outage.[11] In January 2014, the Director of National Intelligence, testified that industrial control systems and SCADA systems used in electrical power distribution and other industries provided an enticing target to malicious actors and that, although newer architectures provide flexibility, functionality, and resilience, large segments remain vulnerable to attack, which might cause significant economic or human impact. Further, in 2015 the Director testified that studies asserted that foreign cyber actors were developing means to access industrial control systems remotely, including those that manage critical infrastructures such as electric power grids. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

Cyber incidents continue to affect the electric industry. For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team noted that the number of reported cyber incidents affecting control systems of companies in the electricity subsector increased from 3 in 2009 to 25 in 2011. The response team reported that the energy sector, which includes the electricity subsector, led all others in fiscal year 2014 with 79 reported incidents. Reported incidents affecting the electricity subsector have had a variety of impacts, including hacks into smart meters to steal power, failure in control systems devices requiring power plants to be shut down, and malicious software disabling safety monitoring systems.

[10] GAO-07-1036.

[11] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

Actions Have Been Taken to Secure the Electricity Grid, but Continued Attention Is Required

As we have previously reported, multiple entities have taken steps to help secure the electricity grid, including NERC, NIST, FERC, and the Departments of Homeland Security and Energy. For example, NERC developed critical infrastructure standards for protecting electric utility–critical and cyber-critical assets. These standards established requirements for key cybersecurity-related controls: the identification of critical cyber assets, security management, personnel and training, electronic "security perimeters," physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets. In December 2011 we reported that NERC's cybersecurity standards, along with supplementary guidance, were substantially similar to NIST guidance applicable at the time to federal agencies.[12]

NERC had also published security guidelines for companies to consider for protecting electric infrastructure systems, although these guidelines were voluntary and typically not checked for compliance. For example, some of this guidance was intended to assist entities in identifying and developing a list of critical cyber assets. As of October 2015, NERC listed about 30 critical infrastructure protection standards for cybersecurity, some of which were subject to enforcement, some which were subject to future enforcement, and some which were pending regulatory filing or approval. NERC also had enforced compliance with mandatory cybersecurity standards through its Compliance Monitoring and Enforcement Program, including assessing monetary penalties for violations.

NIST, in accordance with its responsibilities under the Energy Independence and Security Act of 2007, has identified cybersecurity standards for smart grid systems. Specifically, in August 2010 NIST had identified 11 such standards and issued the first version of a cybersecurity guideline.[13] As we reported in January 2011, NIST's guidelines largely addressed key cybersecurity elements, with the exception of the risk of attacks using both cyber and physical means—an element essential to securing smart grid systems. We recommended that

[12] GAO-12-92.

[13] GAO-11-117.

NIST finalize its plan and schedule for incorporating the missing elements into its guidelines. In 2014, NIST issued updated guidelines, which address the relationship of smart grid cybersecurity to cyber-physical attacks and cybersecurity testing and certification.[14] In addition, it describes the relationship of smart grid cybersecurity to NIST's cybersecurity framework that was issued in February 2014.[15] This framework, which was developed in accordance with Executive Order 13636,[16] is to enable organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the cybersecurity and resilience of critical infrastructure.

FERC had also taken several actions, including reviewing and approving NERC's critical infrastructure protection standards in 2008. It had also directed NERC to make changes to the standards to improve cybersecurity protections. However, in 2012 the FERC Chairman stated that many of the outstanding directives had not been incorporated into the standards. We also noted in our January 2011 report that FERC had begun reviewing smart grid standards identified by NIST, but declined to adopt them due to insufficient consensus.

The Department of Homeland Security, in its capacity as the lead federal agency for cyber-critical infrastructure protection, had issued recommended practices to reduce risks to industrial control systems in critical infrastructure sectors, including the electricity subsector. The department has also provided on-site support to respond to and analyze security incidents and shared actionable intelligence, vulnerability information, and threat analysis with companies in the electricity subsector. In addition, the department, in accordance with Executive Order 13636, established a program to promote the adoption of the NIST cybersecurity framework.

As the lead agency responsible for critical infrastructure protection efforts in the energy sector, the Department of Energy, as we reported in December 2011, was involved in efforts to assist the electricity subsector in the development, assessment, and sharing of cybersecurity standards,

[14] NIST Interagency Report 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity*, September 2014.

[15] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Feb. 12, 2014).

[16] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

according to department officials.[17] In addition, the department has created sector-specific guidance to assist the sector in implementing the NIST cybersecurity framework. The guidance includes sections that explain framework concepts for its application, identify example resources that may support framework use, provide a general approach to framework implementation and identify an example of a tool-specific approach to implementing the framework.

Challenges Existed to Securing Electricity Systems and Networks

In our January 2011 report we identified a number of key challenges that industry and government stakeholders faced in securing the systems and networks supporting the electricity grid.[18]

- *Monitoring implementation of cybersecurity standards.* Best practices for information security call for monitoring the extent to which security controls have been implemented. In our report, we noted that FERC had not developed an approach coordinated with other regulators to monitor, at a high level, the extent to which industry follows the voluntary smart grid standards it adopts. We recommended that FERC, in coordination with state regulators and groups that represent utilities subject to less FERC and state regulation, periodically evaluate the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards and develop strategies for addressing any gaps in compliance with standards that are identified as a result of this evaluation. However, FERC has not implemented this recommendation. While FERC has reported that it has taken steps to collaborate with stakeholders, it has not taken steps to determine the extent to which the voluntary standards have been integrated into products or whether they are effective. Monitoring such efforts would help FERC and other regulators know if their approach to standards setting is effective or if changes are needed.

- *Clarifying regulatory responsibilities.* Experts we spoke with during the course of our review in 2011 expressed concern that there was a lack of clarity about the division of responsibility between federal and state regulators, particularly regarding cybersecurity. While jurisdictional responsibility has historically been determined by whether a

[17] GAO-12-92.

[18] GAO-11-117.

technology is located on the transmission or distribution system, experts raised concerns that smart grid technology may blur these lines because, for example, devices deployed on parts of the grid traditionally subject to state jurisdiction could, in the aggregate, affect the reliability of the transmission system, which falls under federal jurisdiction. Experts also noted concern about the ability of regulatory bodies to respond quickly to evolving cybersecurity threats. Clarifying these responsibilities could help improve the effectiveness of efforts to protect smart grid technology from cyber threats.

- *Taking a comprehensive approach to cybersecurity.* To secure their systems and information, entities should adopt an integrated, organization-wide program for managing information security risk. Such an approach helps ensure that risk management decisions are aligned strategically with the organization's mission and security controls are effectively implemented. However, as we reported in 2011, experts told us that the existing federal and state regulatory environment had created a culture within the utility industry of focusing on compliance with regulatory requirements instead of one focused on achieving comprehensive and effective cybersecurity. By taking such a comprehensive approach, utilities could better mitigate cybersecurity risk.

- *Ensuring that smart grid systems have built-in security features.* Information systems should be securely configured, including having the ability to record events that take place on networks to allow for detecting and analyzing potential attacks. Nonetheless, experts told us that certain currently available smart meters had not been designed with a strong security architecture and lacked important security features, such as event logging.[19] By ensuring that smart grid systems are securely designed, utilities could enhance their ability to detect and analyze attacks, reducing the risk that attacks will succeed and helping to prevent them from recurring.

- *Effectively sharing cybersecurity information.* Information sharing is a key element in the model established by federal policy for protecting critical infrastructure. However, the electric industry lacked an effective mechanism to disclose information about cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices.

[19] Event logging is the ability of an IT system to record events occurring within an organization's systems and networks, including those related to computer security.

For example, experts we spoke with stated that while the industry had an information sharing center, it did not fully address these information needs. Establishing quality processes for information sharing will help provide utilities with the information needed to adequately protect cyber assets against attackers.

- *Establishing metrics for evaluating cybersecurity.* Metrics are important for comparing the effectiveness of competing cybersecurity solutions and determining what mix of solutions will make the most secure system. The electric industry, however, was challenged by a lack of cybersecurity metrics, making it difficult to determine the extent to which investments in cybersecurity improve the security of smart grid systems. Developing such metrics could provide utilities with key information for making informed and cost-effective decisions on cybersecurity investments.

In our January 2011 report, we recommended that FERC, working with NERC as appropriate, assess whether any cybersecurity challenges identified in our report should be addressed in commission cybersecurity efforts.

Since that time, FERC took the following actions. First, in 2011, it began evaluating whether cybersecurity challenges, including those identified in our report, should be addressed under the agency's existing cyber security authority and efforts. As a part of this effort, the commission directed NERC to revise the electricity industry's critical infrastructure protection (CIP) standards with the aim of addressing, among other things, cybersecurity challenges identified in our report. In November 2013, NERC issued updated CIP standards to address these and other cybersecurity challenges. Second, the commission held a technical conference in 2011 in which it solicited feedback from industry stakeholders to help inform the agency's cybersecurity efforts. Third, in September 2012, the commission established an Office of Energy Infrastructure Security, which is to, among other things, help mitigate cyber security threats to electricity industry facilities, and to improve cybersecurity information sharing.

In summary, as they become increasingly reliant on computerized technologies, the electricity industry's systems and networks are susceptible to an evolving array of cyber-based threats. Key entities, including NERC and FERC, are critical to approving and disseminating cybersecurity guidance and standards, while NIST, DHS, and the Department of Energy have additional roles to play in providing guidance and providing other forms of support for protecting the sector against cyber threats. Moreover, without monitoring the implementation of voluntary cybersecurity standards in the industry, FERC does not know the extent to which such standards have been adopted or whether they are effective. Given the increasing use of information and communications technology in the electricity subsector and the evolving nature of cyber threats, continued attention can help mitigate the risk these threats pose to the electricity grid.

Chairman Weber, Chairwoman Comstock, Ranking Members Grayson and Lipinski, and Members of the Subcommittees, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Contact and Acknowledgments

If you or your staffs have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other staff who contributed to this statement include Franklin J. Rusco, Director; Michael W. Gilmore; Bradley W. Becker; Kenneth A. Johnson; Jon R. Ludwigson; Lee McCracken; Jonathan Wall; and Jeffrey W. Woodward.

Biography

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the federal government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.

Chairman WEBER. Thank you, Mr. Wilshusen, and I now recognize myself for five minutes of questions. Wow, where do we start?

Mr. Gaines, the Department of Energy's Office of Electricity works with electric utilities on information sharing and encouraging utilities to learn from the challenges faced by their regional counterparts. The Department of Homeland Security also operates programs to facilitate the information sharing you referred to in your comments. What information do you feel is most important to share with each other and for the industry to share with regulators, and the third part to my question really is, in your comments I think you said information had to be actionable.

Mr. GAINES. Correct.

Chairman WEBER. Define what you mean by "actionable." Let me reiterate. What information do you feel is most important for industry to share with each other and then to share with the regulators? It may be one and the same. And then define "actionable information" for us.

Mr. GAINES. I'll start out with your first questions in that we have spent the last two years working directly with both agencies and within the confines of the programs that they have, which are the CRISP tool and the enhanced cybersecurity tool, and they are very effective. The difficulty of both of those tools, they're historical; they look back. They don't look at real-time incidents, and in some cases, there can be a lag between three to six months from when an incident occurred. It's not correlated on a timely manner as to what is going on with the rest of the industry so that we can take action on those events, and in some cases, you could have a dormant piece of malware sitting in your environment that you didn't take action on but that was alerted months earlier.

As it relates to actionable, it's having real-time information, and a technical term—I don't want to lose you—is the actual threat actors' IP address and the specific information that's time-framed within that window. An illustration of that would be——

Chairman WEBER. You're not losing me. I was wondering about that earlier when you said up to 4 months since 2011, 300 attacks, and no suspects.

Mr. GAINES. That's correct.

Chairman WEBER. Go ahead.

Mr. GAINES. And that is the difficulty is that by the time the actor penetrates your environment, they're not the actor that you see. There's an alias that sits behind that wall and the difficulty is following that breadcrumb back to the original source, and one of the difficulties that we have in the industry is, is the information we get from the federal government is not timely, and so for us to take action on something that really we have no control over is very difficult. My suggestion would be to reverse that, is for us to provide across the industry real-time incidents, and it's doable, and to be able to track not only the source but the actual follow-on activity that occurs from that event.

One of the things that we don't do is we don't do a good diagnostics of what happens once the event occurs, and we move on to the next one.

Chairman WEBER. Let me jump over to Mr. Wilshusen. You talked about having conferences, I think, you met around the country, probably industry and I presume government as well. How often are those conferences held and how many attendees, and should we increase that frequency and are they sharing that information?

Mr. WILSHUSEN. Well, what I referred to were conferences that were being held by NERC, which is the North American Electric Reliability Corporation, and they hold those annually, but to the extent that Mr. Gaines talked about in providing useful, actionable information in a timely manner, annual is not enough. They do talk about different threats——

Chairman WEBER. It would almost have to be daily or weekly.

Mr. WILSHUSEN. Much more frequently. This has been——

Chairman WEBER. Absolutely.

Mr. WILSHUSEN. Right. This has been——

Chairman WEBER. I'm talking about the sharing of the information.

Mr. WILSHUSEN. Right, the sharing of the information, particularly between federal government and the private sector and even among private sector entities has been a longstanding problem and a challenge throughout all critical infrastructure sectors including the, electricity subsector. What we have found in the past is that there have been certain obstacles to doing that including from the government sector to private sector, making sure that those individuals at the private sector had the appropriate security clearances—that's been a challenge—as well as having a secure mechanism to share that information timely.

Chairman WEBER. Is there one office that oversees what you're describing? Is there one office within your agency, for example, that oversees that? Who oversees that?

Mr. WILSHUSEN. Well, overall, DHS has a responsibility across federal government for taking the lead in the——

Chairman WEBER. So does DHS—you may not know this—forgive me for interrupting, but does DHS have one office that allocates their time and manpower and resources to just this cybersecurity for energy companies alone? Do you know?

Mr. WILSHUSEN. Well, it does have a group that's responsible overall but the Department of Energy, known as the sector-specific agency, also has responsibility for interacting with the energy sector to include the electricity sector for sharing information and assisting that sector in securing its systems.

Chairman WEBER. I am running out of time, but I have one last question. So what could be done better to help streamline this process?

Mr. WILSHUSEN. Well, one of the requirements under the Executive Order 13–636 is for agencies and particularly I think it's DOD and perhaps DHS to come up with a mechanism that will allow for faster sharing of information to the private sector.

Chairman WEBER. All right. Thank you.

I'm over time, and I yield to the gentlelady from Oregon.

Ms. BONAMICI. Thank you very much, Mr. Chairman, and thank you to the witnesses for bringing your expertise on an important issue.

I also serve on the Education and Workforce Committee, and I'm going to focus at first on some of the workforce issues making sure that we have the workforce that we need to continue to address this serious issue, and I know Mr. Stacey, you said that the demand for trained cyber defenders with control systems knowledge vastly exceeds the supply.

Now, my alma mater, the University Of Oregon, has just created an Oregon Center for Cybersecurity and Privacy. They received a federal—some federal funding, and a Center of Excellence designation, and they plan to begin enrolling students by next summer. But how can we incentivize more universities to support educating this workforce, and once we have a strong pipeline of students and get them into the workforce, how can we attract them to public service and government jobs when typically the private sector would pay more and be perceived as more innovative?

So I'll start with Ms. Lee and also ask Mr. Wilshusen and anybody who wants to weigh in.

Ms. LEE. As I noted in my statement, I previously was in the federal government for 14 years. I think one of the real advantages of working in the federal government is the kind of work you can do and the impact that you have. I mentioned the guidelines for smart grid cybersecurity products that we developed. There were 150 volunteers from around the world that participated in developing that document. These were senior-level people literally around the world. I kept getting asked, do you pay these people, and my response was no, these are volunteers. I think one thing in the federal government and working with the federal government for several decades, you can have an impact and influence that you don't have anywhere else, and to me, that's a real benefit for working in the public sector. Private sector does compete. It is difficult now. There're very few—as mentioned earlier, there are not significant numbers of people who are in cybersecurity, and those who focus on control systems, and as I mentioned, there are some basic differences between cybersecurity for control systems and our IT systems. That community is even smaller. We need to beef up that workforce. There are controls that you don't put on OT systems that are typical on IT systems, and we need to—we definitely need to grow this area.

Ms. BONAMICI. And do you agree with Mr. Stacey that there's a serious need, that we don't have the workforce?

Ms. LEE. We don't have the workforce.

Ms. BONAMICI. I want to follow up because I know the U of O Center is going to be working with the faculty from several different departments including computer and information science, philosophy, business, law. What role—you talked about the role of human behavior but how can we really capitalize on understanding human behavior to deal with the threats, and also hopefully to be out in front and prevent them.

I'll open it up to the panel. Ms. Lee, do you want to start?

Ms. LEE. As you mentioned, I think human behavior is very important. Historically—and I've been doing cybersecurity now for almost three decades—the solution was, have longer passwords, and so what does everybody do? They write them down because you can't remember 12- or 15-character passwords that you have to change every 3 or 4 months.

Ms. BONAMICI. We've all done that.

Ms. LEE. Yeah. You write them down. That's the only way you can remember them. Is to look at cybersecurity and the solution has to be yes, we need to figure it out. As I say, it's a messy environment.

If you look at the reality of cybersecurity, the devices that are out there, the controls you may need to implement. you can't do. You either can't afford them or they affect the performance. You need to figure out the solutions. And I think that's the direction that cybersecurity needs to go. Historically——

Ms. BONAMICI. Thank you. I need to get a couple more questions in.

Mr. Gaines, you talked about the TIM, the Threat Intelligence Management. That seems like a sound approach. What are the barriers to improving and expanding that approach?

Mr. GAINES. The barriers are twofold. One, there are limitation that industry has today in communicating with the government vulnerabilities, and that is a real challenge in that we are limited to some extent because we hold the liability if there's a breach or vulnerability to the network. I think that needs to looked at and in some cases eliminated so that we can share openly very specific information about vulnerabilities.

The second is, is the actual technologies themselves. Today, we are one of only two utilities that have a completely integrated security operation center, and Ms. Lee spoke about that center. It's a center that we integrate the physical, being badge access, building access. We integrate the IT, being the cyber component, and we integrate the operational, the SCADA systems together. All three of those systems are actually monitored, reviewed, and we take actions against events, and I'll use a simple analogy so you can understand——

Ms. BONAMICI. I'm afraid my time's going to expire. Can I just have a few more seconds, Mr. Chairman?

Chairman WEBER. Without objection.

Ms. BONAMICI. I want to get in a quick question for Mr. Wilshusen. You mentioned in your testimony that FERC was adopting standards from NIST's efforts but according to FERC officials, the statute did not provide any authority to allow FERC to require the smart grid technologies to follow the standards and now it's voluntary. How's that working?

Mr. WILSHUSEN. Well, it is voluntary. One of the problems that we noted is that FERC has not—because the standards are voluntary and have not been adopted, it has not gone out to examine the effectiveness or the extent to which those voluntary standards have been implemented.

Ms. BONAMICI. Thank you, and I'm very over time.

Thank you, Mr. Chairman. Yield back.

Chairman WEBER. No problem.

And now the Chairman is pleased to recognize for his first appearance in a hearing in this Committee, the gentleman from Illinois, Darin LaHood. Welcome.

Mr. LAHOOD. Thank you, Mr. Chairman, very much. I appreciate it. Great to be part of this Subcommittee.

I want to thank the witnesses for your testimony this morning.

I guess, Mr. Stacey, I wanted to just maybe see if you could highlight a couple examples of cyber attacks that maybe recently happened where systems have been compromised and maybe the cost to a particular company and how it affected citizens or customers.

Mr. STACEY. Yes. Two of the most recent are BlackEnergy and Havex attacks. These have been to the human-machine interface associated with the industrial control systems. Near as we can tell, those are primarily associated with collecting information, trying to map out systems and see what they look like, although the payloads on those are dynamic. There's been a very active response from DHS on this along with other entities, in fact, traveling around the country in briefings with the FBI and notifying people about that.

As far as the costs associated with individual utilities in mitigating that, I don't have insight into that, but I know the federal government and the laboratory took a very aggressive stance on notifying and making people aware of those particular malware.

Mr. LAHOOD. And I guess as a follow-up maybe to Mr. Gaines, when we talk about cybersecurity and talk about really what these entities are engaged in is criminal activity, when we talk about deterring that, I mean, are there currently any active prosecutions by the federal government, either the U.S. Attorney's Office or anybody that we can kind of use as examples to deter this behavior?

Mr. GAINES. I don't—I'm not aware of any criminal activity so I say that. I do know that there have been incidents that have been nation-state and/or in some cases domestic that probably warrant the investigation of that. A good example of that would've been the Metcalf incident that occurred in southern California in 2013. That substation lost 17 transformers. There were 127 rounds of ammunition that was shot into the substation and power had to be rerouted.

To the Chairman's point, though, that actor has not—and/or actors have not been found, and the evidence obviously is very clear that it was multiple actors very potentially.

But to the extent that there has been prosecution, that has not occurred, to my knowledge.

Mr. LAHOOD. And on that specific case with Metcalf, is there an ongoing investigation to try to determine who the perpetrator was?

Mr. GAINES. There absolutely is, and following that incident, FERC issued a number of standards on physical security that the industry is now implementing, and a lot of that has to do with both the monitoring both of the physical asset and the cyber asset, and so we've learned from an industry but to the extent that we've seen that replicated or duplicated in industry, it has not.

Mr. LAHOOD. In terms of becoming aware when a system is compromised, walk me through a little bit of, if a company is compromised, the reporting on that in terms of to the federal government. Is that something that's made public, or who's the repository of threats or compromises that happen, and then how does that get made public or is there some secrecy involved with that? I mean, I guess what I'm getting at, do companies, you know, in a competitive marketplace not want people to be aware that their systems were compromised for vulnerabilities? How is that addressed?

Mr. GAINES. I'll give you a real-life example. At 11 o'clock yesterday afternoon, our systems were attempted to be penetrated by a denial of service, so they're flooding your network. That flooding of the network slows down your network, and at that point we pick it up on our firewalls, we shut the traffic down, and then we do forensics on that. Within an hour, we report that to the ES ISAC. That ISAC is our sector group that we use to facilitate that type of information. Now, I go back to my original point that I made earlier. That happened to me. I venture to say that that same actor was scanning other networks and that that same DDoS attack was being attempted. At 4 o'clock, we get an acknowledgement back from the government that they received the information. As of 11 o'clock, 24 hours later, I still don't have a response back from the government.

There's a good example of the timeliness of information. If we could share that information real time within the industry, think about the potential of being able to collaborate very quickly and take action because most likely that actor has shut down their server and they've moved on, and so we have no time again to take any reasonable mitigation steps. The good news is, our security systems worked. To the extent that that threat I reported gets communicated, it does get communicated. Most likely it'll be a few months from now. It'll be watered down, and the real sad part about it is, it doesn't have the level of detail to take any action on it.

Mr. LAHOOD. Thank you.

Thank you, Mr. Chairman.

Chairman WEBER. Thank you.

And before I go to the gentleman from New York, if I can just take one second here, so what you just described, Mr. Gaines, gets back to those conferences. If you could come in with that kind of information in real time to everybody that was in a like business and say expect this kind of attack, is that a doable deal?

Mr. GAINES. I would—if I may——

Chairman WEBER. Sure.

Mr. GAINES. I would argue slightly different. I have security clearance, and to the gentleman's point, Homeland Security does offer briefings to those that have security clearance. They're non-industry-specific so they can be across any sector. And ironically, the same approaches that an actor uses in finance is very similar to an attempt that they would use in our industry. That's still not soon enough. Those briefings occur once every three months.

Chairman WEBER. But is there no platform to broadcast this information industry-wide? And let's be energy industry specific. Is there no platform for that?

Mr. GAINES. There is. My point being is, it's not timely enough. There is, and it's a very good tool. It's not timely enough and it's not detailed enough.

Chairman WEBER. All right. Thank you.

I appreciate the gentleman from New York's indulgence. You're recognized.

Mr. TONKO. Thank you, Mr. Chairman.

Welcome to our panelists.

The line between federal and state power has historically been drawn at the intersection between the high-voltage transmission system and the lower-voltage distribution system. However, the relevance of this distinction is less clear when it comes to cybersecurity, and Ms. Lee, you addressed some of that with the new technologies, but to both you and Mr. Gaines, Ms. Lee and Mr. Gaines, could the increase of smart grid and distributed energy technologies being deployed on the electrical distribution system increase those cybersecurity risks to the high-voltage transmission system.

Ms. LEE. As I said in my statement, the increase in technology and the inclusion of IT and communications, the new technology, yes, that does increase the potential for cybersecurity events. I will add another one, and that is the interconnection of these systems. If we look at the new technology, our distributed energy resources, renewable devices where you transmit the electricity that may be generated in one state to another state, all of that increases the attack surface and the potential for cybersecurity events.

On the other side, utilities, reliability is number one. Cybersecurity should support the reliability of the grid, and there are a number of tools and techniques that the electric sector has been using for decades to address reliability that can also be used to address cybersecurity. This is not a totally foreign area, and so it's taking advantage of what they're currently doing, and then looking at the techniques and technologies that the IT community uses to address these new threats.

Mr. TONKO. Thank you.

And Mr. Gaines, do you also concur that it increases risk here?

Mr. GAINES. If I may, not to differ, I might add a different perspective——

Mr. TONKO. Okay.

Mr. GAINES. —if I could, please? The distribution system and transmission system are two separate systems. The distribution system is a regional, local system and smart grid and/or tied to that smart grid is a meter. That's an individual IP address. It's an individual computer. Think of it like that. There are securities around that through a certificate and encryption, and in our design, that particular meter is not tied into our core distribution system. We have what we call a head-in system that sits outside of our company.

So I would suggest to you that from a smart meter and smart grid perspective, the design and construct of that is secure. Is there a risk in our cases in Pennsylvania? We have two million customers, and I'm convinced given enough time with a bad actor, they could figure out how to be destructive with that. But to the extent that our design and configuration within the industry and our design and configuration is very similar to most smart grids and the technology is very similar. So there's a risk but I don't see it as a huge threat.

Mr. TONKO. And no specific recommendations you would make to address that increased risk, either of you?

Mr. GAINES. I would—the gentleman, Mr. Stacey, made some very good points. I think good hygiene is important, good engineering is important, and constant management. These devices are now computers and so they have to be maintained. They don't have the life of an existing meter, which is 20 to 30 years. These devices have a life of between five to seven years, and so the challenge that the industry is making sure they maintain their smart grid environment, not neglect it.

Mr. TONKO. Ms. Lee?

Ms. LEE. There are things that the industry, as Mr. Gaines said, is doing, and I mentioned in my testimony all utilities do risk assessments. They need to prioritize their system, prioritize the risks and vulnerabilities, and then make decisions about which ones they want to mitigate. They do not have unlimited resources. Utilities deal with many areas of risk. Cybersecurity is one area. And they need to prioritize and determine what they want to do for their mitigation strategies and then make decisions that way.

Mr. TONKO. There was some exchange—thank you. There was some exchange over the role of forensics in cybersecurity. What do we need—this is to all of you. What is needed to adequately conduct a forensic analysis after a cyber event? What are the best——

Mr. GAINES. Directed to me, sir?

Mr. TONKO. Any of the four.

Mr. GAINES. Two things. First of all, there needs to be—I go back to what we can share and what we cannot share with the government during an incident. That's a—there's a lag that occurs there. If I have a major incident in my environment, I have to report that to several agencies. That can be days or weeks in some cases. Secondly, once we determine it truly was a cyber incident, then I have to put together a full investigative report, and then it goes through a very lengthy process of determining the actual degree or significance of that. I suggest to you that we cut all that or most of that away, and that if I truly know that I've been breached inside of my network, I think there's an obligation that we work much closer with the federal government on a real-time basis of defining the problem first and then let's go assess the penalties or determine who was at fault later, and that lag at times can be weeks and months before we actually get into the real forensics and do the real what I think are important things are mitigating it. And more importantly, that information is not shared with the industry in some cases for a year.

Mr. TONKO. Thank you very much.

Mr. Chair, I yield back.

Chairman WEBER. I thank the gentleman.

And now the gentleman from Arkansas, Mr. Westerman, is recognized for five minutes.

Mr. WESTERMAN. Thank you, Mr. Chairman, and thank you, panel, for your insight today.

Mr. Wilshusen, I'll direct this question to you, but others may wish to add in on it. I've visited several power-generating facilities, and I was pleased to find out that the control systems inside the power plants are totally isolated from the outside world in the facilities I've visited, so the chance of a cyber attack on the actual generating facilities is pretty much mitigated unless a bad actor got into the facility and messed with the control system, which could cause a huge issue. So when we're talking about a cyber attack, what physically are the risks there since these power plants are basically just getting a demand signal from the grid? What kind of destruction do you anticipate could happen from a cyber attack?

Mr. WILSHUSEN. Well, first of all, I would first ask about your premise that the industrial control systems networks are indeed isolated and separated from other external networks or company communications networks. What we have found and what I have seen reported through ICS–CERT and others is that often companies believe their industrial control systems networks may be air-gapped, if you will, but are surprised to find when in fact they are not. With the increasing introduction of information and communications technologies, we're finding, increasingly, that these networks are indeed interconnected with other networks. That's one thing. But given that, if they are air-gapped, it does provide an additional level of security certainly to where remote access may not be available and where an attacker may have to have physical access to the device. But to be sure that's something that if they are air-gapped, that is an improvement and a control over it, but—and that's what has been historically but increasingly we're finding on what's being reported is that they are being interconnected with internal and external networks, thereby as Ms. Lee mentioned, increasing the attack surface and increasing the likelihood of a potential incident over those industrial control systems networks.

Mr. WESTERMAN. So is that the main concern with cyber attacks is getting into those power-generating facilities' control systems or is it more to protect the distribution and transmission systems?

Mr. WILSHUSEN. Well, I think you have that probably at multiple sections throughout the entire electricity grid, depending upon where the control systems or the sensors are located. If they are indeed interconnected to external networks, there's an increased likelihood that they may be vulnerable to attack if they're not sufficiently hardened. Of course, there are actions that an entity can take to better secure those connections and to better secure those devices. If those are being done, that will help, but historically, that always hasn't been done for a number of reasons.

Mr. WESTERMAN. It just seems like it would be a good operating protocol to have those industrial control systems isolated from the outside world as far as having the best way to keep a cyber attack from happening on one of those facilities.

Mr. WILSHUSEN. Yes, that's correct, but often they're interconnecting in order to provide greater efficiency and usefulness, if you will, and so there's always that balance, but yes, it would be better from a security perspective to keep them isolated.

Mr. WESTERMAN. So when we talk about the role that smart grid technology plays in creating cyber vulnerabilities, does the fact that the smart grid relies on two-way communication make the grid more susceptible to cyber attacks, and if so, how is that?

Mr. WILSHUSEN. Well, potentially, and that would be as Mr. Gaines mentioned more at the distribution level rather than the power-generating and transmission level where there could be attacks against individual smart meters. Indeed, I believe there have been reported attacks against smart meters, but more for the purpose of committing fraud and addressing some of the programming that is in those smart meters, but the threat potentially is, and again, absent other controls that may now be in place, is that collectively as millions of smart meters out there could that have an impact on the larger electricity grid, and that's something that there potentially could.

Mr. WESTERMAN. And when you talk about smart meters, are you talking about the meters that give the feedback or just the ones that the meter reader can drive through the neighborhood and read the meters without getting out of the vehicle? Are those——

Mr. WILSHUSEN. Yeah, those would be included in that, yes.

Mr. WESTERMAN. I think I'm out of time, Mr. Chairman.

Chairman WEBER. Okay. The gentleman yields back.

The gentlelady from Connecticut, Ms. Esty, is recognized.

Ms. ESTY. Thank you, Mr. Chairman and to our Ranking Members for today's very important hearing.

In Connecticut, we're very focused on grid reliability just actually from natural disasters we've been coping with, and certainly the cybersecurity threat has gotten us all to pay much closer attention.

I have two quick questions. First for Ms. Lee and Mr. Gaines. Can you explain a little bit more how we should address the challenges between the difference in lifespan of operational technology and information technology? All of us who know, who have any of those devices in our pockets, and if you've got teenagers, you really know within a year they want a new one, and yet we're looking at overall systems on the utility side that are decades long. What do we know about from prior history that can help us in Congress think about how to meld together these two systems, one of which is highly capital-intensive over decades and another which is changing constantly?

Mr. GAINES. Ms. Lee, go ahead.

Ms. LEE. Thank you. Yes, as I mentioned earlier, the difference in lifecycle—and it's amazing when you think our device if it's a year old, it's ancient.

What needs to be done, and talking about the modernization of the grid, and I think of that more than just a smart grid. If you want to talk about all of the domains—generation, transmission and distribution—the new devices are using commercially available operating systems and applications rather than the proprietary solutions that were used historically, and so when you look at these devices, yes, they may have a lifespan of 30 or 40 years but you have Windows, you have your internet protocols. It's having the two communities, and Mr. Gaines talked about that, having the communities, the IT and OT communities together, figure out the best solutions, and a lot of utilities are putting them in the same room and addressing these difficulties because when you get away from the proprietary solutions, you need to figure out how do you do it with all of these commercially available products.

Mr. GAINRS. I would add to that two things you heard me in the testimony. We have and are converging both the operational side of our business and the IT side of our business, and we're doing it a lot with technology first of all. Inside of a substation, 15 years ago it was an analog substation and it was not two-way communication. What sits in a substation now is a communications network, and so we are building out with inside substations a very protected, secure network inside of that substation, and it comes with us—it comes with cyber risk but it also comes with the ability to monitor that substation. And so that is the piece that some of those in industry are doing. We are thinking of that substation as a physical asset as well as a logical asset. And so when I actually manage our substations, I think of them as a computer. I think of them as an asset in transmitting and/or transferring energy, and in one place we look at both of those. We don't separate those two. We don't separate the operational side of our business from the cyber side or the technology side. And as more communication devices go into substations, that's going to be required.

Ms. ESTY. Thank you. That is very helpful.

And just a quick question for anyone who wants to chime in. Part of what we do is direct research dollars from this Committee, and if you had to divide up the federal research dollars between on cybersecurity, in prevention, detention, mitigation, and recovery, at this stage of the game, what do you think for us—those of us who sit here in Congress as we're allocating funds and we all know we should have more funds, but with the not enough money that we have, as I think about it, how should we think about dividing those up?

Mr. GAINES. Mine would be prevention. It has the greatest opportunity to be able to share, and I think the greatest opportunity to expand and grow.

Mr. STACEY. Yes. Thank you for the question.

I would offer that we're spending an awful lot today on the measure-countermeasure. The threats and the daily bombardment is consuming most of our resources. We need to make sure that we're investing a significant amount of our research dollars in how do we take some of these critical assets off the table with either some kind of disruption zone—which is now a terminology that's being used where you put some kind of a——

Chairman WEBER. A firewall? A firewall?

Mr. STACEY. Well, it's not quite as sophisticated as a firewall. It's an analog circuit that allows the electrons to go in and only do one thing, and it requires the cyber hacker to have physical access to the other side. And so research associated with trying to help define the critical assets and then we create an environment to take some of these critical assets off the table.

So to answer your question shortly, I believe more needs to be done to get us out of this paradigm of measure-countermeasure and how we're going to solve this long term because, frankly, the resources aren't scalable. Thank you.

Ms. ESTY. Thank you. That's very helpful, yes.

We all remember Mad Men and Spy versus Spy. I think you're right. We need to be removing assets from vulnerability. It makes a lot of sense.

Thank you all very much.

Chairman WEBER. The gentlelady yields back.

I now recognize the gentleman from Alabama, Mr. Palmer.

Mr. PALMER. Thank you, Mr. Chairman, and thank you to the witnesses for coming in this morning. It's extremely important.

Mr. Gaines, the National Institute for Standards and Technology has developed voluntary guidelines for smart grid cybersecurity, and the Federal Energy Regulatory Commission continues to approve cybersecurity standards. How helpful are these types of standards to the industry?

Mr. GAINES. The standards are invaluable. They create a baseline. However, I suggest to you that's just what they are is a baseline, and that the threats that we see today are going forward, they're not going back. And so we identify most of the vulnerabilities associated with those standards and things that happen to us, not what things are going to happen to us. And I don't think that you can regulate or put standards in this to control every vulnerability. What I think you have to have is a collaborative effort across industry and government to address some of the issues that we have.

Mr. PALMER. Part of my concern is that these are industry standards, and James Clapper, the Director of National Intelligence, said the greatest threat to our national security is cyber attacks. I think he identified 140 attacks against U.S. corporations by China, and it appears to me that we're in the middle of a digital arms race in terms of cyber attacks, and specifically my concern right now is with our energy infrastructure and how devastating it would be if we had a cyber attack against our infrastructure that shut it down. Do you think industry standards alone are enough or does the government need to take a more active role in this, particularly in developing the technology to protect us against cyber attacks?

Mr. GAINES. First of all, to answer your first question, are the standards adequate, they are adequate, and I repeat again, they create a baseline. If you would suggest, though, that could more be done, I do, and I apologize. I don't remember the member's name. More research needs to be put into technology, number one, and it can be on any one of those three fronts. Prevention is the area that I suggest. Information sharing is a big piece of that, how we can be more collaborative and develop tools between government and industry to share and within industry, and so I would suggest where the management can be a major player is, they have access to information we don't and vice versa, and the idea is, how can we get that to be a timely sharing of information and a more detailed level of sharing of information. That's the area that I suggest that we put more emphasis on, not necessarily standards.

Mr. PALMER. Well, in regard to the timeliness, Mr. Stacey, in your testimony, you mentioned that intrusion detection technology is not well developed for control system networks and that it can often take months before malware is detected. What are the factors that account for such a significant amount of time that elapses before detection?

Mr. STACEY. Well, first, let me characterize, as Ms. Lee did, the difference between IT technology and OT. With IT technology, we're fairly mature now in proactively managing systems. We have configurations and patchings that we use to manage these systems.

Operational technology, or industrial control systems, may manage several hundreds or even thousands of points a minute, and if you try to proactively manage that network, you can do a denial-of-service attack on yourself. And so the tools today are basically passive monitoring—watching for things in and out—and the sophisticated hackers are aware of that and can go slow and low. And so the detection oftentimes, as I said, comes from a third party.

And this is another research area that could be invested in is the detection technology for industrial control systems. Thank you.

Mr. PALMER. Is that, in your opinion, where we need to go in terms of improving the detection time?

Mr. STACEY. Correct.

Mr. PALMER. Mr. Chairman, I yield the balance of my time.

Chairman WEBER. I thank the gentleman.

The gentleman from California is now recognized.

Mr. SWALWELL. Thank you, Mr. Chairman, and thank you to our panelists.

This issue, it just—it seems to evolve faster than we can stay pace with it, whether it's hacks or breaches that occur on the private sector side or hacks and breaches that we're seeing at OPM or other federal agencies that have, you know, certainly compromised millions of people's personal information, and so I guess my first question is, if one of our power grids went down tomorrow in a major metropolitan area because of a cyber attack, would anyone here be surprised? Just a yes or no up and down. Mr. Stacey, yes or no?

Mr. STACEY. It's certainly possible.

Mr. SWALWELL. But would you be surprised if it happened? If you learned tomorrow that, say, the San Francisco Bay area was out of power because of a cyber attack, would that surprise you?

Mr. STACEY. No.

Mr. SWALWELL. Mr. Gaines?

Mr. GAINES. Yes, it would.

Mr. SWALWELL. Ms. Lee?

Ms. LEE. Yes.

Mr. SWALWELL. And Mr. Wilshusen?

Mr. WILSHUSEN. Yes.

Mr. SWALWELL. Okay. And so for those who said—well, let me start with you, Mr. Stacey. Why would it not surprise you?

Mr. STACEY. I just believe—because our monitoring and detection for those kinds of events is not sophisticated enough for me to give an answer of yes.

Mr. SWALWELL. Do you believe that we have made the necessary investments across our country in protecting against cyber attacks, and not just the investments but is our workforce trained in a way that our cyber hygiene is good enough to prevent this from happening?

Mr. STACEY. Yes, I think we have invested properly. I think there's a lot of work being done both in the utility sector and within the government sector. I think we're short of staff certainly and we're working on that in a number of areas with universities, et cetera. But we've heard from several leaders within the federal government that we likely have people inside the infrastructure, and these are very complex systems and the complexity even independent of a malware attack, adds a level of vulnerability.

Mr. SWALWELL. Thank you.

And for the three who said they would be surprised if they learned tomorrow that a major metropolitan area had been hit, can you just maybe elaborate briefly on why it would surprise you? Mr. Gaines?

Mr. GAINES. I'll give you a fact-based answer.

Mr. SWALWELL. Sure.

Mr. GAINES. And I certainly know that there are vulnerabilities that exist in every network, but I would suggest to you at FirstEnergy, I feel we have done the right things to secure our company and that component of the grid.

The other thing that's unique to the grid is, we have the interconnects, in our case, PJM, and so in this case, we would work very hard with PJM given that if our company was breached, to minimize that impact across the network. Is it possible? Yes, but your black-and-white answer is, would I be surprised? Yes, I would be. And it's because of those two specific entities, and I would suggest to you the peers around me that are on PJM and the grid probably have the same level of confidence that their business, their company is secure also.

Mr. SWALWELL. Great. Thank you.

Ms. Lee?

Ms. LEE. Yes, I will agree completely with Mr. Gaines on that, and just add to that, if you look at—and it was referenced earlier the Metcalf attack, that their end result was no power failure. The reliability of the grid is paramount, and as he mentioned, working with the interconnections and the different utilities, the intent is to maintain the reliability of the grid. So yes, it is a hypothetical possibility but if you look at all that's in place to ensure the reliability, it still is a very stable system.

Mr. SWALWELL. And then can you tell me who you fear an attack would come from if it came—if it was—if it occurred? Do you think it would be a state actor or a non-state actor? Which one would be more likely based on your experience and what you've learned? Mr. Wilshusen?

Mr. WILSHUSEN. I think initially I would say it's probably going to be a non-state actor but I think also I've been reading where there could be state actors involved too. But certainly terrorists and groups that may wish to do us harm would do so. I think state actors are probably, depending on the state, also are relying on the electricity and our national economy to support them as well.

Mr. SWALWELL. And Mr. Gaines, are you cleared? Do you have a security clearance?

Mr. GAINES. I do have a security clearance.

Mr. SWALWELL. Do you feel that enough people in your company are cleared to work with the federal government on the threats or could we do a better job of bringing more people in?

Mr. GAINES. I don't think it's the volume; it's the quality. And I would suggest that today I have secret that it would be beneficial to move a smaller group to top secret, and the difference there is this, and it gets back to the timeliness and the level of detail, and for the sensitivity of my clearance, I just have to leave it at that, is that it would be much more beneficial to see things on a timely basis and at a much deeper level to be able to take action, but I feel at this point it's adequate but could be improved.

Mr. SWALWELL. Great. Thank you.

And Mr. Chair, I yield back.

Chairman WEBER. Well, thank you, and I appreciate your bringing that up.

Back to Mr. Stacey's lack of surprise at an attack, I was talking with the Ranking Member here, and it's kind of like a lot of terrorism. What is it we say, that we have to be 100 percent vigilant, diligent all the time; they have to be lucky one time.

So I now recognize the gentleman from Michigan, Mr. Moolenaar.

Mr. MOOLENAAR. Thank you, Mr. Chairman.

Mr. Gaines, I wanted to follow up with you one some of your comments. You had talked about the area of prevention and thinking about what we could do to complement the efforts you're doing in the industry, and you talked about, you know, prevention investments maybe could be—there could be benefits across industries. Can you describe that a little bit more?

Mr. GAINES. Across the industry?

Mr. MOOLENAAR. Across the industry.

Mr. GAINES. Across the industry itself?

Mr. MOOLENAAR. Yes.

Mr. GAINES. And I do have to come back to this issue, and I know it's uncomfortable maybe to repeat it again, but we do have in the industry a set of standards, and those standards hold us to a level, and if we're not compliant, then there's liability, and I think that has to be looked at first because there is the—there's not the lack of interest in wanting to be able to share from an industry but there's certainly a level of hesitancy at times at what level we share. So I remind us of that.

To that point, though, I don't think it can be done on a voluntary basis. I think that there has to be an open, collaborative environment between the government, and I speak of probably two or three agencies that I think we could all do a better job, and I start out with Homeland because they own the infrastructure. I start out with DOE because they are our sector control. Those are two. The third would be the FBI because they become the investigative arm in the event that something happens. I do believe that there is a way with the industry to be able to collaborate real-time threat analysis information, and it isn't a voluntary but rather a requirement that should occur, but it does start with the issue of our ability to be able to manage that directly industry to government.

Mr. MOOLENAAR. So it sounds to me like some of the effort, you're talking about people getting together in a room and meeting and discussing this. You aren't talking about major investments in infrastructure or some kind of——

Mr. GAINES. Both.

Mr. MOOLENAAR. —technology. You are talking about both?

Mr. GAINES. I am talking about both. I'm talking about the industry being able to have the necessary technology within their company to be able to provide that level of information, and I'm talking about the government being able to have and being a recipient and being able to use it, so it's technology and it's also skills and resources.

Mr. MOOLENAAR. And do you think that when you think about prevention, you know, you prevent one threat but that another threat emerges that you weren't aware of? How long are the benefits from that kind of an investment? You know, how long does that last?

Mr. GAINES. I think that's one of the things Ms. Lee talked about is that becomes a priority, where do we focus on first. I don't think you can deal with every single threat. There's a lot of work that's being done in the industry right now to define what a critical asset is, and it's very good work. The gentleman asked me, are the standards good. They're really good. They create baseline. I can tell you within our company, what are by definition the critical substations that have an impact on our entire network. Now, if I start there just alone with those critical assets and you multiply that times 120 investor-owned utilities, that's pretty valuable information. And so—and again, I don't want to give you any idea how many that is other than to say it is a manageable number.

Mr. MOOLENAAR. And just, it was mentioned earlier this idea of improving early detection, and I don't know if that was you, Mrs. Lee, or who it was that talked about the importance of that. Is that where we should be focusing?

Ms. LEE. I will add, I think early detection is important. One of the difficulties, and I believe it's been discussed here, is when you have an event, it can be very difficult to determine whether it's a cybersecurity event. I've done exercises with utilities and their frustration was, I didn't know it was a cybersecurity event. So it's a matter of, we talked about on the protection side but also as we've all discussed, using commercially available products. They have built-in vulnerabilities. The utilities are—as they're developing their mitigation strategies, you have to assume your systems at some point are going to be compromised, and so you take that as a given, maybe not significant but you use that when you develop your mitigation strategies. So I think it's a combination of looking at it from the protection side but then what do you do if there is a cybersecurity event. You want the electricity to continue to flow.

Mr. MOOLENAAR. Mr. Wilshusen?

Mr. WILSHUSEN. Yes, I would agree with that too because I know there's been a lot of discussion about the standards out there, and that's fine and they may be adequate, but what also needs to happen is the implementation of those standards consistently over time throughout the enterprise, and in our work at federal agencies and other entities, that often does not occur. Vulnerabilities exist because standards aren't being implemented consistently over time across the enterprise. And so it's through that that attacks often occur. So the aspect of monitoring the effectiveness of the security controls is also going to be a key part of the overall defense—in-depth strategy.

Mr. MOOLENAAR. Thank you, and thank you, Mr. Chairman. I yield back.

Chairman WEBER. The gentleman yields back.

I now recognize the gentleman from Louisiana, Dr. Abraham.

Mr. ABRAHAM. Thank you, Mr. Chairman.

Mr. Stacey, let me start with you at kind of the 30,000-foot view. If we have a full-scale cyber attack, what does it do to the nation's economy and to the nation's security infrastructure?

Mr. STACEY. It would be significant. All the other infrastructures run off the energy infrastructure.

Mr. ABRAHAM. And that leads me to the next question. How often is a cyber attack or an attempted attack tried on our nation's power grid?

Mr. STACEY. What I can tell you is that from ICS–CERT, they're seeing a 32 percent increase in fiscal year 2014 of target attacks on the energy sector. I don't have the specific number for the grid.

Mr. ABRAHAM. But it has increased in the last——

Mr. STACEY. It is increasing.

Mr. ABRAHAM. And I read something in USA Today that the U.S. power grid faces physical or online attacks approximately once every four days. Is that a fairly accurate statement?

Mr. STACEY. That's fair.

Mr. ABRAHAM. Okay. That's all, Mr. Chairman. I yield back.

Chairman WEBER. Thank you. The gentleman yields back.

The gentleman from Georgia, Mr. Loudermilk, is recognized.

Mr. LOUDERMILK. Thank you, Mr. Chairman, and I appreciate all of the witnesses being here. I apologize that I wasn't here for the earlier testimony but we also have Homeland Security issues going on. I'm doing the ping pong between the committees.

But prior to coming to Congress, I spent 30 years in the IT industry. Twenty of that time, I had my own business, and a good portion of our business was going into smaller utility systems and helping them automate. So I have some background in this, predominantly smaller municipal co-op systems to where we would put fiber optics into the city to tie the different SCADA systems together, pump stations, substations, et cetera, so they can more effectively monitor—getting more to a smart grid. During that time, many of those smaller operations saw the value of bringing in revenue, especially in small utilities, of selling the interconnectivity to businesses that had multiple locations within their jurisdiction. That also led to bringing in high-speed internet, which allowed them to connect and sell internet services on the same backbone or the same infrastructure that was also running their devices. Now, of course, we put in a lot of technology to segregate those networks, but at the same time, they also saw the functionality of being able to monitor and manage and respond without having to be in the office to an incident that happened within the utility system through the use of the internet.

So as we were trying to implement these new technologies to allow them to be more efficient in operating their utility, and many of those provide electricity throughout their cities or their area of responsibility, it did help a lot, but then there was the concern that we had of someone from the outside being able to get in. And so what we would do is, we would do a lot of research, and one of the things that we did not have was an approved products list that we could go to, that the government had said all right, if you use this type of gateway, use this firewall, use this type of filter, then we know it'll be secure. So we did a lot of research. We went to a lot of vendors and we would get what we believed was the most secure, put that into place, and in most cases we were under contract to maintain it and make sure the security updates were done, the patches, et cetera, et cetera.

The next progression was to then put in the other elements of the smart grid for meter reading and all this. So some of the things we started looking at were points of access, points of failure, points of vulnerability, which growed—which grew exponentially once we started adding the more technology.

In a previous committee, I brought up the lack of an approved products list that vendors such as myself or these smaller electric utilities can go to that has standards, equipment standards, standards of practice, operation, et cetera. Now, I understand the Department of Energy is working on that, and I applaud that effort. But I do believe, and I know that there is a lot of vulnerability accessing the grid, you may say, through smaller electric utility systems. Some of those that we put equipment in, we went out and spent a lot looking at security aspect of it to make sure that they could operate securely. Because of budget cuts, many of them would cut our contract and manage it themselves, and then some of them would actually go and buy parts off of eBay because they were cheaper, but I would try to emphasize to them, there's a reason that part is on eBay is probably because it has been discontinued for security reasons.

Can any of you that would like to comment on where we are, where we're going and if you feel that there is a need to have a standard set of standards for equipment, for upgrade, for maintenance, and operation with the smaller utilities as well as large.

Mr. GAINES. Well, I'll speak as a large utility. I can't speak for a small utility. That would not be accurate for me to do.

Mr. LOUDERMILK. You may be able to opine as far as how vulnerability of the small utilities affect the larger utility.

Mr. GAINES. Well, I'll try to answer your question directly, though, regarding standards associated with equipment, software technologies. I think there certainly has to be some level of verification, validation of equipment. To the extent that you could create a universal standards for every type of equipment that sits inside of a network, I think it would be very difficult, and the question is, who would monitor and manage that. That is the challenge, and it ranges from software to hardware. I do think there are some validation points, though, that you can put in. Do you have—are you building software or are you building equipment—a method of configuring it so that it could be personal to the company versus a standard set of passwords that are set in a piece of software, as an example. Those are things that you could do to design into the technology. As it relates to the vulnerability between a small utility, municipal or not, we work together very well in the industry between our industry association, EEI, groups like EPRI who do research for us, and so I would tell you that there's very little distinction about what the expectations are on a small utility versus a large utility.

Mr. STACEY. Thank you for the question. I'd offer this perspective. Right now, vendors are offering equipment with as much flexibility as they can, with as much functionality as they can. And that's adding to the complexity. If as a sector there was work done on how do I minimize the functionality to really what I need— that the valve only opens and closes as fast as I need for an emergency response, and that sensors on the pipe managing flow only have the fidelity for managing the flow, as we reduce that complexity, initially that would cost more because you're asking for something that's different, but as an industry, as they worked on reducing the complexity and trying to find components that did the minimum functionality required to manage within an industrial control system, I think there'd be some benefits to that.

Mr. LOUDERMILK. Is there currently a rating system or an evaluation that is used as far as how secure a utility is in their operation?

Mr. GAINES. In terms of vendor equipment?

Mr. LOUDERMILK. The whole footprint, the entire topology. Is there a method that some independent organization or the government can come in and evaluate and give some type of security rating?

Mr. GAINES. Yes, there is. The CIPS, the Critical Infrastructure Protection Standards, are a set of standards that originated in 2005. We're on version 5 right now. And they baseline the transmission system and the security around that through those standards and then they are auditable. And to the extent there is remediation associated with those audits, they're managed accordingly. FERC administers those through NERC.

Chairman WEBER. Does the gentleman yield back?

Mr. LOUDERMILK. I'm out of time, Mr. Chairman, so I will yield back the time I don't have remaining.

Chairman WEBER. All right. The gentleman yields.

Mr. Johnson, you're recognized.

Mr. JOHNSON. Thank you, Mr. Chairman, and I want to thank my colleagues on the Committee for allowing me to sit in on this today. It's an area of extreme interest and importance in my regard.

I spent nearly 30 years as an information technology professional, part of that time, a large part of that time, in the Department of Defense being concerned about the security of data systems that support our special opreations folks and things like that. I feel very, very strongly that cybersecurity is an issue across the spectrum. It's getting a lot of talk but it's not getting a lot of focused attention to address the issue. It's an issue—and I don't know if the four of you agree or not. It's not something that's got a finish line. You know, this is not something that we're going to solve and then we're going to move on to the next big problem. As long as the world is connected with computing systems and networks, you're going to have those with the wherewithal, some of them because they can, some of them because they desire to create chaos with malicious or criminal intent are going to try to get into our networks and our energy systems and our power grids are one of those areas that would wreak havoc on America's economy, and I think we can all agree with that.

Mr. Gaines, what in your mind does the integration of IT systems and supervisory control and data acquisition systems have in increasing the risk to grid operations?

Mr. GAINES. First of all, Mr. Johnson, hello. It's good seeing you again.

Mr. JOHNSON. Good to see you, sir.

Mr. GAINES. Thank you.

I would like to start out by saying I don't think it's if; it's when. The OT operational systems technologies and the IT technologies are merging and they go back to exactly what I suggested, that in a substation now, it looks like a small communications network. It's got a device in it that communicates with most of the assets, transformers, that determine the health and in fact the condition of those transformers. That's all communicated back to the SCADA system into the IT systems. Secondly, the IT systems are tied to our power grid and actually help us manage and monitor that from a generation perspective. I think the industry is moving to converge those, not necessarily manage them as you would manage them on the grid as an operator but manage that space so that one, they understand the health of it, they understand the reliability of it, and the impacts that cyber, specifically cyber, has on it.

I go back to the Metcalf incident. There were three things that occurred within an hour: the cutting of a communication line, the actual assault on the location itself, and then the loss of load. Those all three were done within an hour, and they were in the space that if you would've had monitoring and the ability to alert and manage that, I wouldn't suggest that you could avoid but you could have mitigated some of the issues.

Mr. JOHNSON. Can you talk specifically about what FirstEnergy is doing to mitigate this vulnerability?

Mr. GAINES. Yes. We in fact have over the past 12 months built a security operations center, and we manage all three of those from one center, so I manage the operations and the health of those physical assets. We look at that from an IT perspective and overlay IT to that, and then I physically monitor the station through cameras, video and X-ray. And so I see that single pane—as we define it, I single that single pane of our critical assets, and that's not dispersed around the company. I don't have a physical security desk, I don't have an operating center, and I don't have a cyber center. I have one operations center that looks at that, and they're not looking at it on multiple systems; they're looking at it on one system. We are one of the first in the industry. We've worked with EPRI very hard so the industry gets it, and there's a lot of work being done there.

Mr. JOHNSON. Okay. Well, thank you very much.

I had other questions but I think I've exhausted my time. Thank you, Mr. Chairman, for your indulgence.

Chairman WEBER. The gentleman yields back.

Well, I want to thank the witnesses for their valuable testimony and the Members for their questions. The record will remain open for two weeks for additional comments and written questions from Members.

This meeting is adjourned.

[Whereupon, at 11:40 a.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Brent Stacey

Statements of Mr. Brent Stacey, Associate Laboratory Director
National & Homeland Security, Idaho National Laboratory

Response to Questions Submitted for the Record by Committee Members
United States House of Representatives
Subcommittee on Energy
Joint With
Subcommittee on Research and Technology
Committee on Science, Space and Technology
October 21, 2015 Hearing "Cybersecurity for Power Systems"

The Honorable Randy Weber, Honorable Barbara Comstock, and Honorable Lamar Smith:

In addition to the written statement and discussion remarks provided to the United States House of Representatives Subcommittee on Energy and Subcommittee on Research and Technology, I am providing the following responses to the additional questions[1] submitted by the Subcommittees' as included in the Subcommittees' letter dated November 17, 2015:

Question 1. You reference 'air-gapped' systems and insist this is "not a security strategy." How could air-gapped ICS be vulnerable to cyber attacks?

Response to Question 1:

Kim Zetter, author of the Stuxnet book Countdown to Zero Day, defines 'air-gapping' as:

> *"...An air-gapped computer is one that is neither connected to the internet nor connected to other systems that are connected to the internet..."*

Within the context of this definition and the trends I discussed with the Subcommittees: 1) the word 'connected' includes both physical connections as well as wireless connectivity; and 2) the definition describes an ideal state at a single point in time. Air-gapping, when done properly, can be considered a tactic within good cybersecurity hygiene. Generally, while conducting cybersecurity assessments Idaho National Laboratory (INL) has experienced that air-gaps can be difficult to implement or maintain properly. Hence, I do not always assume an immediate position of confidence when a critical infrastructure stakeholder states that they have air-gapped their systems or networks. In practice, air-gapped systems, including industrial control systems, can fail when humans intentionally or inadvertently close the gap by transporting files via USB drives, CD-ROMS, laptops, internal databases, etc. I also have concerns regarding an air-gap's potential susceptibility to other methods for crossing air-gaps including tapping radio wave emanations via proximate cell phones, etc.

[1] Questions for the Record from The Honorable Lamar Smith (R-TX) U.S. House Committee on Science, Space, and Technology – Hearing "Cybersecurity for Power Systems," Tuesday November 17, 2015 "Questions for Mr. Brent Stacey", as enclosed with letter to Mr. Brent Stacey from Representative Randy Weber, Chairman Subcommittee on Energy Space and Technology and Representative Barbara Comstock Chairwoman Subcommittee on Research and Technology, November 17, 2015.

Question 1.a. How is this issue relevant specifically for nuclear power plants?

Response to Question 1.a:

"Air-gapping" is relevant to the nuclear industry in that "air-gapping" is one component that industry may continue as they upgrade from analog devices to digital systems. As a complementary security component, the nuclear industry also has been implementing 'one-way diodes' to protect their most critical digital assets (i.e., safety systems) as a means to separate nuclear systems from exposure to enterprise systems and the internet. I wish to emphasize that "air-gapping" and "one-way diodes" can be an effective tactic, with the understanding that these security components do not eliminate all vulnerabilities from the need to transfer data, upgrade software/firmware, and the supply chain. Additionally, any security program should include full-scale validation to avoid the introduction of additional vulnerabilities resulting from system interdependencies or complexity.

Question 2. In your testimony, you mention that information detection technology for industrial control systems is not "well developed." Is Idaho National Laboratory (INL) conducting any research and development to improve this technology? Please explain.

Response to Question 2:

INL is advancing the state-of-the-art in ICS cybersecurity detection with research and development in both near term solutions and longer term transformational technologies. Near term active R&D includes the "intelligent" modeling of normal control system network behaviors as a comparison for potentially differentiating malicious actions. In addition, INL is pursuing innovations in imitated networks called "honeypots," which trick attackers and provide early warning of attack. Long term transformational R&D includes sophisticated baselining of the operational characteristics of the power grid or typical production plant to recognize both malicious action and unexpected physical failure. This technology, which requires further development, was designed to notify operators of the impacted devices and automatically realign the ICS architecture to maintain operation or gracefully degrade, preventing cascading high consequence impacts. Beyond traditional ICS, INL also is targeting its expertise into the broad use of embedded control systems – with our initial explorations intended to minimize the vulnerabilities within transportation platforms. As a result of these initial efforts, INL has applied for a patent for an anomaly detection technology to protect a Controller Area Network Bus (CanBUS) which is the most prevalent control system architecture in vehicles. Electric vehicles are likely to become a large consumer or storage component of our future energy infrastructure. Beyond these technology innovations, INL has been actively involved in applying interdisciplinary teams and full-scale testing to discover and validate vulnerabilities from infrastructure interdependencies and evolving threats. As an example, we are evaluating cybersecurity vulnerabilities within the wireless communications systems that will be used within the Smart Grid and our Public Safety networks.

Question 3. Idaho National Laboratory works closely with the Department of Homeland Security on their Industrial Control System Cyber Emergency Response Team (ICS-CERT) program and Regional Resilience Assessment Program (RRAP). Can you provide some examples of work conducted at INL within these two programs?

Response to Question 3:

ICS-CERT: INL provides support for ICS-CERT in each of its eight functional areas, which include four operations functions and four risk reduction functions. ICS-CERT's operations functions include: incident response, vulnerability coordination, situational awareness, and technical analysis. Risk reduction functions include: cybersecurity assessments, training, distribution of Cyber Security Evaluation Tool (CSET), and Industrial Control Systems Joint Working Group (ICSJWG) activities. For these eight functions, INL personnel make up a large component of ICS-CERT's overall staff and hosts one of ICS-CERT's three watch floors. During FY 2015, INL personnel assisted ICS-CERT in: responding to the 295 cybersecurity incidents reported to ICS-CERT; coordinating 321 cybersecurity vulnerabilities; performing in-depth analysis on 175 malware samples; performing 99 onsite cybersecurity assessments, conducting multiple online, classroom, and regional training exercises; distribution of over 7,400 copies of CSET in 120 countries; and planning and conducting two successful ICSJWG meetings, in Washington, D.C., and Savannah, Georgia.

Regional Resiliency Assessment Program (RRAP): The DHS Regional Resiliency Assessment Program (RRAP) is a cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure. Each RRAP assessment is led by DHS and addresses a range of hazards that could have regionally and nationally significant consequences. Each year, DHS selects a set of voluntary and non-regulatory RRAP assessments with input and guidance from federal and state partners. These partnerships with federal, state, local, tribal, and territorial government officials are vital to the success of the RRAP process for engagement and information sharing. INL supports these RRAP assessments by providing subject matter experts and leveraging our unique capabilities within the following areas: data sciences and analytics; data integration and design; assessment methodology and tool development; critical infrastructure modeling and simulation; critical infrastructure dependencies and resilience; geospatial technologies and visualization; training and development; and risk/vulnerability assessments. Typically for an RRAP, INL will conduct preliminary research on the infrastructure systems within a project's focus areas; support stakeholder engagement; and perform data collection, aggregation, and analysis utilizing relevant infrastructure modeling capabilities and research tools. An RRAP assessment team can develop key findings of critical interdependencies, resilience options, and provide support for development of an integrated approach for day-to-day planning and preparedness activities for federal, state, local, and private/public sector stakeholders.

Question 4. INL conducts research and development for both DOE and DHS. How do the goals and challenges addressed by each agency correspond? Is there significant overlap between programs or are there gaps that need to be filled?

Response to Question 4:

In many cases there is significant beneficial overlap between programs within DOE and DHS. The U.S. recognized and expected this potential benefit when the Homeland Security Act of 2002 (Section 309) provided DHS with equal access to the DOE National Laboratory complex to support R&D efforts associated with Homeland Security challenges. A few examples of the significant overlap occur in inter-related missions and challenges for: critical infrastructure protection, nuclear/radiological threat protection and emergency response, science and technology research and development, etc. DOE's and DHS's shared interests and mission space with regards to the critical infrastructure protection mission are a result of DHS having the lead role for coordinating the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure and DOE serving as the Sector Specific Agency for the Energy Sector. Due to these multiple commonalities of mission and challenges, DOE and DHS R&D activities have mutually direct and/or indirect application for advancing the mission of both DOE and DHS, whether projects are funded by DOE and DHS. These cross organizational benefits represent opportunities for cost savings, joint investments, and broader impact for other government agencies. The agreements for mutual access to the National Laboratories provides a unique and immediate pathway for both DOE and DHS to respond, evolve, and structure R&D programs to address immediate challenges and when necessary forward-lean to address R&D gaps. For the latter, DOE and DHS leverage both the Laboratories' unique R&D capabilities and their leadership vision and strategy to advance the future of technology. A recent example at INL of how this inter-Department relationship is working is the leveraging of cybersecurity technical capabilities and information sharing methodologies resulting from

DHS projects into DOE cybersecurity R&D plans for the DOE Office of Nuclear Energy and the National Nuclear Security Administration Office of Defense Nuclear Nonproliferation.

Regarding research gaps, I see the most significant gap as an underinvestment in an integrated strategy for assuring that we have an effective control system cybersecurity R&D program and R&D infrastructure that will support future researcher needs for equipment, experimental laboratories, education curricula and operational training. The nation's current efforts focus heavily on the urgency of the moment, which can impact our ability to anticipate and prepare for future highly sophisticated, high consequence cyber events or develop transformational technology solutions that could reduce/eliminate ubiquitous vulnerabilities. Given that our world is becoming more digitally interconnected and that our cyber adversaries may be developing capabilities faster than we can mitigate vulnerabilities, we must make a commitment to develop and implement an integrated R&D strategy. In our role as a National Laboratory, INL has spearheaded discussions with DOE, DHS, Department of Defense and other federal agencies and laboratories to define a framework for an integrated strategy.

Question 5. In your prepared testimony, you mention the 2006 Department of Homeland Security's (DHS) Aurora project test. Can you provide an overview of the significance of this test, and what conclusions were made about the vulnerability of power systems to cyber and physical attacks?

Response to Question 5:

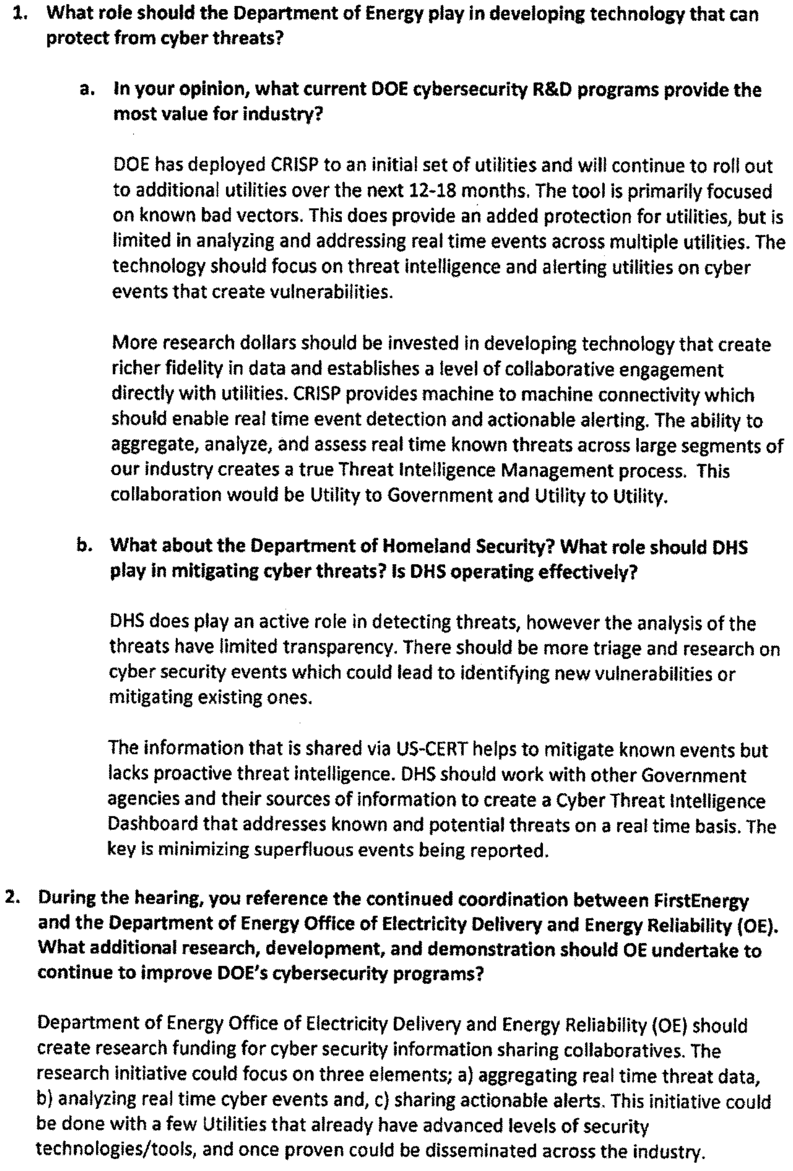
The pilot test conducted in 2006 along with the full-scale Aurora test in 2007 were significant to the Nation in demonstrating physical disruptions to components of critical infrastructure can occur from cyber means. Previous to these tests, there was much uncertainty about the credibility of the vulnerability and consequences due to both the specific Aurora vulnerability and to the prevalence of potential cyber-physical vulnerabilities within our critical infrastructure. The Aurora project, solely focused on proving that a specific vulnerability was real, had some lasting influence – this project proved the effectiveness of a scientific approach that the Nation can use to resolve uncertainty about the credibility and consequences of a potential cyber-physical threat. This approach involves: 1) integrating experts across multiple fields of science and engineering research, intelligence/threat analysts, infrastructure operators, and policy officials to define the technical challenge and experimental plan; 2) modeling and simulating (M&S) the threat against infrastructure systems to establish the bounds of the threat and consequences; and 3) conducting full-scale demonstrations against realistic infrastructure both to refine the M&S results and establish priorities for mitigation actions. For power systems, INL has utilized this approach in recent demonstrations conducted to understand the effects of geomagnetic disturbance (GMD) events on power grid substations and prove the effectiveness of a proprietary protective solution to ballistic attack against transformers. With the DOE Office of Electricity Delivery and Energy Reliability, INL is preparing our power grid test bed for future tests of cybersecurity protection technologies for Smart Grid technologies utilizing wireless communications.

Question 5.a. What Steps were taken following this exercise to address areas of vulnerability?

Response to Question 5.a:

After the Aurora project demonstration, funded by DHS, the North American Electric Reliability Corporation was able to direct utilities in mitigating the specific Aurora vulnerability.

Responses by Mr. Bennett Gaines



1. **What role should the Department of Energy play in developing technology that can protect from cyber threats?**

   a. **In your opinion, what current DOE cybersecurity R&D programs provide the most value for industry?**

   DOE has deployed CRISP to an initial set of utilities and will continue to roll out to additional utilities over the next 12-18 months. The tool is primarily focused on known bad vectors. This does provide an added protection for utilities, but is limited in analyzing and addressing real time events across multiple utilities. The technology should focus on threat intelligence and alerting utilities on cyber events that create vulnerabilities.

   More research dollars should be invested in developing technology that create richer fidelity in data and establishes a level of collaborative engagement directly with utilities. CRISP provides machine to machine connectivity which should enable real time event detection and actionable alerting. The ability to aggregate, analyze, and assess real time known threats across large segments of our industry creates a true Threat Intelligence Management process. This collaboration would be Utility to Government and Utility to Utility.

   b. **What about the Department of Homeland Security? What role should DHS play in mitigating cyber threats? Is DHS operating effectively?**

   DHS does play an active role in detecting threats, however the analysis of the threats have limited transparency. There should be more triage and research on cyber security events which could lead to identifying new vulnerabilities or mitigating existing ones.

   The information that is shared via US-CERT helps to mitigate known events but lacks proactive threat intelligence. DHS should work with other Government agencies and their sources of information to create a Cyber Threat Intelligence Dashboard that addresses known and potential threats on a real time basis. The key is minimizing superfluous events being reported.

2. **During the hearing, you reference the continued coordination between FirstEnergy and the Department of Energy Office of Electricity Delivery and Energy Reliability (OE). What additional research, development, and demonstration should OE undertake to continue to improve DOE's cybersecurity programs?**

   Department of Energy Office of Electricity Delivery and Energy Reliability (OE) should create research funding for cyber security information sharing collaboratives. The research initiative could focus on three elements; a) aggregating real time threat data, b) analyzing real time cyber events and, c) sharing actionable alerts. This initiative could be done with a few Utilities that already have advanced levels of security technologies/tools, and once proven could be disseminated across the industry.

3. **What role does smart grid technology play in creating cyber vulnerabilities? Does the fact that smart grid technology relies on two-way communication make the grid more susceptible to cyber attacks as this technology is integrated?**

   The right design and architecture, along with necessary security technologies, should minimize or eliminate vulnerabilities to a smart grid deployment. Two-way communication does create a risk in any network design, however the necessary steps are being taken to eliminate cyber security vulnerabilities. The key is properly deploying security systems around and within the network.

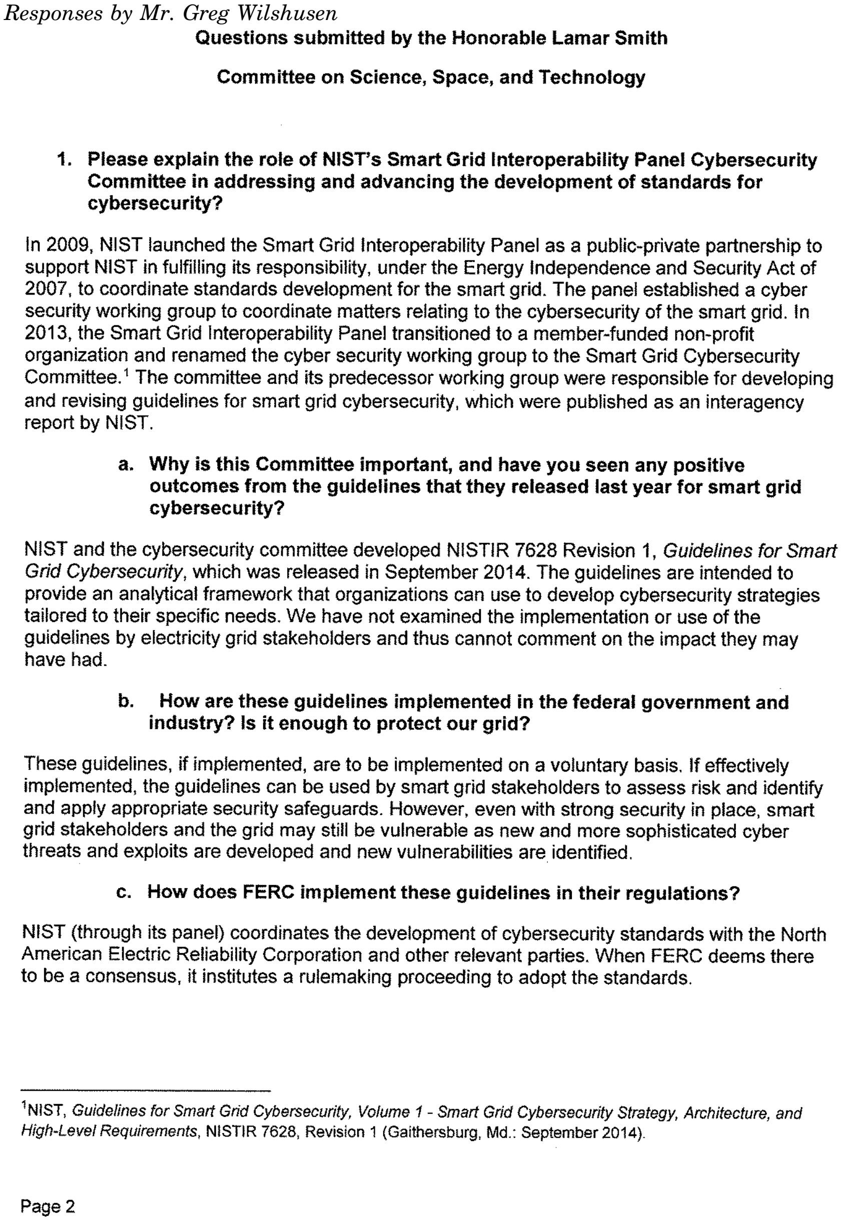
   a. **What research and development is necessary to improve security of smart grid systems?**

      More research and development should be done on data analytics as smart grid technologies continue to be deployed by utilities. Situational awareness is imperative with the increased amount of data that is transacted.

4. **Does FirstEnergy employ any coordinated security operations techniques, such as an Integrated Security Operations Center (ISOC)? Why or why not?**

   Yes. In the pursuit of developing a Threat Intelligence Management System it was necessary to create an integrated approach to security operations. FirstEnergy has been an early adopter of integrated cyber security, physical security, and operational technologies.

Responses by Mr. Greg Wilshusen



Questions submitted by the Honorable Lamar Smith

Committee on Science, Space, and Technology

1. **Please explain the role of NIST's Smart Grid Interoperability Panel Cybersecurity Committee in addressing and advancing the development of standards for cybersecurity?**

In 2009, NIST launched the Smart Grid Interoperability Panel as a public-private partnership to support NIST in fulfilling its responsibility, under the Energy Independence and Security Act of 2007, to coordinate standards development for the smart grid. The panel established a cyber security working group to coordinate matters relating to the cybersecurity of the smart grid. In 2013, the Smart Grid Interoperability Panel transitioned to a member-funded non-profit organization and renamed the cyber security working group to the Smart Grid Cybersecurity Committee.[1] The committee and its predecessor working group were responsible for developing and revising guidelines for smart grid cybersecurity, which were published as an interagency report by NIST.

a. **Why is this Committee important, and have you seen any positive outcomes from the guidelines that they released last year for smart grid cybersecurity?**

NIST and the cybersecurity committee developed NISTIR 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity*, which was released in September 2014. The guidelines are intended to provide an analytical framework that organizations can use to develop cybersecurity strategies tailored to their specific needs. We have not examined the implementation or use of the guidelines by electricity grid stakeholders and thus cannot comment on the impact they may have had.

b. **How are these guidelines implemented in the federal government and industry? Is it enough to protect our grid?**

These guidelines, if implemented, are to be implemented on a voluntary basis. If effectively implemented, the guidelines can be used by smart grid stakeholders to assess risk and identify and apply appropriate security safeguards. However, even with strong security in place, smart grid stakeholders and the grid may still be vulnerable as new and more sophisticated cyber threats and exploits are developed and new vulnerabilities are identified.

c. **How does FERC implement these guidelines in their regulations?**

NIST (through its panel) coordinates the development of cybersecurity standards with the North American Electric Reliability Corporation and other relevant parties. When FERC deems there to be a consensus, it institutes a rulemaking proceeding to adopt the standards.

[1] NIST, *Guidelines for Smart Grid Cybersecurity, Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*, NISTIR 7628, Revision 1 (Gaithersburg, Md.: September 2014).

d. How do these guidelines lead us to a more resilient grid?

If electricity grid stakeholders effectively implement the guidelines, they would be in a better position to prevent, or detect and respond to, security incidents in a manner that reduces their impact and increases grid resiliency.

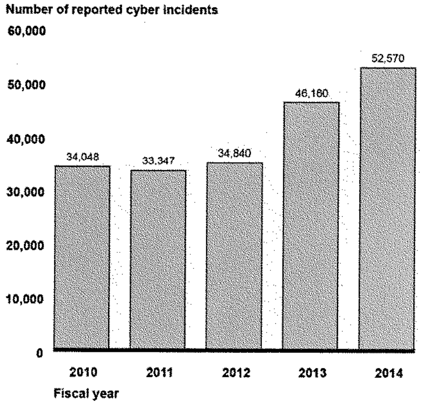
2. **You have authored a number of reports at GAO about cybersecurity deficiencies across the federal government. What is the next possible hack that we should be worried about – is it the grid? What keeps you up at night as the next potential cybersecurity failure in the federal government?**

It is difficult to predict the next hack or cybersecurity failure with certainty, in part because our cyber adversaries are becoming increasingly sophisticated and our nation and the federal government have a large cyber-attack surface. Clearly, a successful attack on the electricity grid that results in widespread outages could have a catastrophic effect because of the dependencies of other critical infrastructures on the grid. Other worrisome scenarios are successful cyber intrusions into our military's command and control systems and systems supporting our nation's financial markets. Any of these scenarios could impair our national security and economy.

3. **Can you quantify the increase in cyber activity targeting U.S. computers and systems over the past few years?**

As the following figure indicates, the number of cyber incidents reported by federal agencies has increased over the past 4 years, rising from 34,048 in fiscal year 2010 to 52,570 in fiscal year 2014, an increase of about 54 percent.

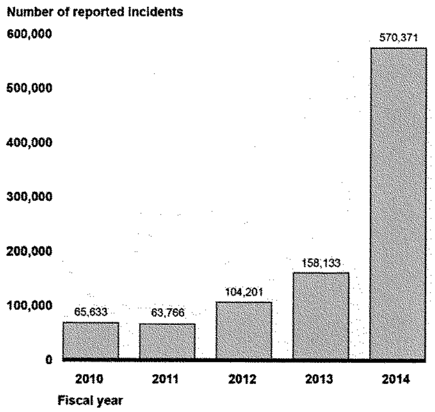
Figure 1: Cyber Incidents Reported to US-CERT by Federal Agencies: Fiscal Years 2010-2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2010-2014.

The number of information security incidents reported by non-federal entities has recently spiked. In fiscal year 2010, non-federal entities reported 65,033 incidents and in fiscal year 2014 reported 570,371, an increase of about 777 percent. The number of actual security incidents incurred by non-federal entities is almost certainly understated since reporting by non-federal entities is voluntary and many such entities likely do not report.

Figure 2 : Total Incidents Reported to US-CERT by Non-Federal Entities: Fiscal Years 2010-2014



Source: GAO analysis of Office of Management and Budget and United States Computer Emergency Readiness Team data for fiscal years 2010-2014.

4. **Does the increasing interconnectivity of the grid make it more vulnerable? Why or why not?**

As we have previously reported,[2] the electric power industry is increasingly incorporating information and communications technologies into its existing infrastructure. The use of these technologies can provide many benefits, such as greater efficiency and lower costs to consumers. However, if not securely implemented, the increasing interconnectivity of industrial control systems and supervisory control and data acquisition (or SCADA) systems that support the electricity grid with external networks and information systems also creates opportunities for attackers to disrupt critical services, including electrical power. The increased reliance on IT systems and networks also exposes the grid to potential and known cybersecurity vulnerabilities including:

- an increased number of entry points and paths that can be exploited by potential adversaries and other unauthorized users;

[2] GAO, *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention*, GAO-16-174T (Washington, D.C.: Oct. 21, 2015) and *Cybersecurity; Challenges in Securing the Electricity Grid*, GAO-12-926T (Washington, D.C.: July 17, 2012).

- the introduction of new, unknown vulnerabilities due to an increased use of new networking and system technologies;
- wider access to systems and networks due to increased interconnectivity; and
- an increased amount of customer information being collected and transmitted, providing incentives for adversaries to attack these systems and potentially putting private information at risk of unauthorized disclosure and use.

a. What are the potential downsides and consequences of this interconnectivity?

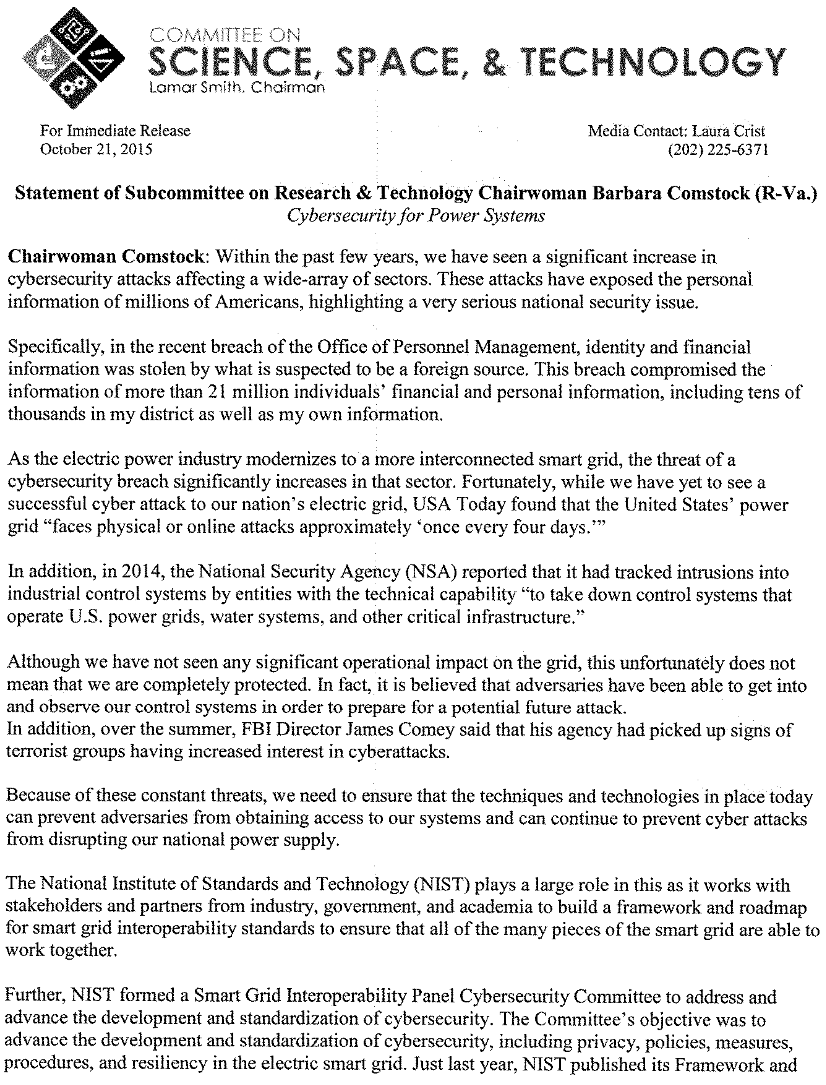
Exploitation of these and other vulnerabilities through the increased interconnectivity can have significant consequences for the electricity grid. For example, as we previously reported,[3] cybersecurity experts have demonstrated that certain smart meters can be successfully attacked, possibly resulting in disruption to the grid. Control systems used in industrial settings such as electricity generation have vulnerabilities that could result in serious damage and disruption if exploited. One experiment known as "Aurora" demonstrated that an unauthorized user could remotely control, misuse, and cause physical damage to a small commercial electric generator. Stuxnet, a sophisticated computer attack, targeted control systems used to operate industrial processes in the energy, nuclear, and other critical sectors. It was designed to exploit a number of vulnerabilities to gain access to its target and modify code to change the process. In 2008, the Central Intelligence Agency reported that malicious activities against IT systems and networks have caused disruption of electrical power capabilities in multiple regions overseas, including a case that resulted in a multi-city power outage.

[3] GAO-16-174T and GAO-12-926T.

Appendix II

Additional Material for the Record

STATEMENT SUBMITTED BY SUBCOMMITTEE CHAIRWOMAN BARBATA COMSTOCK



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
October 21, 2015

Media Contact: Laura Crist
(202) 225-6371

Statement of Subcommittee on Research & Technology Chairwoman Barbara Comstock (R-Va.)
Cybersecurity for Power Systems

Chairwoman Comstock: Within the past few years, we have seen a significant increase in cybersecurity attacks affecting a wide-array of sectors. These attacks have exposed the personal information of millions of Americans, highlighting a very serious national security issue.

Specifically, in the recent breach of the Office of Personnel Management, identity and financial information was stolen by what is suspected to be a foreign source. This breach compromised the information of more than 21 million individuals' financial and personal information, including tens of thousands in my district as well as my own information.

As the electric power industry modernizes to a more interconnected smart grid, the threat of a cybersecurity breach significantly increases in that sector. Fortunately, while we have yet to see a successful cyber attack to our nation's electric grid, USA Today found that the United States' power grid "faces physical or online attacks approximately 'once every four days.'"

In addition, in 2014, the National Security Agency (NSA) reported that it had tracked intrusions into industrial control systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems, and other critical infrastructure."

Although we have not seen any significant operational impact on the grid, this unfortunately does not mean that we are completely protected. In fact, it is believed that adversaries have been able to get into and observe our control systems in order to prepare for a potential future attack.
In addition, over the summer, FBI Director James Comey said that his agency had picked up signs of terrorist groups having increased interest in cyberattacks.

Because of these constant threats, we need to ensure that the techniques and technologies in place today can prevent adversaries from obtaining access to our systems and can continue to prevent cyber attacks from disrupting our national power supply.

The National Institute of Standards and Technology (NIST) plays a large role in this as it works with stakeholders and partners from industry, government, and academia to build a framework and roadmap for smart grid interoperability standards to ensure that all of the many pieces of the smart grid are able to work together.

Further, NIST formed a Smart Grid Interoperability Panel Cybersecurity Committee to address and advance the development and standardization of cybersecurity. The Committee's objective was to advance the development and standardization of cybersecurity, including privacy, policies, measures, procedures, and resiliency in the electric smart grid. Just last year, NIST published its Framework and

Roadmap for Smart Grid Interoperability Standards, Release 3.0, around the same time that it made revisions to its guidelines for smart grid cybersecurity.

I am interested in learning about how the NIST guidelines for smart grid cybersecurity are implemented in government and industry and how they contribute to a more resilient grid. In addition, I am looking forward to hearing about the technologies and techniques that are being developed and used in order to protect our nation from a massive attack to our control systems.

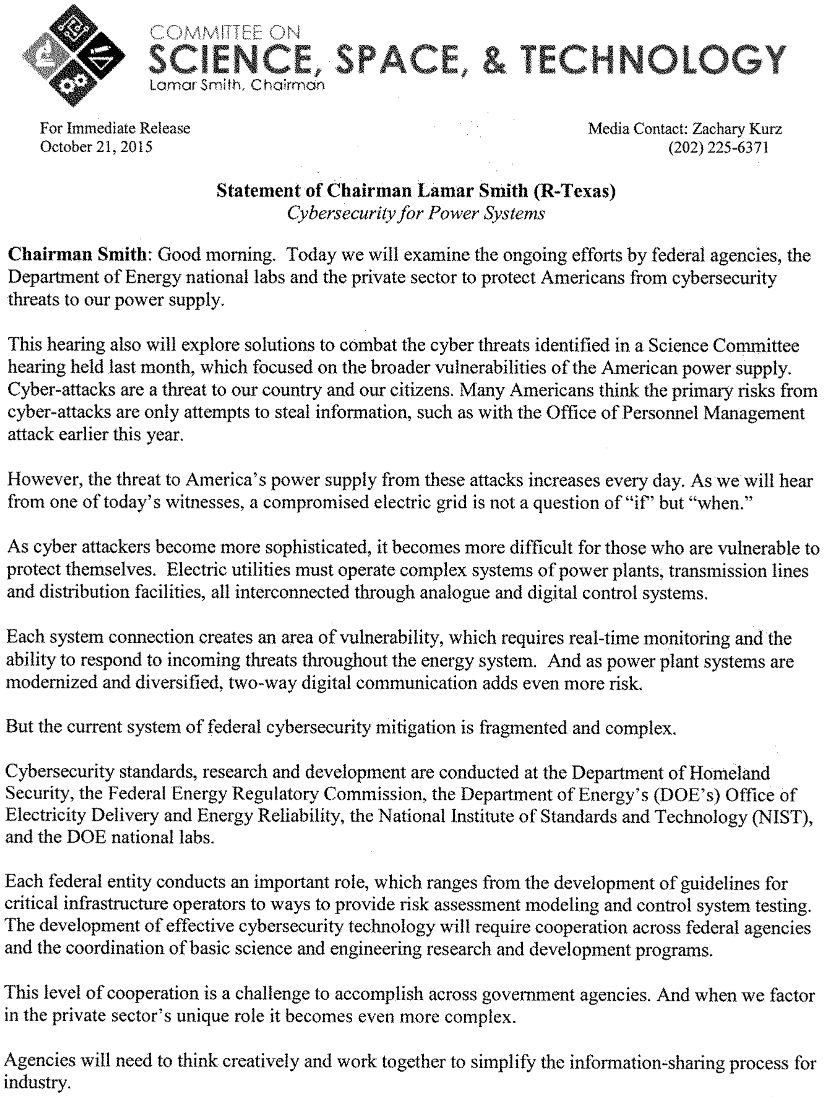
As someone who was personally affected by the OPM breach, which occurred despite years of warnings from the OPM Office of Inspector General and the U.S. Government Accountability Office to OPM leadership about critical vulnerabilities to their information systems, I know firsthand that we cannot ignore any kind of cybersecurity threats and vulnerabilities.

The fact that we know of adversaries who have been able to get into and observe our systems highlights the need to be proactive in protecting our grid to prevent such bad actors from being capable of taking down our control systems.

I look forward to today's hearing and thank our witnesses for being here. It is clear that there are many threats to our critical infrastructure, and we must ensure that our federal systems are adequately protected, especially as we transition to the Smart Grid.

Continuing to evolve our technologies and standards in order to mitigate these vulnerabilities and their potential consequences is ultimately essential for the safety and security of all Americans.

Statement submitted by Chairman Lamar Smith



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
October 21, 2015

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)
Cybersecurity for Power Systems

Chairman Smith: Good morning. Today we will examine the ongoing efforts by federal agencies, the Department of Energy national labs and the private sector to protect Americans from cybersecurity threats to our power supply.

This hearing also will explore solutions to combat the cyber threats identified in a Science Committee hearing held last month, which focused on the broader vulnerabilities of the American power supply. Cyber-attacks are a threat to our country and our citizens. Many Americans think the primary risks from cyber-attacks are only attempts to steal information, such as with the Office of Personnel Management attack earlier this year.

However, the threat to America's power supply from these attacks increases every day. As we will hear from one of today's witnesses, a compromised electric grid is not a question of "if" but "when."

As cyber attackers become more sophisticated, it becomes more difficult for those who are vulnerable to protect themselves. Electric utilities must operate complex systems of power plants, transmission lines and distribution facilities, all interconnected through analogue and digital control systems.

Each system connection creates an area of vulnerability, which requires real-time monitoring and the ability to respond to incoming threats throughout the energy system. And as power plant systems are modernized and diversified, two-way digital communication adds even more risk.

But the current system of federal cybersecurity mitigation is fragmented and complex.

Cybersecurity standards, research and development are conducted at the Department of Homeland Security, the Federal Energy Regulatory Commission, the Department of Energy's (DOE's) Office of Electricity Delivery and Energy Reliability, the National Institute of Standards and Technology (NIST), and the DOE national labs.

Each federal entity conducts an important role, which ranges from the development of guidelines for critical infrastructure operators to ways to provide risk assessment modeling and control system testing. The development of effective cybersecurity technology will require cooperation across federal agencies and the coordination of basic science and engineering research and development programs.

This level of cooperation is a challenge to accomplish across government agencies. And when we factor in the private sector's unique role it becomes even more complex.

Agencies will need to think creatively and work together to simplify the information-sharing process for industry.

If the system of federal guidelines and regulations is too complex, industry will not be able to effectively use monitoring and information-sharing networks established by federal agencies. The Department of Energy, NIST, and the Department of Homeland Security cannot effectively protect the electric grid without interagency cooperation.

I thank our witnesses today for their efforts to protect our critical infrastructure. I look forward to hearing how federal agencies can work with industry to secure the electric grid and what role Congress should play in the direction and oversight of this complex process.

Affordable, reliable power is the foundation of the American economy. Federal research and development that leads to ways to secure our power supply from cyber-attacks should be a priority, particularly through cooperation between the national labs and industry.

We must develop smart technology that can protect consumer data and keep our electric grid secure.

Statement submitted by Ranking Member Eddie Bernice Johnson

OPENING STATEMENT

RANKING MEMBER
EDDIE BERNICE JOHNSON (D-TX)
"Cybersecurity for Power Systems"
October 21, 2015

Thank you, Mr. Chairman, for holding this timely and important hearing on the cybersecurity of our nation's electric grid.

Our aging energy infrastructure is certainly in need of significant upgrades if we hope to have a reliable and resilient power supply in the decades ahead. One of the most notable upgrades would introduce what are called smart grid technologies to the electric grid. Allowing this two-way communication between consumers and operators in the management of our electricity supply could have a major impact on increasing the efficiency and resiliency of the entire system.

Major technological advancements like the smart grid come with a variety of challenges and concerns that must be addressed as new innovations like this are introduced into the market. Cybersecurity may be the most notable challenge facing the long-term implementation of these technologies.

If an entire system is interconnected and can respond more quickly to problems, as smart grids aim to do, then it also has the potential to be more quickly taken down by a malicious actor. As we will hear from our witnesses today, another basic challenge arises when combining information technology, or IT, with operational systems. IT cybersecurity solutions and safeguards cannot be used in operational technology without modification, and we must be mindful of this when planning for the future. While this is not a new challenge, it is certainly a difficult one.

However, none of these challenges should delay progress in creating a more efficient and reliable electric grid. We need to invest in cybersecurity research. We must foster productive relationships between the federal government, utilities, operators, vendors, and state and local governments. And we must ensure that any advancements in our power supply properly prioritize cybersecurity at every step.

Thank you again Mr. Chairman for holding this hearing. I look forward to hearing the testimony from our witnesses. I yield back the balance of my time.