CRITICAL INFRASTRUCTURE CYBERSECURITY: ASSESSMENTS OF SMART GRID SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

FEBRUARY 28, 2012

Serial No. 112–120

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

76–641 PDF WASHINGTON : 2013

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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

CLIFF STEARNS, Florida
Chairman

LEE TERRY, Nebraska
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
CORY GARDNER, Colorado
H. MORGAN GRIFFITH, Virginia
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

DIANA DEGETTE, Colorado
Ranking Member
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
KATHY CASTOR, Florida
EDWARD J. MARKEY, Massachusetts
GENE GREEN, Texas
DONNA M. CHRISTENSEN, Virgin Islands
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

[1] Mr. Trimble did not offer oral remarks for the record. Mr. Trimble and Mr. Wilshusen submitted a joint statement.

CRITICAL INFRASTRUCTURE CYBERSECURITY: ASSESSMENTS OF SMART GRID SECURITY

TUESDAY, FEBRUARY 28, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:19 a.m., in room 2322 of the Rayburn House Office Building, Hon. Cliff Stearns (chairman of the subcommittee) presiding.

Members present: Representatives Stearns, Terry, Myrick, Burgess, Blackburn, Gingrey, DeGette, and Waxman (ex officio).

Staff present: Carl Anderson, Counsel, Oversight and Investigations; Todd Harrison, Chief Counsel, Oversight and Investigations; Katie Novaria, Legislative Clerk; Andrew Powaleny, Deputy Press Secretary; Alvin Banks, Democratic Investigator; Brian Cohen, Democratic Investigations Staff Director and Senior Policy Advisor; and Kiren Gopal, Democratic Counsel.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Good morning, everybody. I call the subcommittee's second hearing on cybersecurity and critical infrastructure protection to order.

My colleagues, America's infrastructure systems have become more automated and more reliant on information systems and computer networks to operate. While our systems are more efficient, they also open the door to cyber threats and cyber-attacks. Today, the subcommittee focuses on that part of the critical infrastructure known as smart grid, which refers to the information technology systems increasingly incorporated into the Nation's electricity networks.

Smart grid technologies are designed to lower operation costs, reduce maintenance costs, and expand the flexibility of operational control relative to the current grid system. Their operational efficiency and improved asset use is driven by advanced communication and information technologies.

I believe that we must update our electric grid with better technology integration, which is why I spearheaded the effort to secure funding for Energy Smart Florida, the largest smart grid demonstration project in the country. This initiative will invest hundreds of millions of dollars in smart grid technology and renewable

energy in Florida and throughout the entire county. Energy Smart Florida will revolutionize how people use energy in their homes and enable them to make smarter choices about energy consumption and better control their carbon emissions. In addition, the widespread deployment of smart meters will provide Floridians with more reliable electrical service through an intelligent network that will be able to detect potential problems and automatically reconfigure the grid to minimize or eliminate outages.

But ask any expert in the national security field and see what keeps them up at night. They would probably tell you, as they tell me, that it is the increased possibility of a devastating cyber-attack. This threat is real and is why it is virtually important—vitally important for us to do what we can to protect our critical infrastructure from these threats. We have seen in the past decade what impact both man-made and natural disasters have on our Nation's utility systems. Imagine the impact of a cyber-attack to the electrical grid. How many days could hospitals operate with onsite electric generation? How would metro rail systems operate, if at all? How would we recharge our smart phones or access the internet? The goal of the smart grid is to improve efficiency, reliability and interoperability. An equal goal, however, must be to improve upon the security controls and to minimize the impact from a man-made or natural disaster to ensure reliability and avoid such possibilities.

Now, a recent report completed by the Pike Research company estimated that utilities' initiatives to secure their infrastructure will drive increasing investments to involve cybersecurity systems and total roughly $14 billion from now through the year 2018. While the Department of Energy has emphasized investment in technologies such as smart meters, among other technologies, we want to ensure that where there is investment, there is not a cybersecurity gap. We want to emphasize that there is also investment in securing control system segments including transmission upgrades, substation automation, and distribution automation systems.

Protecting critical infrastructure is a complicated issue. We are talking about facilities and frameworks owned by private companies, and by Federal, State, and local governments. They are interconnected. Electricity powers water systems that cool nuclear reactors, for example. They are vulnerable to threats from a number of different sources, including nation-states, criminals, and hackers.

The issues surrounding critical infrastructure protection and security are complex. To help analyze these complexities, I am pleased to be joined by our panel of experts in the field. Today, we will hear testimony from two witnesses at GAO: Mr. Gregory Wilshusen, Director of Information Security Systems, and Mr. David Trimble, Director of Natural Resources and the Environment. I look forward to their testimony, and getting a better understanding of their extensive work examining cybersecurity implications of the smart grid. I also would like to welcome Mr. Richard Campbell, of the Congressional Research Service, who has examined this very subject and we look forward to his contributions today.

My colleagues, as I mentioned previously, this is the subcommittee's second hearing in this Congress on critical infrastructure protection and cybersecurity. The purpose of this hearing, in particular, is to get an overview of smart grid cybersecurity, and how it is working and what can be done better. It is my intention to call the Department of Energy and possibly other stakeholders to a future hearing for further consideration of smart grid security.

I have enjoyed working with the Ranking Member, Ms. DeGette and the Minority in these matters and look forward to working with them on overseeing cybersecurity issues again. So I look forward to this hearing, the perspectives of our expert witnesses about the safety of this vital part of critical infrastructure, and whether we are taking the right steps to protect them from cybersecurity risks and threats.

[The prepared statement of Mr. Stearns follows:]

Statement of the Honorable Cliff Stearns
Committee on Energy and Commerce
Chairman, Subcommittee on Oversight and Investigations
Hearing on "Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security"
February 28, 2012

(As Prepared for Delivery)

I call to order this subcommittee's second hearing on cybersecurity and critical infrastructure protection.

America's infrastructure systems have become more automated and more reliant on information systems and computer networks to operate. While our systems are more efficient, they also open the door to cyber threats and cyber-attacks. Today, the subcommittee focuses on that part of the critical infrastructure known as Smart Grid, which refers to the information technology systems increasingly incorporated into the nation's electricity networks.

Smart grid technologies are designed to lower operation costs, reduce maintenance costs, and expand the flexibility of operational control relative to the current grid system. Their operational efficiency and improved asset use is driven by advanced communication and information technologies.

I believe that we must update our electric grid with better technology integration, which is why I spearheaded the effort to secure funding for Energy Smart Florida, the largest smart grid demonstration project in the country. This initiative will invest hundreds of millions in smart grid technology and renewable energy in Florida and throughout the entire county. Energy Smart Florida will revolutionize how people use energy in their homes and enable them to make smarter choices about energy consumption and better control their carbon emissions. In addition, the widespread deployment of smart meters will provide Floridians with more reliable electrical service through an intelligent network that will be able to detect potential problems and automatically reconfigure the grid to minimize or eliminate outages.

But ask any expert in the national security field and see what keeps them up at night. They would probably tell you, as they tell me, that it is the increased possibility of a devastating cyber-attack. This threat is real and is why it is vitally important for us to do what we can to protect our critical infrastructure from these threats. We have seen in the past decade what impact both man-made and natural disasters have on our nation's utility systems. Imagine the impact of a cyber-attack to the electrical grid: How many days could hospitals operate with on-site electricity generation? How would metro rail systems operate if at all? How would we recharge our smart phones or access the internet? The goal of the Smart Grid is to improve efficiency, reliability and interoperability. An equal goal however, must be to improve upon the security controls and to minimize the impact from a man-made or natural disaster to ensure reliability and avoid such possibilities.

A recent report completed by Pike Research, estimated that utilities' initiatives to secure their infrastructure will drive increasing investments in cybersecurity systems and total roughly $14 billion from now through 2018. While DOE has emphasized investment in technologies such as smart meters, among other technologies, we want to ensure that where there is investment, there is not a cybersecurity gap. We want to emphasize that there is also investment in securing control system segments including transmission upgrades, substation automation, and distribution automation systems.

Protecting critical infrastructure is a complicated issue. We are talking about facilities and frameworks owned by private companies, and by federal, state, and local governments. They are interconnected — electricity powers water systems that cool nuclear reactors, for example. They are vulnerable to threats from a number of different sources, including nation-states, criminals, and hackers.

The issues surrounding critical infrastructure protection and security are complex. To help analyze these complexities, I am pleased to be joined by our panel of experts in their field.

Today, we will hear testimony from two witnesses at GAO: Mr. Gregory Wilshusen, Director of Information Security Issues, and Mr. David Trimble, Director of Natural Resources and the Environment. I look forward to their testimony, and getting a better understanding of their extensive work examining cybersecurity implications of the Smart Grid. I also would like to welcome Mr. Richard Campbell, of the Congressional Research Service, who has examined this very subject and we look forward to his contributions today.

As I mentioned previously, this is the Subcommittee's second hearing in this Congress on critical infrastructure protection and cybersecurity. The purpose of this hearing, in particular, is to get an overview of Smart Grid cybersecurity, and how it is working and what can be done better. It is my intention to call DOE and possibly other stakeholders to a future hearing for further consideration of Smart Grid security.

I have enjoyed working with Ranking Member DeGette and the Minority in these matters and look forward to working with her on overseeing cybersecurity issues.

I look forward to hearing the perspectives of our expert witnesses about the safety of this vital part of critical infrastructure, and whether we are taking the right steps to protect them from cyber risks and threats.

Mr. STEARNS. And with that, I recognize the ranking member, Ms. DeGette.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you very much, Mr. Chairman, for holding this hearing on smart grid cybersecurity.

Last year in July, representatives of the Department of Homeland Security came before this subcommittee to discuss their efforts to protect and deploy Federal resources and to coordinate with the private sector to prevent and respond to cyber attacks. This hearing, as you mentioned, is an important follow-up to that hearing.

Protecting our critical infrastructure from cyber attacks is, of course, of vital importance. As our electric grid evolves, we become more and more dependent on so-called smart technologies to control, connect, and maintain this interconnected system. This is a good thing. It will make the grid more efficient and more reliable. For example, consumers will soon be able to track the price of electricity minute by minute and adjust electricity use accordingly, waiting, for example, until prices are right to do the laundry or start the dishwasher.

However, these investments also expose us to new threats. These new technologies can be easy prey for hackers or terrorists who seek to bring down unprotected networks. As the smart grid becomes more interoperable, these attacks could have debilitating effects nationwide, as you mentioned, Mr. Chairman. In 2007, DHS ran a test known as Aurora, which showcases just how dangerous grid vulnerabilities can be. They used a dial-up modem to rewrite computer code and remotely detonate an industry-controlled system generator. That is why I am pleased we are having this hearing today. We as a Congress must do everything in our power to ensure that the grid remains safe and secure.

The testimony we hear today will help us understand our successes and identify flaws in the current approach so that we can understand what else can be done to protect the smart grid. This hearing will also help us understand if Congress needs to provide more resources or more legislative authority for key cybersecurity agencies.

The administration has made cybersecurity a priority, launching a comprehensive national cybersecurity initiative to protect the digital infrastructure. The President's 2013 budget includes $769 million to support the National Cybersecurity Division within the Department of Homeland Security. These funds are targeted at improving monitoring on Federal networks to respond to cyber threats, and supporting cyber attack responses for critical infrastructure owners and operators, and for State and local authorities.

I commend this targeted focus on cybersecurity, but I am hoping that today our witnesses will help us learn more about any gaps in security that may still exist.

Mr. Chairman, as I said, I appreciate that you are holding this hearing, and I am encouraged that you have announced that we are going to keep looking into other areas where we can work together in a bipartisan fashion. For example, we will hear from wit-

nesses today the issue of cybersecurity goes well beyond the protection of the critical infrastructure. Consumers entrust important personal information on their banks—to their banks, their internet service providers, their credit card companies, and the retailers from whom they purchase items from online. These companies should ensure that they are protecting this information and Congress needs to be doing its oversight job to make sure that this is the case.

Every day we hear stories about e-mail accounts being hacked, credit card information being hijacked, and Social Security numbers or other important personal information being stolen by cyber criminals. It has even happened to some of us who sit on this panel. The loss of this information can be costly and personally damaging. In September of last year, the internet security company, Symantec, issued the Norton Cyber Crime Report and calculated that cyber crimes cost companies and consumers $114 billion annually. That same report found that more than 2/3 of adults online had been victims of a cyber crime.

As our use of internet services becomes more and more integrated, using the same internet services for e-mail, social networking, photo sharing, bill paying, and browsing and search, we have to be more vigilant in ensuring the protection of our personal information. Sites like Google, Yahoo, and Facebook will be targets for hackers, and if successful, these cyber attacks will have a major impact on the American public.

For that reason, Mr. Chairman, in addition to investigating how the government can improve critical infrastructure cybersecurity, I think this subcommittee should also look closely at what the private sector is doing to prevent cyber attacks and keep consumers' personal information safe.

I look forward to working with you on all of these issues, Mr. Chairman, and with that, I will yield back.

Mr. STEARNS. Thank the gentlelady and recognize the gentleman from Nebraska, Mr. Terry, for 2 minutes.

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Mr. TERRY. Thank you, Mr. Chairman, for holding this important hearing. Of course, one of the cornerstone responsibilities of this Committee is finding—determining reliability of our electricity delivery system. In today's world, that means when we are protecting the grid, it means we have to look into the cyber attacks.

Let me just give you one quick story from University of Nebraska at Omaha, PKI Institute of Information Assurance. They set up as a class project in their master's program an electric company fake Web site, and then tracked who would attack it. Within about 48 hours, there was probably about 50 hack attempts, most of them coming from a certain region in China, but all over the world. This just shows how vulnerable we are.

Now as we move to more of a smart grid, that also means that we have more vulnerabilities, whether it is from EMPs or from cyber attacks. So looking at how we can strengthen our ability to defend from these attacks is just part of our core effort here.

So at this time, I would like to yield the rest of my time to——

Mr. STEARNS. The gentleman yields back the balance of his time?
Mr. TERRY. Yes.
Mr. STEARNS. And so we have extra time here, and we recognize Dr. Burgess for a minute and a half to 2 minutes.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. Thank you, Mr. Chairman for the recognition. I want to thank our witnesses for being here today, because this is an issue of extreme importance. We are facing threats from around the world, and certainly, all of us want to remain vigilant.

From hearings that we have had in previous Congresses in this subcommittee, and from talking to people who are charged with protecting our country, defending our country in an increasingly adverse cyber environment, we are well aware that every day from around the world, as Mr. Terry mentioned, are trying to break into our vital modes of infrastructure and technology, and not the least of that being the electric grid.

We are also concerned about cost and that is why I am so grateful that some of the testimony today has focused on the effectiveness and the effectiveness of even the metrics that we use in order to assess how we are doing, and I think that is of critical importance, both as a consumer and certainly, it is clear that the utility companies themselves will be interested in knowing what the effectiveness of the measures that we are asking them to implement—they have to be interested in the effectiveness of those measures.

We want these to be informed decisions. We do not want them to be emotional or political decisions, but we want them to be based on the best possible information, so that is why I am grateful, Mr. Chairman, that you called this hearing. I am grateful for our witnesses to be here, and I will yield back to the chairman.

Mr. STEARNS. Gentleman yields back and we recognize the gentlelady from Tennessee, Ms. Blackburn——
Mrs. BLACKBURN. Thank you so much——
Mr. STEARNS [continuing]. For a minute and a half.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. Thank you. I appreciate that. I do want to welcome our witnesses.

We all know and we realize how very—how debilitating these attacks would be. Some of the reports that I have read indicate that we could see blackouts for 9 to 18 months in areas if we were hit with a cyber attack, and certainly last year as we have looked at the series of attacks known as Night Dragon and how the hackers broke into and stole proprietary information worth millions of dollars, we see how this has a direct impact on not only U.S. but European energy companies.

I think that one of the things that concerns me is looking at what we have found out with the increase from '06 to '10 a 650 percent increase in the number of attacks and the incidences that have been tracked. So we welcome you and we look forward to hearing

what you have to say, and some of the accelerated planning issues that are in front of us.

Thank you very much. Yield back.

Mr. STEARNS. Gentlelady yields back and I recognize the gentleman from Georgia, Mr. Gingrey, for 1 minute.

OPENING STATEMENT OF HON. PHIL GINGREY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. GINGREY. Mr. Chairman, I thank you for giving me a minute of time. I was looking for an e-mail on my iPhone, but I don't know how to use the iPhone so I couldn't pull up the e-mail. But basically I received an e-mail on my iPhone just a couple of days ago, purportedly from literally my best friend, who happens to be of European descent, and it was this typical e-mail, "I am contacting you with tears in my eyes. We went on vacation in Spain, we got mugged at the—we can't get home, could you please e-mail us or wire us 1,600 Euros? God bless you and thank you for your help." I mean, that kind of thing is amazing. It is the first time I have ever received one of those, but that is small potatoes, of course, compared to what we are talking about here, but it just is a small example of the seriousness of cyber attack on the smart grid, so I am really looking forward to hearing from the witnesses and learning more about this——

Ms. DEGETTE. Will the gentleman yield? Maybe your iPhone doesn't work because you opened that e-mail from your friend and now they have destroyed all your network.

Mr. GINGREY. I have been attacked.

Ms. DEGETTE. Yes.

Mr. GINGREY. Thank you, Ms. DeGette.

Ms. DEGETTE. You are welcome.

Mr. STEARNS. All right, our side is complete. With that, recognize the Ranking Member of the Full Committee, the gentleman from California for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you, Mr. Chairman. I appreciate your holding this hearing, and I want to say, this is exactly the type of oversight this subcommittee should be conducting, ensuring that our government uses its resources wisely, and that the private sector is taking appropriate steps to guarantee the safety and security of our Nation's critical infrastructure.

Today's hearing will give us an opportunity to learn about the key challenges to ensuring the security of this Nation's electric grid. As the grid becomes more technologically advanced, it becomes more exposed to hackers, terrorists, and foreign enemies. As the grid becomes more interoperable, the potential effect of a cybersecurity breach becomes more widespread.

The smart grid offers tremendous potential benefits. Modernizing the grid will make electricity cheaper, more efficient, more reliable, but at the same time, we must take appropriate action to protect the electric grid and to improve services and access for citizens across the Nation.

In 2007, Congress and then-President Bush approved the Energy Independence and Security Act of 2007. This legislation authorized the Smart Grid Investment Grant Program and the smart grid Demonstration Program. The 2009 Recovery Act amended these programs and provided funding to ensure their implementation.

The first program, the Smart Grid Demonstration Program, funded 32 projects to verify the viability of smart grid technology and quantify the costs and benefits of these improvements. The second program, the Smart Grid Investment Grant Program, awarded grants for smart grid technology updates. These grants have allowed the installation of smart meters in millions of homes, implementation of automatic peak pricing, response for commercial and industrial customers, and the development of comprehensive demand response programs. These programs provided 99 grants to recipients in 42 States, the District of Columbia, and Guam. In total, the Energy Department invested $3.4 billion in grants, which was matched by $4.6 billion in private investments, for a total public private investment of over $8 billion.

Today will give us an opportunity to evaluate what is working and what can be improved in these programs. The Department of Energy's Inspector General recently issued a report on the Smart Grid Grant Program and identified some reimbursement issues and concerns about approval of some cybersecurity plans. Today's hearing will allow us to explore those issues.

Beyond oversight, we must also do our part in protecting the electrical grid. Both GAO and the DOE Inspector General have acknowledged that Federal Energy Regulatory Commission has only limited authority to ensure the grid is truly secure. In fact, the Inspector General found that FERC does not have the authority to develop its own standards or mandatory alerts, even when new threats are identified. This gap in authority creates serious potential risks.

Last May, the Subcommittee on Energy and Power held a hearing to discuss the bipartisan Grid Reliability and Infrastructure Defense Act, a bill that would give FERC additional authority to protect the electric grid from potentially dangerous vulnerabilities. Today's hearing will again demonstrate why we need to act on this legislation without further delay. We must continue to invest in making our electric grid the best in the world. That includes investing in standards and technologies so that the electric grid is secure in the face of unexpected terror attacks or hacking attempts. This hearing is an important step in identifying what can be done to ensure that the electric grid is protected.

I have focused my opening statement on the electric grid, but I hope this hearing produces some ways for members to learn how to use their iPhones, and to be able to realize that when they get e-mails asking for money, they had better think twice about it. I nearly fell for that one myself. A good friend was evidently not able to afford to leave Paris. Things could be worse, but they wanted something worse, they wanted my money. This shows that our security of our technology is very important objective, and I think it is worthwhile for our hearing to do it.

I am sure, since I have 19 second left, I want to comment that I am sure by the end of this hearing, whatever we find we don't

like, the Republicans will blame on President Obama. Such is life. But I think this is a good hearing and I compliment the chairman for holding it. I will yield back my second.

Mr. STEARNS. The gentleman yields back his second, and I point out that sometimes we hear on your side everything is blamed on Bush, so——

Mr. WAXMAN. Too late for that.

Mr. STEARNS. All right. Let me direct my comments to our witnesses this morning. As you know, the testimony that you are about to give is subject to Title 18 Section 1001 of the United States Code. When holding an investigative hearing, this Committee has a practice of taking testimony under oath. Do you have any objection to testifying under oath?

The Chair then advises you that under the rules of the House and the rules of this Committee, you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony today? If not, would you please rise and raise your right hand?

[Witnesses sworn.]

Mr. STEARNS. You may now give your 5-minute summary of your written statement, and Mr. Wilshusen, you are first.

TESTIMONY OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY DAVID C. TRIMBLE, DIRECTOR, NATURAL RESOURCES AND ENVIRONMENT, GOVERNMENT ACCOUNTABILITY OFFICE; AND RICHARD J. CAMPBELL, SPECIALIST, ENERGY POLICY, CONGRESSIONAL RESEARCH SERVICE

TESTIMONY OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Thank you, Mr. Chairman.

Chairman Stearns, Ranking Member DeGette, and members of the subcommittee, thank you for the opportunity to testify today at today's hearing on cybersecurity for the smart grid. I am joined today by David Trimble, who is the Director for GAO's Natural Resources and Environment team. In addition, Mr. Chairman, if I may, I would like to recognize John Logoson, Mike Gilmore, and especially Lee McCracken for their efforts——

Mr. STEARNS. Ask them to raise their hand. We are not sure——

Mr. WILSHUSEN. For their efforts in developing our written statement that we submitted today.

As you know, the electric power industry is increasingly incorporating information technology systems and networks into its existing infrastructure as it modernizes the electricity grid. In 2007, the Energy Independence and Security Act established that it is Federal policy to support this modernization. Known as a smart grid, these nationwide efforts are aimed at improving the reliability and efficiency of the grid, and facilitating the use of alternative energy sources. Smart grid technologies include smart meters that enable two way communications between utilities and customers, smart components that provide system operators with detailed data on the conditions of transmission and distribution systems, and advanced methods for controlling equipment. The use of these sys-

tems may have a number of benefits, such as fewer and shorter outages of electrical service, lower electricity rates, and an improved ability to respond to attacks on the electric grid.

However, the increased reliance on IT systems and networks also exposes the grid to cybersecurity vulnerabilities. For nearly a decade, GAO has identified the protection of systems supporting our Nation's critical infrastructures as—which include the electric grid—as a government-wide high risk area. Mr. Chairman, the threats to these systems supporting these infrastructures are evolving and growing. They include both unintentional and intentional threats, and may come in the form of equipment failure, as well as targeted and untargeted attacks from our adversaries.

The interconnectivity between information systems, the internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructures, the security of sensitive information, and the flow of commerce.

In January 2011, GAO reported on a number of key challenges to securing smart grid systems and networks. For example, the Federal Energy Regulatory Commission, or FERC, which has responsibility for adopting cybersecurity and other standards it deems necessary to ensure grid functionality and interoperability, had not developed a coordinated approach with other regulators to monitor industry compliance with voluntary standards. In addition, we reported other challenges affecting industry efforts to secure the smart grid. Specifically, the electricity industry had not consistently built security features under certain smart grid devices, established an effective mechanism for our sharing cybersecurity information, and created a set of metrics for evaluating the effectiveness of cybersecurity controls.

GAO made several recommendations to FERC aimed at addressing these challenges, and the Commission agreed with our recommendations.

To summarize, Mr. Chairman, the electricity industry is in the midst of a major transformation as a result of smart grid initiatives. While these initiatives hold the promise of significant benefits, including a more resilient electric grid, lower energy costs, and the ability to tap alternative sources of power, the prevalence of cyber threats aimed at the Nation's critical infrastructure and the cyber vulnerabilities arising from the use of new technologies highlight the importance of securing smart grid systems. In particular, it will be important for Federal regulators and other stakeholders to work closely with the private sector to address key cybersecurity challenges posted by the transition—posed by the transition to smart grid technology. While no system can be made 100 percent secure, proven security strategies could help reduce risks to a manageable and acceptable level.

Chairman Stearns, Ranking Member DeGette, and other members of the subcommittee, this completes my statement, and David and I would be happy to answer your questions.

[The prepared statement of Mr. Wilshusen and Mr. Trimble follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:15 a.m. EST
Tuesday, February 28, 2012

CYBERSECURITY

Challenges in Securing the Modernized Electricity Grid

Statement of Gregory C. Wilshusen, Director
Information Security Issues

David C. Trimble, Director
Natural Resources and Environment

GAO-12-507T

GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-507T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

February 2012

CYBERSECURITY

Challenges in Securing the Modernized Electricity Grid

Why GAO Did This Study

The electric power industry is increasingly incorporating information technology (IT) systems and networks into its existing infrastructure as part of nationwide efforts—commonly referred to as the "smart grid"—aimed at improving reliability and efficiency and facilitating the use of alternative energy sources such as wind and solar. Smart grid technologies include metering infrastructure ("smart meters") that enable two-way communication between customers and electricity utilities, smart components that provide system operators with detailed data on the conditions of transmission and distribution systems, and advanced methods for controlling equipment. The use of these systems can bring a number of benefits, such as fewer and shorter outages, lower electricity rates, and an improved ability to respond to attacks on the electric grid. However, this increased reliance on IT systems and networks also exposes the grid to cybersecurity vulnerabilities, which can be exploited by attackers. Moreover, for nearly a decade, GAO has identified the protection of systems supporting our nation's critical infrastructure—which include the electric grid—as a governmentwide high-risk area.

GAO is providing a statement describing (1) cyber threats facing cyber-reliant critical infrastructures and (2) key challenges to securing smart grid systems and networks. In preparing this statement, GAO relied on its previously published work in this area.

View GAO-12-507T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or David C. Trimble at (202) 512-3841 or trimbled@gao.gov.

What GAO Found

The threats to systems supporting critical infrastructures are evolving and growing. In a February 2011 testimony, the Director of National Intelligence noted that there had been a dramatic increase in cyber activity targeting U.S. computers and systems in the previous year, including a more than tripling of the volume of malicious software since 2009. Varying types of threats from numerous sources can adversely affect computers, software, networks, organizations, entire industries, and the Internet itself. These include both unintentional and intentional threats, and may come in the form of targeted or untargeted attacks from criminal groups, hackers, disgruntled employees, hostile nations, or terrorists. The interconnectivity between information systems, the Internet, and other infrastructures can amplify the impact of these threats, potentially affecting the operations of critical infrastructures, the security of sensitive information, and the flow of commerce. Moreover, the smart grid's reliance on IT systems and networks exposes the electric grid to potential and known cybersecurity vulnerabilities, which could be exploited by attackers.

As GAO reported in January 2011, securing smart grid systems and networks presented a number of key challenges that required attention by government and industry. These included:

- **A lack of a coordinated approach to monitor industry compliance with voluntary standards.** The Federal Energy Regulatory Commission (FERC) is responsible for regulating aspects of the electric power industry, which includes adopting cybersecurity and other standards it deems necessary to ensure smart grid functionality and interoperability. However, FERC had not, in coordination with other regulators, developed an approach to monitor the extent to which industry will follow the voluntary smart grid standards it adopts. As a result, it would be difficult for FERC and other regulators to know whether a voluntary approach to standards setting is effective.
- **A lack of security features built into smart grid devices.** According to a panel of experts convened by GAO, smart meters had not been designed with a strong security architecture and lacked important security features. Without securely designed systems, utilities would be at risk of attacks occurring undetected.
- **A lack of an effective information-sharing mechanism within the electricity industry.** While the industry has an information-sharing center, it had not fully addressed the need for sharing cybersecurity information in a safe and secure way. Without quality processes for sharing information, utilities may lack information needed to protect their assets against attackers.
- **A lack of metrics for evaluating cybersecurity.** The industry lacked metrics for measuring the effectiveness of cybersecurity controls, making it difficult to measure the extent to which investments in cybersecurity improve the security of smart grid systems. Until such metrics are developed, utilities may not invest in security in a cost-effective manner or be able to make informed decisions about cybersecurity investments.

GAO made several recommendations to FERC aimed at addressing these challenges. The commission agreed with these recommendations and described steps it is taking to implement them.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on assessments of security for the smart grid.

As you know, the electric power industry is increasingly incorporating information technology (IT) systems and networks into its existing infrastructure (e.g., electricity networks including power lines and customer meters) as part of nationwide efforts—commonly referred to as the "smart grid"—aimed at improving reliability and efficiency and facilitating the use of alternative energy sources (e.g., wind and solar). Along with these anticipated benefits, however, cybersecurity and industry experts have expressed concern that, if not implemented securely, smart grid systems will be vulnerable to attacks that could result in widespread loss of electrical services essential to maintaining our national economy and security.

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

In our testimony today, we will describe (1) cyber threats facing cyber-reliant critical infrastructures, which include the electric grid,[2] and (2) key challenges to securing smart grid systems and networks. In preparing this statement in February 2012, we relied on our previous work in this area, including a review of efforts to secure the smart grid and associated challenges.[3] The products upon which this statement is based contain

[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 high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure—referred to as cyber-critical infrastructure protection, or cyber CIP. See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[2]Federal policy established 18 critical infrastructure sectors: banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; food and agriculture; government facilities; health care and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water.

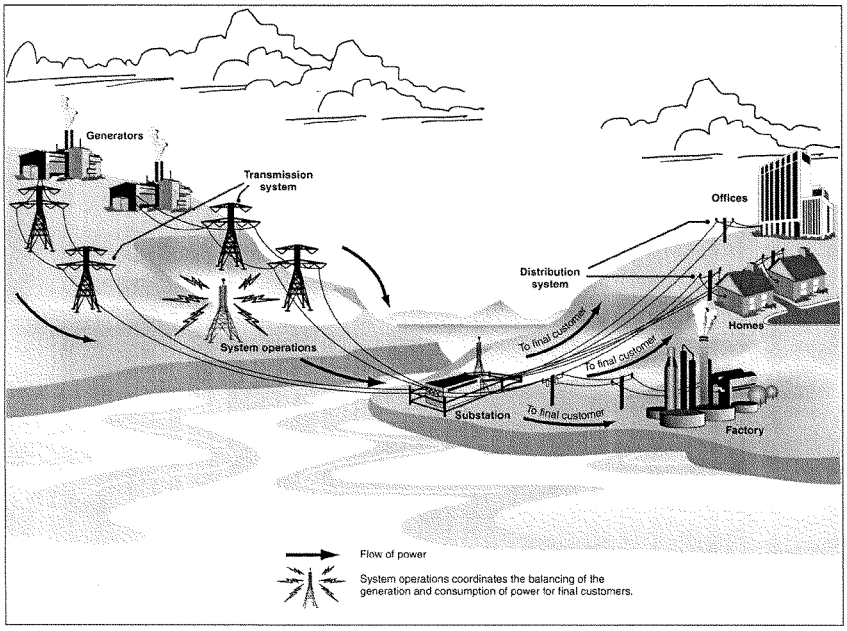
[3]GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, GAO-11-117 (Washington, D.C.: Jan. 12, 2011).

detailed overviews on the scope of our reviews and the methodology we used. The work on which this statement is based was performed 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. We believe that the evidence obtained provided 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



Source: GAO analysis.

Utilities 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.[4] As we have previously reported, the effective functioning of the electricity industry is highly dependent on these control systems.[5] However, for many years, aspects of the electricity network lacked (1) adequate 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.

Smart Grid Aims to Modernize 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.

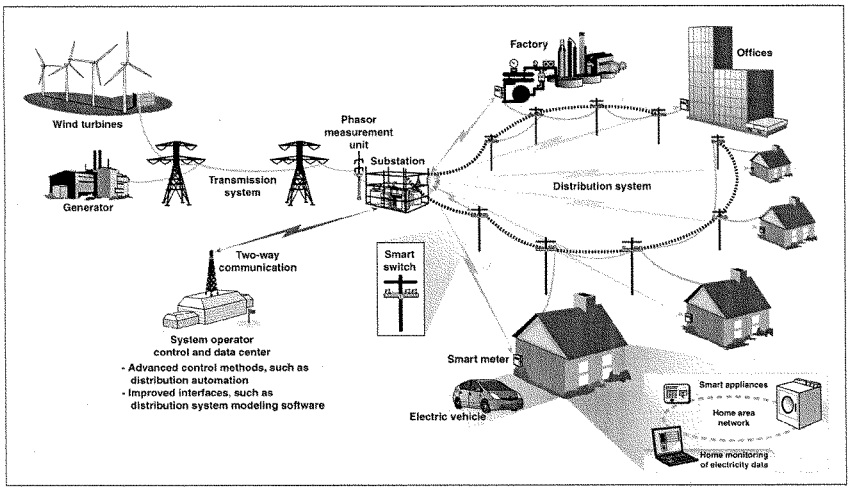
This vision—the smart grid—would increase the use of IT systems and networks and two-way communication to automate actions that system operators formerly had to make manually. Smart grid modernization is an ongoing process, and initiatives have commonly involved installing advanced metering infrastructure (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 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 that communicate with each other to reroute electricity around a

[4]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.

[5]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).

troubled line and high-resolution, time-synchronized monitors—called phasor measurement units—on the transmission system. Figure 2 illustrates one possible smart grid configuration, though utilities making smart grid investments may opt for alternative configurations depending on cost, customer needs, and local conditions.

Figure 2: Common Smart Grid Components



Source: GAO analysis.

According to the National Energy Technology Laboratory, a Department of Energy (DOE) national laboratory supporting smart grid efforts, smart grid systems fall into several different categories:

- Integrated communications, such as broadband over power line communication technologies or wireless communications technologies.
- Advanced components, such as smart switches, transformers, cables, and other devices; storage devices, such as plug-in hybrid electric

vehicles and advanced batteries; and grid-friendly smart home appliances.
- Advanced control methods, including real-time monitoring and control of substation and distribution equipment.
- Sensing and measurement technologies, such as smart meters and phasor measurement units.
- Improved interfaces and decision support, which includes software tools to analyze the health of the electricity system and real-time digital simulators to study and test systems.

The use of smart grid systems may have a number of benefits, including improved reliability from fewer and shorter outages, downward pressure on electricity rates resulting from the ability to shift peak demand, an improved ability to shift to 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 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 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.

Federal Smart Grid Activities

The Energy Independence and Security Act of 2007 (EISA)[6] established federal support for the modernization of the electricity grid and required actions by a number of federal agencies, including the National Institute of Standards and Technology (NIST), FERC, and DOE. With regard to cybersecurity, the act called for 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 planned to identify cybersecurity standards for these systems and also identified the need to develop guidelines for organizations such as electric companies on how to securely implement smart grid systems. In January 2011,[7] 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.[8]
- FERC was to adopt standards resulting from NIST's efforts that it deemed necessary to ensure smart grid functionality and interoperability.

The act also authorized DOE to establish two initiatives to facilitate the development of industry smart grid efforts. These were the Smart Grid Investment Grant Program and the Smart Grid Regional Demonstration Initiative. DOE made $3.5 billion and $685 million of American Recovery and Reinvestment Act ("Recovery Act")[9] funds available for these two initiatives, respectively. The Smart Grid Investment Grant Program provided grant awards to utilities in multiple states to stimulate the rapid deployment and integration of smart grid technologies, while the Smart Grid Regional Demonstration Initiative was to fund regional demonstrations to verify technology viability, quantify costs and benefits, and validate new business models for the smart grid at a scale that can be readily adopted around the country. The federal government has also

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

[7]GAO-11-117.

[8]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.

[9]Pub. L. No. 111-5 (Feb. 17, 2009).

undertaken various other smart-grid-related initiatives, including funding technical research and development, data collection, and coordination activities.

In January 2012, the DOE Inspector General reported that cybersecurity plans submitted by Smart Grid Investment Grant Program recipients were not always complete or they did not describe intended security controls in sufficient detail.[10] The report also stated that DOE officials approved cybersecurity plans for smart grid projects even though some of the plans contained shortcomings that could result in poorly implemented controls. The report recommended, among other things, that DOE ensure that grantees' cybersecurity plans were complete, including thorough descriptions of potential security risks and related mitigation through necessary controls. The responsible DOE office stated that it will continue to ensure that the security plans are complete and are implemented properly.

Smart Grid Is Potentially Vulnerable to a Variety of Cyber Threats

Threats to systems supporting critical infrastructure—which includes the electricity industry and its transmission and distribution systems—are evolving and growing. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009.[11] Different types of cyber threats from numerous sources may adversely affect computers, software, networks, organizations, entire industries, or the Internet. Cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists. Moreover, these groups have a wide array of

[10]U.S. Department of Energy, Office of Inspector General, Office of Audits and Inspections, *Audit Report: The Department's Management of the Smart Grid Investment Grant Program*, OAS-RA-12-04 (Washington, D.C.: Jan. 20, 2012).

[11]Director of National Intelligence, *Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community*, statement before the Senate Select Committee on Intelligence (Feb. 16, 2011).

cyber exploits at their disposal. Table 1 provides descriptions of common types of cyber exploits.

Table 1: Common Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Logic bomb	A piece of programming code intentionally inserted into a software system that will cause a malicious function to occur when one or more specified conditions are met.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users to direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
SQL injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
Trojan horse	A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed time frame between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from NIST, the United States Computer Emergency Readiness Team, and industry reports.

The potential impact of these threats is amplified by the connectivity between information systems, the Internet, and other infrastructures, creating opportunities for attackers to disrupt critical services, including electrical power. For example, in May 2008, we reported that the corporate network of the Tennessee Valley Authority (TVA)—the nation's largest public power company, which generates and distributes power in an area of about 80,000 square miles in the southeastern United States—

contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[12] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing TVA's critical infrastructures and 73 recommendations to address specific weaknesses in security controls. TVA concurred with the recommendations and has taken steps to implement them. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

We have reported[13] that cyber incidents can affect the operations of energy facilities, as the following examples illustrate:

- **Stuxnet.** In July 2010, a sophisticated computer attack known as Stuxnet was discovered. It targeted control systems used to operate industrial processes in the energy, nuclear, and other critical sectors. It is designed to exploit a combination of vulnerabilities to gain access to its target and modify code to change the process.
- **Browns Ferry power plant.** In August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.
- **Northeast power blackout.** In August 2003, failure of the alarm processor in the control system of FirstEnergy, an Ohio-based electric utility, prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid. When several key transmission lines in northern Ohio tripped due to contact with trees, they initiated a cascading failure of 508 generating units at 265 power plants across eight states and a Canadian province.
- **Davis-Besse power plant**. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.

[12]GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

[13]GAO-07-1036 and GAO-12-92.

Smart Grid Faces Cybersecurity Vulnerabilities

While presenting significant potential benefits, the smart grid vision and its increased reliance on IT systems and networks also expose the electric grid to potential and known cybersecurity vulnerabilities, which could be exploited by a wide array of cyber threats. This creates an increased risk to the smooth and reliable operation of the grid. As we and others have reported,[14] these vulnerabilities include

- an increased number of entry points and paths that can be exploited by potential adversaries and other unauthorized users;
- the introduction of new, unknown vulnerabilities due to 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, providing incentives for adversaries to attack these systems and potentially putting private information at risk of unauthorized disclosure and use.

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.[15] Further, in 2009, the Department of Homeland Security, in cooperation with DOE, 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.[16]

[14]GAO-11-117.

[15]GAO-07-1036.

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

Securing Smart Grid Systems and Networks Presents Challenges

In our January 2011 report, we identified a number of key challenges that industry and government stakeholders faced in ensuring the cybersecurity of the systems and networks that support our nation's electricity grid.[17] Among others, these challenges included the following:

- *Lack of a coordinated approach to monitor whether industry follows voluntary standards.* As mentioned above, under EISA, FERC is responsible for adopting cybersecurity and other standards that it deems necessary to ensure smart grid functionality and interoperability. However, FERC had not developed an approach coordinated with other regulators to monitor, at a high level, the extent to which industry will follow the voluntary smart grid standards it adopts. There had been initial efforts by regulators to share views, through, for example, a collaborative dialogue between FERC and the National Association of Regulatory Utility Commissioners (NARUC), which had discussed the standards-setting process in general terms. Nevertheless, according to officials from FERC and NARUC, FERC and the state public utility commissions had not established a joint approach for monitoring how widely voluntary smart grid standards are followed in the electricity industry or developed strategies for addressing any gaps. Moreover, FERC had not coordinated in such a way with groups representing public power or cooperative utilities, which are not routinely subject to FERC's or the states' regulatory jurisdiction for rate setting. We noted that without a good understanding of whether utilities and manufacturers are following smart grid standards, it would be difficult for FERC and other regulators to know whether a voluntary approach to standards setting is effective or if changes are needed.[18]

[17]GAO-11-117.

[18]In an order issued on July 19, 2011, FERC reported that it had found insufficient consensus to institute a rulemaking proceeding to adopt Smart Grid interoperability standards identified by NIST as ready for consideration by regulatory authorities. While FERC dismissed the rulemaking, it encouraged utilities, smart grid product manufacturers, regulators, and other smart grid stakeholders to actively participate in the NIST interoperability framework process to work on the development of interoperability standards and to refer to that process for guidance on smart grid standards. Despite this result, we believe our recommendations to FERC in GAO-11-117, with which FERC concurred, remain valid and should be acted upon as consensus is reached and standards adopted.

- *Lack of security features being built into certain smart grid systems.* Security features had not been consistently built into smart grid devices. For example, according to experts from a panel convened by GAO, currently available smart meters had not been designed with a strong security architecture and lacked important security features, such as event logging[19] and forensics capabilities, which are needed to detect and analyze attacks. In addition, these experts stated that smart grid home area networks—used for managing the electricity usage of appliances and other devices in the home—did not have adequate security built in, thus increasing their vulnerability to attack. Without securely designed smart grid systems, utilities may not be able to detect and analyze attacks, increasing the risk that attacks would succeed and utilities would be unable to prevent them from recurring.
- *Lack of an effective mechanism for sharing cybersecurity information within the electricity industry.* The electricity industry lacked an effective mechanism to disclose information about smart grid cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices in the industry. For example, experts stated that while the industry has an information-sharing center, it had not fully addressed these information needs. According to these experts, information regarding incidents such as both successful and unsuccessful attacks must be able to be shared in a safe and secure way; this is crucial to avoid publicly revealing the reported organization and penalizing entities actively engaged in corrective action. Such information sharing across the industry could provide important information regarding the level of attempted attacks and their methods, which could help grid operators better defend against them. In developing an approach to cybersecurity information sharing, the industry could draw upon the practices and approaches of other industries. Without quality processes for information sharing, utilities may not have the information needed to adequately protect their assets against attackers.
- *Lack of industry metrics for evaluating cybersecurity.* The electricity industry was also challenged by a lack of cybersecurity metrics, making it difficult to measure the extent to which investments in cybersecurity improve the security of smart grid systems. Experts noted that while such metrics[20] are difficult to develop, they could help

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

[20]Metrics can be used for, among other things, measuring the effectiveness of cybersecurity controls for detecting and blocking cyber attacks.

in comparing the effectiveness of competing solutions and determining what mix of solutions best secure systems. Further, our panel of experts noted that having metrics would help utilities develop a business case for cybersecurity by helping to show the return on a particular investment. Until such metrics are developed, increased risk exists that utilities will not invest in security in a cost-effective manner or be able to have the information needed to make informed decisions about their cybersecurity investments.

Accordingly, in our January 2011 report, we made multiple recommendations to FERC, including that it develop an approach to coordinating with state regulators to evaluate the extent to which utilities and manufacturers are following voluntary smart grid standards and develop strategies for addressing any gaps in compliance with standards that are identified as a result. We further recommended that FERC, working with NERC as appropriate, assess whether commission efforts should address any of the cybersecurity challenges identified in our report. FERC agreed with our recommendations and described steps the commission intended to take to address them. We are currently working with FERC officials to determine the status of their efforts to address these recommendations.

In summary, the electricity industry is in the midst of a major transformation as a result of smart grid initiatives and this has led to significant investments by many entities, including utilities, private companies, and the federal government. While these initiatives hold the promise of significant benefits, including a more resilient electric grid, lower energy costs, and the ability to tap into alternative sources of power, the prevalence of cyber threats aimed at the nation's critical infrastructure and the cyber vulnerabilities arising from the use of new technologies highlight the importance of securing smart grid systems. In particular, it will be important for federal regulators and other stakeholders to work closely with the private sector to address key cybersecurity challenges posed by the transition to smart grid technology. While no system can be made 100 percent secure, proven security strategies could help reduce risk to an acceptable level.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee, this completes our statement. We would be happy to answer any questions you have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at [redacted] or David C. Trimble at [redacted] Other key contributors to this statement include Michael Gilmore (Assistant Director), Jon R. Ludwigson (Assistant Director), Paige Gilbreath, Barbarol J. James, and Lee A. McCracken.

Mr. STEARNS. All right, and I understand, Mr. Campbell, your opening statement is welcome.

TESTIMONY OF RICHARD J. CAMPBELL

Mr. CAMPBELL. Good morning, Chairman, Ranking Member, and members of the subcommittee, my name is Richard Campbell. I am a Specialist in Energy Policy for the Congressional Research Service. On behalf of CRS, I would like to thank the Committee for inviting me to testify here today. I would like to request that my written testimony be entered into the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. CAMPBELL. My testimony will provide background on the development of the smart grid, the Department of Energy's vision for the smart grid, and plans for the cybersecurity of the smart grid. I should note that CRS does not advocate policy or take a position on specific legislation.

The electrical grid in the United States comprises all of the power plants generating electricity, together with the transmission and distribution systems which bring power to end-use customers. The grid also connects the many public and private electricity companies and power companies throughout the United States. The modernization of the grid to accommodate today's power flows, serve reliability needs, and meet future projected uses is leading to the incorporation of the electronic intelligence capabilities for power control and operations monitoring. The smart grid is the name given to this evolving intelligent electricity network. While these intelligent components may enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to cyber, that is, computer-generated, attack, since they are built around microprocessor devices controlled by software programming. The potential for a major disruption or widespread damage to the Nation's power system from a large-scale cyber attack has increased focus on the cyber security of the smart grid.

The Department of Energy summarized its view of the potential of the smart grid by the year 2030 as a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between.

Federal funding has been provided to help develop concepts and technologies for the smart grid. The American Recovery and Reinvestment Act of 2009 provided $4.5 billion in funding to the DOE for projects to modernize the grid. DOE's Smart Grid Investment Grant program received $3.5 billion of these funds with the expressed purpose of stimulating the rapid deployment of advanced digital technologies needed to modernize the grid.

The SGIG is a cost-shared program, meaning recipients of grants were to provide as much as 50 percent of a project's total costs.

According to a recent report from the DOE's Office of Inspector General, all the available grant funds from the SGIG program have been awarded to 99 recipients, with awards ranging in value from $397,000 to $200 million. An approach to cybersecurity was required as part of the SGIG application process. Recipients of awards were required to submit a detailed plan addressing specific

cybersecurity elements and concerns. The DOEIG report observed that DOE approved these cybersecurity plans even though weaknesses in the plans were identified and not fully addressed. The DOE responded to the report saying that it will require award recipients to update their cybersecurity plans later this year.

The DOE funded the development of the recently released Roadmap to Achieve Energy Delivery Systems Cybersecurity. This Roadmap provides a plan to improve the cybersecurity of the electricity, oil, and natural gas sectors.

The Roadmap recognizes the changing landscape of cybersecurity, and the continuing need to seek out and address cybersecurity gaps, and includes an implementation strategy for cybersecurity built on milestones to be achieved by the year 2020.

The DOE has recently begun to update its vision for the smart grid, focusing on three key attributes it sees as desirable for the smart grid of the future: a seamless, cost-effective electricity system; a system capable of accommodating all generation choices; a system which enables customer choice.

According to this updated vision, the smart grid will still see regional diversity in power choices, while allowing for the development of a national framework. According to DOE, a reliable, secure, and resilient grid will be the key to achieving this vision.

In conclusion, it is the very features which can add seamless integration and utility to the smart grid that also add cyber vulnerabilities to electricity networks. Some assert that the smart grid and cybersecurity systems will have to develop along parallel but interconnected paths if the electric grid of the future is to develop in a manner that can enhance, and not impair, future economic development.

Congress could provide funding for research and development of systems to bridge gaps in cybersecurity and build the smart grid. Federal funding could also be used to bring government and industry together in forums to address the needs and directions of these developing systems.

Congress may also provide for a regulatory framework which could achieve a basic level of cybersecurity. But due to the constantly changing nature of cyber threats, it is unlikely that effective cybersecurity of the grid will be achieved by regulation alone. Some assert that electric utilities must be focused on cybersecurity as keenly as they are on their current obligation to serve or to provide shareholder value.

Thank you for the invitation to appear today. I will be pleased to address any questions you may have.

[The prepared statement of Mr. Campbell follows:]

The Evolution of the Smart Grid

The modernization of the grid to accommodate today's power flows, serve reliability needs, and meet future projected uses is leading to the incorporation of electronic intelligence capabilities for power control purposes and operations monitoring. The "Smart Grid" is the name given to this evolving intelligent electric power network. While these intelligent components may enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to "cyber" (i.e., computer-generated) attack, since they are built around microprocessor devices whose basic functions are controlled by software programming. The potential for a major disruption or widespread damage to the nation's power system from a large-scale cyber attack has increased focus on the cyber security of the Smart Grid.

Department of Energy's Vision for the Smart Grid

The U.S. Department of Energy (DOE) summarized its view of the potential of the Smart Grid by the year 2030 as "... a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between."

DOE's Smart Grid Investment Grant (SGIG) program received $3.5 billion from the American Recovery and Reinvestment Act of 2009. The program used the funds with the intent of stimulating the rapid deployment of advanced digital technologies needed to modernize the grid. According to a recent report from the DOE's Office of Inspector General (DOEIG), all the available grant funds from the SGIG program have been awarded to 99 recipients. An approach to cybersecurity was required as part of the SGIG application process. The DOEIG report observed that DOE approved these cybersecurity plans even though weaknesses in the plans were identified. The DOE responded to the report saying that it will require award recipients to update their cybersecurity plans later this year.

A Cybersecurity Roadmap for 2020

The DOE funded the development of the "Roadmap to Achieve Energy Delivery Systems Cybersecurity," (Roadmap) released in September 2011 by the Energy Sector Control System Working Group. This Roadmap provides a plan to improve the cybersecurity of the electricity, oil, and natural gas sectors. The Roadmap recognizes the changing landscape of cybersecurity, and the continuing need to seek out and address cybersecurity gaps and includes an implementation strategy for cybersecurity built on milestones to be achieved by the year 2020.

Current Status of DOE Smart Grid Efforts

The DOE has recently begun to update its vision for the Smart Grid, focusing on three key attributes it sees as desirable for the Smart Grid of the future. According to DOE, a reliable, secure, and resilient grid will be the key to achieving this vision.

Considerations for Congress

The very features which can add seamless integration and utility to the Smart Grid also add cyber vulnerabilities to electricity networks. Some assert that the Smart Grid and cybersecurity systems will have to develop along parallel but interconnected paths if the electric grid of the future is to develop in a manner that can enhance, and not impair, future economic development.

Testimony of Richard J. Campbell
Specialist in Energy Policy
Congressional Research Service

Before the Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
February 28, 2012

Good Morning Chairman, Ranking Member, and Members of the Subcommittee. My name is Richard Campbell. I am a Specialist in Energy Policy for the Congressional Research Service (CRS). On behalf of CRS, I would like to thank the Committee for inviting me to testify here today. My testimony will provide background on the development and cybersecurity of the Smart Grid, discussing the evolution of the Smart Grid, and planning for Smart Grid development and cybersecurity. I should note that CRS does not advocate policy or take a position on specific legislation.

The Evolution of the Smart Grid

The electrical grid in the United States comprises all of the power plants generating electricity, together with the transmission and distribution lines and systems which bring power to end-use customers. The "grid" also connects the many publicly and privately owned electric utility and power companies in different states and regions of the United States.[1]

[1] As of 2007, there were 210 investor-owned electric utilities, 2,009 publicly-owned electric utilities, 883 consumer-owned rural electric cooperatives, and nine federal electric utilities. Energy Information Administration (EIA), *Electric Power Industry Overview 2007*, http://www.eia.doe.gov/electricity/page/prim2/toc2.html.

However, with changes in federal law,[2] regulatory changes, and the aging of the electric power infrastructure as drivers, the grid is changing from a largely patchwork system built to serve the needs of individual electric utility companies to essentially a national interconnected system, accommodating massive transfers of electrical energy among regions of the United States.

The modernization of the grid to accommodate today's power flows, serve reliability needs, and meet future projected uses is leading to the incorporation of electronic intelligence capabilities for power control purposes and operations monitoring. The "Smart Grid" is the name given to this evolving intelligent electric power network.[3] While these intelligent components may enhance the efficiency of grid operations, they also potentially increase the susceptibility of the grid to "cyber" (i.e., computer-generated) attack, since they are built around microprocessor devices whose basic functions are controlled by software programming. The potential for a major disruption or widespread damage to the nation's power system from a large-scale cyber attack has increased focus on the cyber security of the Smart Grid.

Department of Energy's Vision for the Smart Grid

Expectations vary of what a Smart Grid could accomplish, and the estimated costs of a system rise with the increased scope and attributes of a system. Some see the Smart Grid of the future as a system spanning the nation from coast to coast, able to seamlessly combine distributed

---

[2] Key legislation include the Public Utility Regulatory Policies Act of 1978, the Energy Policy Acts of 1992 and 2005, and the Energy Independence and Security Act of 2007.

[3] The Smart Grid is one of the options being discussed for the future of U.S. electricity networks and would build interactive intelligence into electricity transmission and distribution systems across the United States. Energy efficiency and energy conservation could be enhanced by demand-side management programs enabled by the wide scale deployment of smart meters. Energy storage projects could enhance such a system, providing options for peak load management and potentially allowing for even greater cost savings. See CRS Report R41493, *Options for a Federal Renewable Electricity Standard*, by Richard J. Campbell.

resources and central power stations across the three major interconnections[4] of the United States. Under such visions, distributed and renewable energy resources could be efficiently integrated into the grid, with power (for example) from intermittent wind generation channeled by sensors and intelligent electronics from multiple widely dispersed sites to where power is needed anywhere on the grid. The efficiency and economy of all grid operations could conceivably be optimized by similarly harnessing all power generation to take advantage of a wide range of generation and storage resources across the United States.[5]

The U.S. Department of Energy (DOE) summarized its view of the potential of the Smart Grid by the year 2030 as:

> ... a fully automated power delivery network that monitors and controls every customer and node, ensuring a two-way flow of electricity and information between the power plant and the appliance, and all points in between.[6]

Federal funding has been provided to help develop concepts and technologies for the Smart Grid. The American Recovery and Reinvestment Act of 2009 (P.L.111-5) provided $4.5 billion in funding to DOE for projects to modernize the grid.[7] DOE's Smart Grid Investment Grant (SGIG) program[8] received $3.5 billion of these funds with the expressed purpose of stimulating the rapid deployment of advanced digital technologies needed to modernize the grid.[9]

---

[4] The Eastern, Western, and Texas interconnections of the U.S. grid. See http://www.eia.doe.gov/cneaf/electricity/chg_stru_update/fig7.html.

[5] CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[6] United States Department of Energy, Office of Electric Transmission and Distribution, *"GRID 2030" A NATIONAL VISION FOR ELECTRICITY'S SECOND 100 YEARS*, July 2003, p. 27, http://www.oe.energy.gov/DocumentsandMedia/Electric_Vision_Document.pdf.

[7] CRS Report R40412, *Energy Provisions in the American Recovery and Reinvestment Act of 2009 (P.L. 111-5)*, coordinated by Fred Sissine.

[8] The SGIG program was established by the Energy Independence and Security Act of 2007 (P.L. 110-140).

[9] See FEDCONNECT Opportunity: Recovery Act - Smart Grid Investment Grant Program, http://www.fedconnect.net/FedConnect/?doc=DE-FOA-0000058&agency=DOE.

The SGIG is a cost-shared program, meaning recipients of grants were to provide as much as 50% of a project's total costs. Topics for grants from the program focused on:

- Equipment Manufacturing.
- Customer Systems.
- Advanced Metering Infrastructure.
- Electric Distribution Systems.
- Electric Transmission Systems.
- Cross Cutting Systems.

According to a recent report[10] from the DOE's Office of Inspector General (DOEIG), all the available grant funds from the SGIG program have been awarded to 99 recipients, with awards ranging in value from $397,000 to $200 million. An approach to cybersecurity was required as part of the SGIG application process. Recipients of awards were required to submit a detailed cybersecurity plan addressing specific elements including threat detection, risk assessment, and risk mitigation.[11] The DOEIG report observed that DOE approved these cybersecurity plans even though weaknesses in the plans were identified and not fully addressed. The DOEIG was concerned that if these weaknesses are not properly addressed in the 3-year duration of the award, they could lead to cybersecurity gaps and subsequent compromises in system integrity.[12] The DOE responded to the report saying that it will require award recipients to update their cybersecurity plans later this year.[13]

---

[10] DOE Office of Inspector General, Office of Audits and Inspections, *The Department's Management of the Smart Grid Investment Grant Program*, OAS-RA-12-04, January 2012, http://energy.gov/sites/prod/files/OAS-RA-12-04.pdf.

[11] Ibid.

[12] Ibid.

[13] Ibid. See Appendix 3, Memorandum to DOEIG from DOE's Office of Electric Delivery and Energy Reliability.

A Cybersecurity Roadmap for 2020

The DOE funded the development of the "Roadmap to Achieve Energy Delivery Systems Cybersecurity,"[14] (Roadmap) released in September 2011 by the Energy Sector Control System Working Group. This Roadmap provides a plan to improve the cybersecurity of the electricity, oil, and natural gas sectors.

The Roadmap is an update of an earlier 2006 effort which established a "common vision" for industry and government to develop, deploy, and maintain control systems capable of surviving an intentional cyber attack without the loss of critical functions. The Roadmap recognizes the changing landscape of cybersecurity, and the continuing need to seek out and address cybersecurity gaps. Cyber threats to energy delivery systems are seen as real and becomingly increasingly innovative. The Roadmap recognizes that developing a culture of security that focuses on more than simple compliance with a list of requirements will be needed to achieve a resilient energy system. The Roadmap includes an implementation strategy for cybersecurity built on milestones to be achieved by the year 2020. The milestones focus on continual risk assessment, incident management, and sustained cybersecurity improvements.

---

[14] Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

Current Status of DOE Smart Grid Efforts

The DOE has recently begun to update its vision for the Smart Grid, focusing on three key attributes it sees as desirable for the Smart Grid of the future:[15]

- A seamless, cost-effective electricity system from generation to end use.
- A system capable of meeting clean energy demands and capacity requirements, accommodating all generation choices.
- A system which allows all consumers to participate and enables customer choice.

According to this updated vision, the Smart Grid will still see regional diversity in power choices, while allowing for the development of a national framework. The Smart Grid should also be able to accommodate new products and services. According to DOE, a reliable, secure, and resilient grid will be the key to achieving this vision.

Considerations for Congress

The very features which can add seamless integration and utility to the Smart Grid also add cyber vulnerabilities to electricity networks. Some assert that the Smart Grid and cybersecurity systems will have to develop along parallel but interconnected paths if the electric grid of the future is to develop in a manner that can enhance, and not impair, future economic development.

---

[15] U.S. Department of Energy, *Visioning the 21st Century Electricity Industry: Strategies and Outcomes for America*, February 2012, http://www.nationalelectricityforum.org/pdfs/DOE_vision_presentation.pdf.

Congress could provide funding for research and development of technologies and systems to bridge gaps in cybersecurity and build the Smart Grid. Federal funding could also be used to bring government and industry together in forums to address the needs and directions of these developing systems.

Congress may also provide for a regulatory framework which could achieve a basic level of cybersecurity. But due to the constantly changing nature of cyber threats, it is unlikely that effective cybersecurity of the grid will be achieved by regulation alone. Some assert that electric utilities must be focused on cybersecurity as keenly as they are on their current obligation to serve or to provide shareholder value.

Thank you again for the invitation to appear today. I will be pleased to address any questions you may have.

Mr. STEARNS. Thank you, Mr. Campbell. I will start with my questions.

Let us see if we get something that is current here. A 2011 bulletin by the Department of Homeland Security titled "Insider Threats to Utilities" stated that "based on the reliable reporting of previous incidents, we have a high confidence in our judgment that insiders and their actions pose a significant threat to the infrastructure and information systems of the United States facilities," vis-&-vis the grid. Mr. Wilshusen, are you aware of any specific power outage or threat to the electric grid that has transpired in such a way that is talked about in this Homeland Security report from 2011?

Mr. WILSHUSEN. You mean specifically from an insider threat?

Mr. STEARNS. Yes.

Mr. WILSHUSEN. I can't say I know of a specific incident where that occurred; however, certainly insider threats are very important and a threat that our agencies and entities need to consider, because insiders typically have advanced knowledge and even access to the systems and the types of systems that contain information that they could have the ability then to perpetrate, if they have malicious intent to cause disruptions and damage. And it is not just those with malicious intent, but also insiders who may be careless or who may be untrained that conduct activities that also impair or harm their systems and networks. But clearly, that is a key threat.

Mr. STEARNS. Are you aware of any outsiders soliciting people in the smart grid viable areas? Are you aware of any outsiders that are trying to do this?

Mr. WILSHUSEN. In terms of corrupting——

Mr. STEARNS. Yes.

Mr. WILSHUSEN [continuing]. And using insider threats? I can't say I know of specific examples of where that occurs—that occurred.

Mr. STEARNS. Can you describe the controls and checks in place at utilities to prevent these kinds of attacks?

Mr. WILSHUSEN. Well, clearly one of the key controls that utilities and, indeed, agencies should do is background checks on their employees and those——

Mr. STEARNS. Are they doing the background checks, in your opinion, adequately?

Mr. WILSHUSEN. We haven't examined the—how the securities are——

Mr. STEARNS. So there has been no examination of how those background checks have been done and how they have been corroborated, or the credibility of those checks?

Mr. WILSHUSEN. No, we have not assessed that as part of our review.

Mr. STEARNS. Do you think that should be done?

Mr. WILSHUSEN. Well certainly it should be monitored and checked, because I do believe that individuals that have sensitive positions and hold—and have sensitive access to systems should have some level of background investigation performed. And there are other controls, too, that should be in place to help restrict and limit insiders, either careless or untrained insiders, as well as mali-

cious from performing these types of acts, and that includes by limiting their access to only that level needed for them to perform their jobs, as opposed to giving them broader access to systems.

Mr. STEARNS. The MacAfee Corporation did a report in early 2011, another current report, in which they surveyed about 200 executives from critical electricity infrastructure across the United—across the world, in fact. That found that 85 percent had experienced network infiltrations, and 80 percent had faced a large scale denial of service attack. Do you think that number is correct? That is quite large, 80 percent of both network infiltrations and 80 percent faced a large scale denial of service attack. Do you think those figures are accurate?

Mr. WILSHUSEN. I have no basis to form whether they are accurate or not, but I will say as it relates to Federal Government agencies——

Mr. STEARNS. Is that typical?

Mr. WILSHUSEN. In terms of those that have reported security incidents, yes, most Federal agencies have done that and as the Congresswoman mentioned earlier, the number of reported security incidents within the Federal Government has risen by 650 percent from 2006 through 2010.

Now, what one disparity or inconsistency with that comment that you made, the statistics in that MacAfee report is that within the Federal Government, there was only about 1 percent or so of the reported security incidents were considered to be denial of service attacks, which would be those that would disrupt the——

Mr. STEARNS. So I assume you reviewed the MacAfee report yourself?

Mr. WILSHUSEN. No, I have not.

Mr. STEARNS. How do these people get into cause these infiltrations? I mean, do you have any idea how it actually happens?

Mr. WILSHUSEN. Well, there are a number of different attack patterns——

Mr. STEARNS. Just give me two quick, the most prevalent.

Mr. WILSHUSEN. Well, one would be, for example, if they put malicious software on a thumb drive and then an employee of that corporation——

Mr. STEARNS. Puts that thumb drive into the computer?

Mr. WILSHUSEN. Pardon?

Mr. STEARNS. He puts that thumb drive in the software?

Mr. WILSHUSEN. Puts the thumb drive into the computer and then downloads the malicious software onto the computer. That is one way.

Mr. STEARNS. To the hard disk, yes.

Mr. WILSHUSEN. Another way would be if the attacker would set up a malicious Web site and which would also then entice employees of the service center to—or wherever—to go to that Web site and download what appears to be an innocuous or an attractive program, when in fact, that too contains malicious code that could then allow——

Mr. STEARNS. Could the facility put software in place to prevent both of those from occurring?

Mr. WILSHUSEN. They can, and disable certain functions—physical ports on the laptop or on the desktop to prevent that from hap-

pening. And indeed, the Department of Defense had such an attack on their networks based upon a thumb drive that led them to disable the thumb drives on the vast majority of their——

Mr. STEARNS. Last question. Has the Department of Homeland Security or the Department of Energy issued any guidance to the electricity sector on best practices that we just talked about in these two cases?

Mr. WILSHUSEN. Well, as part of the Energy Independence and Security Act, NIST, the National Institute of Standards and Technology, had responsibilities for developing security guidelines in connection with input from a number of different organizations that were then to be provided to FERC at Department of Energy to either approve if there is a consensus on those, and some of those controls would help to prevent such attacks, or could.

Ms. DEGETTE. Thank you. Mr. Wilshusen, were those controls, in fact, promulgated by FERC?

Mr. WILSHUSEN. No.

Ms. DEGETTE. Why not?

Mr. WILSHUSEN. It determined that there wasn't a consensus on those—development of those standards and cybersecurity guidelines, and under the Act, there—in the process are required to develop a consensus for——

Ms. DEGETTE. So now what? Are they developing standards?

Mr. WILSHUSEN. My understanding is that NIST is working to gain such a consensus.

Ms. DEGETTE. OK. I want to talk with you a minute more about FERC, because what I am wondering is if they need extra authorities to protect the electric grid from these potentially dangerous vulnerabilities.

Can you just give us a quick example of the types of security flaws that might leave the grid vulnerable to hackers?

Mr. WILSHUSEN. One would be if they do not appropriately assess the risk to those various different components of the smart grid and implement the appropriate security controls over that. For example, if the access controls are not appropriately applied to different components of the grid, that could potentially allow a path into——

Ms. DEGETTE. And of course, the development of this smart grid increases this risk because it is more and more computerized, correct?

Mr. WILSHUSEN. Yes, the increased use of IT systems and networks provide additional paths and access points for potential attackers to gain access to it. In addition, the increasing interconnectivity of these systems and networks also allow potential attackers broader range and access to other devices.

Ms. DEGETTE. And yet at the same time that there is broader vulnerability, the increased interconnection and the smart—development of the smart grid, it is a really valuable part of our system because it gives us—number one, it gives us more efficiency so consumers can get better prices, and number two, it allows us to use some of these renewable technologies that the chairman was talking about in his opening statement, correct?

Mr. WILSHUSEN. Yes.

Ms. DEGETTE. And so here is my question. The GAO and others have said that there could be gaps in the FERC's regulatory authority to deal with development of these standards to respond to new vulnerabilities. Can you talk about that for a minute?

Mr. WILSHUSEN. Well in our recent report that we issued back in January of 2011, we identified that FERC did not have appropriate authorities, that their authorities were pretty much—since they didn't have the appropriate authorities, their authorities were limited to basically adopting and approving standards that were developed by others for the smart grid, and then primarily just at the bulk power level and bulk power supply level, not necessarily at the distribution level where certain smart grid investments and devices are being implemented. And we made the recommendation to NERC that they need to really work with these other parties and stakeholders to include the State public utility commissions that do have such authorities and responsibilities to monitor the implementation of any standards that it adopts.

Ms. DEGETTE. So——

Mr. WILSHUSEN. And it had not done that.

Ms. DEGETTE. So do they have the authority to do that, or does Congress need to give them more authority to coordinate with those other operators?

Mr. WILSHUSEN. Well, they have the authority to coordinate with the other operators——

Ms. DEGETTE. OK.

Mr. WILSHUSEN [continuing]. And utility commissions at the State level——

Ms. DEGETTE. OK.

Mr. WILSHUSEN [continuing]. But they don't have the authority to mandate particular cybersecurity standards.

Ms. DEGETTE. Do you think they need that authority?

Mr. WILSHUSEN. We do not make that recommendation or really go there. We just actually made the recommendation to FERC that it determined whether, you know, what gaps overlaps exist, so——

Ms. DEGETTE. Yes, so if FERC determined that, they could come to us——

Mr. WILSHUSEN. Right.

Ms. DEGETTE [continuing]. And ask for that authority.

Mr. WILSHUSEN. That is correct.

Ms. DEGETTE. Now, there are some—do you know how many of these local and State authorities there are that FERC would need to be coordinating with?

Mr. TRIMBLE. Well, you are—FERC is——

Ms. DEGETTE. Mr. Trimble?

Mr. TRIMBLE. Yes, sorry.

Ms. DEGETTE. That is OK.

Mr. TRIMBLE. FERC is—has jurisdiction over the bulk power system, but once it gets into the distribution system at the State level or at the local level, it falls to the State utilities. So the——

Ms. DEGETTE. There are thousands of them, right?

Mr. TRIMBLE. Right, so you are talking about 50 States plus those that aren't under State control or under minimal State control.

Ms. DEGETTE. Right, and then there is other agencies like Homeland Security, Energy and National Security Agency that also have oversight responsibilities over the critical electrical infrastructure, correct?

Mr. TRIMBLE. Um-hum.

Ms. DEGETTE. So all of those individual utilities would have to work together to really address this, right?

Mr. TRIMBLE. That is correct.

Ms. DEGETTE. OK. Now, one last question, Mr. Chairman. I have got a lot more questions in this line, but maybe I will have an opportunity to ask then, but the Energy Independence and Security Act of 2007 directed the National Institute of Standards and Technologies to develop those standards, but those standards haven't been adopted for the reasons Mr. Wilshusen just explained, right?

Mr. TRIMBLE. Right.

Mr. WILSHUSEN. That is correct.

Ms. DEGETTE. And do we have any sense when they are going to be adopted, now that it has gone back to the agency?

Mr. TRIMBLE. We have not seen a timeline.

Ms. DEGETTE. OK, thank you.

Mr. STEARNS. The gentlelady from Tennessee is recognized for 5 minutes.

Mrs. BLACKBURN. I thank you all and appreciate so much the time that you are giving us today, and continuing to work with us through this issue.

I have found it so interesting, as we have worked through these hearings, how our constituents are paying attention to this, and how they come back to us, those constituents that are working in informatics or in energy delivery systems, and they have different things they want to add to the discussion that we are having.

One question I do have on the smart meters that are out there. Is there a way that someone's proprietary information is being tracked or pulled or hacked into—what are the protections that are on these meters? Can you give me just a little bit of information on that, because some of our constituents—and Ms. DeGette talked about this when she said people can watch and find out when the electricity is going to cost them less and then do chores at that time, but our customers are saying now wait a minute. Is this—while it is giving me information, is this going to be giving—what are the protections, the privacy protections that are going to exist to the consumer about protecting that virtual presence and knowledge of themselves?

Mr. WILSHUSEN. Right, that is certainly an area of concern insofar as that those meters need to have the appropriate cybersecurity, information security controls built into them. We convened a panel of cybersecurity experts as part of our review that we issued a report back in January of 2011, and they identified that there are control deficiencies in some of those meters, to include not having the appropriate login capabilities, which would help and—or the forensics capabilities to determine how and whether an attack had occurred.

Mrs. BLACKBURN. OK, then let me ask you this. With those meters, would it be easy just to—is it very easy just to hack into

them? Should people consider there to be so much transparency in these that they are not protecting their usage? Help me with that.

Mr. WILSHUSEN. Well, I would just say that it really depends upon the facts and circumstances of each individual type of meter——

Mrs. BLACKBURN. OK.

Mr. WILSHUSEN [continuing]. And the security vulnerabilities or strengths relative to the individual meters.

Mrs. BLACKBURN. OK. Mr. Wilshusen, I want to ask you, May '08 you made some comments about TVA's corporate network contains security weaknesses that could lead to disruption of their control systems, and of course, for those of us in the Tennessee Valley and TVA as the main power generator, we are very concerned about that. You had 19 specific recommendations that you had for the TVA at that point in time. In your follow ons, has TVA implemented these? Have they been responsive to putting these controls in place? How are we doing with tightening that system up?

Mr. WILSHUSEN. Yes, TVA has been responsive in implementing not only the 19 recommendations that were made in the public report, but also we made a number of other recommendations in a limited distribution report——

Mrs. BLACKBURN. Exactly, yes.

Mr. WILSHUSEN [continuing]. That dealt more with the technical controls over their networks and their industrial control system networks. TVA has been responsive, has implemented most, if not all, of our recommendations and we have closed them out.

Mrs. BLACKBURN. Thank you. With that, I will yield back.

Mr. STEARNS. Gentlelady yields back. Ms. Myrick is recognized for 5 minutes.

Mrs. MYRICK. Thank you, and really, this is for any of you, but it concerns giving the cybersecurity threats and the weaknesses that were identified in the GAO report and in the Inspector General for the Department of Energy's report. It seems to be that cybersecurity is not a real high priority with some companies today, and given the wealth of information that is out there about the threats that exist—I am also on Intel and we deal with this all the time. And it just seems apparent to me that we—that companies really aren't taking this as seriously as they should. Not just companies, of course, dealing with the electric grid, but other companies as well when it comes to how they fit into the big picture in the country.

Is it because they don't feel that there is any incentive for them to do it in any way? I am at a little of a loss, I guess, because some of them just seem to be kind of blase about it, even though they are so vulnerable. It is unreal and then it affects the rest of us from a national security standpoint.

Mr. TRIMBLE. I would answer in two ways. One, from our expert panel that we convened one of the concerns that they had was confusion and uncertainty over who is in charge in terms of——

Mrs. MYRICK. OK.

Mr. TRIMBLE [continuing]. Where the guidance was given, the complexity of the regulatory oversight. From—if you are putting yourself in the producer of the utilities perspective, they are faced with—so the standards haven't been adopted, even though—even

when they are adopted, they are voluntary, and then if you are a producer under State control, you don't have anything from the States. To recover those costs, to make those investment decisions, those costs have to be recoverable. There is no necessary guarantee that you will recover those costs if you make those investments in this uncertainty.

So again, this goes back to our recommendation as to when you adopt, you need to closely monitor to what extent these standards are being followed and to what extent they are effective, and make changes quickly. So it really, you know, sort of asking the system something it hasn't done necessarily in the past, which is act quickly and sort of more nimbly than it has. But I think part of the answer is really I would just put yourself in the shoes of the utility when faced with making those decisions and trying to balance the cost and benefits and risks that you are looking at.

Mr. WILSHUSEN. And I want to add to that. Also in some instances these utilities may or may not be fully aware of some of the threats and risks that are there, particularly certain incidents. In many cases, some of the most actionable and alert information may not necessarily be able to be shared with the utilities because it is classified.

Mrs. MYRICK. Right.

Mr. WILSHUSEN. And so the information sharing equation is also a factor in terms of the agency—or the utilities receiving timely and actionable information.

We issued a report a year ago or 2 years ago that dealt with the expectations and the delivery of those expectations between the public-private partnership model that is currently in use, and many—this is not only just the electricity industry, but also across other critical infrastructure sectors, in that most of the respondents on the private sector side indicated that—in fact, 98 percent of them said that receiving timely, actionable, alert and threat information was very important to them, but only 27 percent of them responded and said that their Federal partners were greatly or moderately providing that information to them.

Mrs. MYRICK. So it is not a resistance or lack of understanding on the part of the companies from your perspective and what you are seeing, it is really that they—that this aspect of who is in charge and who they report to and how they get the information and what information they get is really the problem?

Mr. WILSHUSEN. It is a contributing factor.

Mrs. MYRICK. OK. Anybody else wish to comment?

Then I yield back, Mr. Chairman. Thank you.

Mr. STEARNS. Gentlelady yields back. The gentleman from Georgia, Mr. Gingrey, is recognized for 5 minutes.

Mr. GINGREY. Thank you, Mr. Chairman, and I am going to address my first question to all three of you, and I think I will start with Mr. Campbell.

Each of you mentioned in the January 2012 report issued by the Department of Energy's Inspector General that 36 of the 99 grant recipients did not have the sufficient security plans in place to provide further risk determent, despite the fact that the Federal Government has spent, I think you said $3.5 billion in taxpayer money for this Smart Grid Investment Grant Program. Now while I am

disappointed that for scheduling purposes it prevented the DOE Inspector General from being here today, I would like to ask each of you your thoughts on these three questions, and I will start with Mr. Campbell. What are the potential implications of these insufficient security controls?

Mr. CAMPBELL. Well basically smart grid devices are being developed that may not have full cybersecurity mechanisms built in. So if these devices do actually make it to market, there could be problems with cybersecurity of the devices going forward.

Mr. GINGREY. Mr. Trimble?

Mr. TRIMBLE. Yes, I will—what I would add to that, and I will defer to my colleague on the cyber aspect of this, that one of the downsides if you end up with devices that don't meet the standards or aren't sufficiently protected and then the utility has to pull those out, you have created a problem in terms of who is going to pay for that mistake, because they will go to the public utility to recover those costs, the public is not going to want to pay for the mistake, and so you will have a very contentious situation.

Mr. WILSHUSEN. Yes, I would agree with both Mr. Trimble and Mr. Campbell in that it could create opportunities where key controls are not being implemented into these devices or not being implemented in whatever the initiative and grant initiative had was developing. One thing that was noted by the IG is that these were approved even though the Department had requested that the plans be updated, which they were, but not in all instances were those key controls addressed and the Department has to approve that.

According to the IG report, if I read that correctly—again, I defer to the DOEIG on that—is that there was apparently an emphasis on the part of the Department to make sure that these grants were approved and gotten out.

Mr. GINGREY. We—as the chairman said in his opening remarks, we had hoped to have the IG from DOE here today, and hopefully we will schedule another hearing and hear from him.

But going back to Mr. Campbell, throughout the life of the grant, is it feasible that these problems that exist could still be corrected?

Mr. CAMPBELL. The DOE's office has responded that it will require the applicant grantees to update their cybersecurity plans, I believe it is by April of this year.

Mr. GINGREY. All right, Mr. Trimble and Mr. W., you all have some comments on that as well?

Mr. WILSHUSEN. Yes. I would just also add that in the report, the IG indicated that the Department was also going to be, as part of their annual review process of these grant initiatives, were to review the recipient's implementation of those cybersecurity controls in their plans.

Mr. GINGREY. And then the last part of this question, and I see I am probably only going to get one question in in the allotted 5 minutes, but with this report in mind, the DOE Inspector General report, do you know of any instances in which the smart grid for which the grant program was supposed to bolster has been compromised from a security standpoint? Mr. Campbell, any specifics there?

Mr. CAMPBELL. I am not aware of any specifics.

Mr. GINGREY. Mr. Trimble?
Mr. TRIMBLE. No, sir.
Mr. WILSHUSEN. No, sir.
Mr. GINGREY. OK. I do have a little bit of time left. Let me go—let us see, back to—well that is all right. I will just save that if there is a second round.
Mr. Chairman, I yield back the balance of my time.
Mr. STEARNS. All right, gentleman yields back. We will do a second round and I will start.
Mr. Wilshusen, in your testimony you stated that Department of Energy Inspector General found that under the Smart Grid Investment Grant Program, recipients were not always complete or lacked sufficient detail in security controls in their submissions to Department of Energy. Is that correct?
Mr. WILSHUSEN. Yes, sir.
Mr. STEARNS. Is that a big deal?
Mr. WILSHUSEN. Yes, it can be.
Mr. STEARNS. And why, specifically?
Mr. WILSHUSEN. Well, if those——
Mr. STEARNS. Why is it a big deal?
Mr. WILSHUSEN. Well, if it is——
Mr. STEARNS. I think it is a big deal, but I just want you to confirm it.
Mr. WILSHUSEN. If those plans are incomplete and do not identify key controls that should be implemented on as part of these smart grid initiatives, that could lead to vulnerable devices and therefore, may subject those devices to increased risk of being compromised.
Mr. STEARNS. So you have a smart meter device being purchased with government grant money that lacks the proper security features and if the guarantees don't have specific or detailed security plans when installing them into the customer's homes, isn't that it?
Mr. WILSHUSEN. That could be a possibility.
Mr. STEARNS. Mr. Trimble, is it conceivable that during the life of the grant period, that these security plans are not complete, are not implemented properly, unless made a condition of the grantee to receive the funding? Should we do that?
Mr. TRIMBLE. I believe that should have been a requirement or——
Mr. STEARNS. Do you have your mic on?
Mr. TRIMBLE. I believe that is what the IG indicated, but that was not our work so I can't speak authoritatively.
Mr. STEARNS. Do you know of any specific examples that I could hear from you, or Mr. Wilshusen?
Mr. WILSHUSEN. Well in the IG report, they identified three of the five security plans that it reviewed. These were the plans that had already been initially identified by the Department as having deficient or shortcomings in the security programs, and then updated by the recipient or the grantee recipients, and they identified that three of the five still had the shortcomings and did not contain complete information. And some of that information dealt, as I recall, with the auditing and some of the technical security controls associated with those initiatives. But as far as more detailed information, I did not review or have access to the work papers supporting the report by the IG.

Mr. STEARNS. Is this all primarily in the smart meter technology? Is that where all this concern is?

Mr. WILSHUSEN. With the IG's report, I don't think it was specific to that. I don't recall if it was specifically mentioned.

Mr. STEARNS. Isn't that where most of the investment is?

Mr. WILSHUSEN. That also I don't know.

Mr. STEARNS. Yes, Mr. Trimble?

Mr. TRIMBLE. I believe it was in a broader range. I thought the bulk of the money was into other systems like phase measurement units and things like that, but again, we haven't done work in that area.

Mr. STEARNS. Mr. Campbell, how many, in your opinion, smart grid cyber incidents have there been?

Mr. CAMPBELL. I am not familiar with the total number, but from I have heard in discussion there has been quite a few cybersecurity incidents.

Mr. STEARNS. Under 10, under 100?

Mr. CAMPBELL. Probably more than that.

Mr. STEARNS. Under 1,000?

Mr. CAMPBELL. I couldn't say with any specific.

Mr. STEARNS. So you have no knowledge of how many specific system cyber attacks there have been, incidents, then?

Mr. CAMPBELL. No, sir.

Mr. WILSHUSEN. Mr. Chairman——

Mr. STEARNS. Yes, sure.

Mr. WILSHUSEN [continuing]. If I might add, I am not even sure if there is a monitoring process or reporting mechanism in place for that information to be reported and collected.

Mr. STEARNS. Mr. Campbell, do you think that waiting 3 years for the grant recipients to implement vigorous cybersecurity plans could lead to cybersecurity gaps and subsequent compromises in the system integrity?

Mr. CAMPBELL. It is my opinion——

Mr. STEARNS. If you might pull the mic just a little closer.

Mr. CAMPBELL. It is my opinion that during the 3-year period for development, there should be adequate time for the DOE to take a look at the requirements in regard to cybersecurity, but we should also note that cyber threats are continuing to change, so any regulations that you may put in place may not be adequate when the final product rolls out.

Mr. STEARNS. OK. My last question, Mr. Wilshusen, are there different cybersecurity challenges that are vulnerabilities for government-run utility services, such as the Bonneville Power Administration versus privately-run utility services?

Mr. WILSHUSEN. We haven't looked at the specific security controls at private utilities. We have looked at them at TVA, and identified a number of security vulnerabilities——

Mr. STEARNS. At TVA?

Mr. WILSHUSEN. At TVA, yes, as this was the report that was referred to earlier. But my understanding is, it is probably likely that what we found at TVA will probably be—could be found at other public utilities as well, you know, of a similar type of electrical power generation and some transmission.

Mr. STEARNS. Mr. Trimble, anyone else, do you have any comments in reference to the private versus government-run utilities?

Mr. TRIMBLE. No, I would defer to Greg on that.

Mr. STEARNS. Mr. Campbell, any suggestions?

Mr. CAMPBELL. No, that seems to be a reasonable response. Private utilities seem to have many of the same systems that public utilities have.

Mr. WILSHUSEN. And one—if I may just add more broadly, when we looked at other sectors, for example, we looked at communications network operated by private sector organizations, we found vulnerabilities in their networks that were similar to the vulnerabilities that we find in the networks of Federal agencies. Now while that is not exactly electricity industry, but I would be fairly confident to say that vulnerabilities identified in government systems are going to probably be found in private sector systems in some respects because the Federal Government security standards and guidelines typically are as robust, if not more robust, than private sector guidelines in many cases.

Mr. STEARNS. Thank you. My concluding comment is if it hits one sector, it hit government utility versus private utility, it is probably the same kind of statistic.

Mr. WILSHUSEN. I would agree with that comment, which is all the more reason why there should be an effective and robust information sharing capability between the public and private sectors.

Mr. STEARNS. With that, my time is expired.

Ms. DEGETTE. Thank you. Thank you, Mr. Chairman.

I want to follow up on the chairman's question about reporting, because I think I shared his concern. Mr. Campbell and Mr. Wilshusen, both of you—all three of you said we don't have any kind of specific knowledge as to how many cyber attacks there have been. And Mr. Wilshusen, you said that we don't really have a systematic approach to reporting. Would it be possible to develop that kind of systematic approach, and if we did, how would it look, who would be in charge of it, et cetera?

Mr. WILSHUSEN. Well, we haven't done the work to come up and just say definitively, but there are some reporting mechanisms in place now. For example, the Department of Homeland Security and the U.S. Cert Federal agencies are required to report their security incidents that occur at their sites to U.S. Cert, and then U.S. Cert collects that information and makes reports on it, summarizes it, identified trends, and also then provides alerts to other Federal agencies.

Private sector organizations can also report through to the U.S. Cert, although in terms of having something formal and required, that is—presently does not exist.

Mr. DEGETTE. Well, so there is a structure that perhaps you could do it, there is just no requirement to do it, is that what you are saying?

Mr. WILSHUSEN. It may be a model that could be considered if one was to develop such a reporting structure.

Ms. DEGETTE. Do you think it would be important to have some sense of incidences of cyber attacks?

Mr. WILSHUSEN. Oh, I certainly do, yes.

Ms. DEGETTE. What do you think, Mr. Campbell?

Mr. TRIMBLE. What I would—I am sorry, what I would just jump in on this point is when we convened our expert panel, one of the challenges and problems that the experts identified was the lack of information sharing among the utilities and the generators and the government on precisely these issues, the cyber attacks, successful or not.

Ms. DEGETTE. So did—so now we have identified—and Mr. Campbell, would you agree there is a problem?

Mr. CAMPBELL. Yes, but I would also think confidentiality of reporting would be a key factor in any system that is developed.

Ms. DEGETTE. Right, so who would develop that system? I mean, we are super good at identifying problems, but now how do we move towards a solution? Anyone?

Mr. WILSHUSEN. Well, within the Federal Government, you know, DHS has the overriding responsibility as the focal point for protecting critical infrastructures. Each of the 18 critical sectors—infrastructure sectors have sector-specific agencies that monitor it for that particular——

Ms. DEGETTE. Yes, I understand all this, so you would say it would probably be DHS to develop this?

Mr. WILSHUSEN. They have a model in place where Federal agencies are required to. It would be a likely place to start.

Ms. DEGETTE. OK, thank you.

Mr. Campbell, I want to follow up on the point about privacy that you just raised, because I don't know if the three of you saw the story in "The Washington Post" today where what it talked about was the National Security Agency is pushing to expand its role in protecting private sector computer networks from cyber attacks. The White House has been concerned about privacy concerns, and then the story said "The most contentious issue was a legislative proposal last year that would have required hundreds of companies that provide such critical services as electricity generation to allow their internet traffic to be continuously scanned using computer threat data provided by the spy agency. Companies would have been expected to turn over evidence of potential cyber attacks by the government." So this really is an issue about how you balance security versus privacy. We have been debating this pretty much since September 11, 2001.

And so maybe, Mr. Campbell, you can talk to me if you have some perspective on the tradeoff of cybersecurity versus privacy.

Mr. CAMPBELL. Well, I would say that cybersecurity versus privacy is a key issue. Other than that, I would say that we—CRS is looking at the issue and we would be happy to talk to you about it at a later time.

Ms. DEGETTE. And you released—CRS released a report on privacy and cybersecurity concerns earlier this month, did it not?

Mr. CAMPBELL. Yes.

Ms. DEGETTE. And so let me ask you, what information can smart meters collect about the people in the households who have them? I mean, what is the security issue?

Mr. CAMPBELL. Well, smart meters collect information on the use of electricity, and so the idea is that smart meters conceivably could develop a profile of the use of electricity within the home. Now if the information is accumulated at a high enough level, then

individual use of information could be lost, but that is an issue that is under development and I think in various States there are various rules concerning smart meter——

Ms. DEGETTE. And that information, it could determine the behavioral patterns of the residents in the home, correct?

Mr. CAMPBELL. Correct.

Ms. DEGETTE. So like burglar could figure out—could use a smart meter to figure if a family was on vacation or not, right?

Mr. CAMPBELL. If they were sophisticated enough to access the information.

Ms. DEGETTE. Or a marketer could even use information about what appliances a consumer might be using to target that consumer, right?

Mr. CAMPBELL. Possibly.

Ms. DEGETTE. So that—I mean, we wouldn't naturally think that there would be security issues relating to these meters, but that is something we need to consider and balance out, right?

Mr. CAMPBELL. Correct.

Ms. DEGETTE. Thank you, Mr. Chairman.

Mr. STEARNS. Gentleman from Georgia is recognized for 5 minutes.

Mr. GINGREY. Thank you, Mr. Chairman.

You know, as I sit here and think about this program and the $3.5 billion worth of grant money going towards these companies, grantees, 99 of them to help develop the smart grid, I also think about the $19 billion that was in the stimulus money for fully developing health information technology, you know, the Offices of National Coordinator and his salary and all the employees there to make sure that people, companies small and large that got grants from that $19 billion pot to help develop health information technology that is fully coordinated, it just makes me concerned that these grantees under this program to develop the smart grid are not following the guidelines that they should follow and in the final analysis 3 years from now we will have wasted a lot of money.

I want to ask you specifically, you mentioned—and maybe some of my colleagues had asked a question about NIST's involvement, the National Institute of Standards and Technology, the 850–3 program as compared, let us say, to the North American Electric Reliability Corporation's critical infrastructure protection standards. Now how do those two compare and are they overlapping? Are they similar? Is one better than the other? What standards should we require of these grantees as they develop these programs with taxpayer money? Mr. Campbell?

Mr. CAMPBELL. My knowledge that the NERC reliability critical infrastructure standards are just applied to those on the bulk electric system, so when we are talking about the Smart Grid Investment Grant Program, that is looking at developing products, so I think what we are talking about is two different types of requirements.

Mr. GINGREY. Mr. Trimble and Mr. Wilshusen?

Mr. WILSHUSEN. I will field that one. Also there is—we actually compared the NERC's eight cyber—critical infrastructure protections cybersecurity reliability standards to the controls that are identified and NIST Special Publication 850–3, and we found that

of the 198 controls in 850–3 that the NIST or the NERC standards had about 151 of those. One of the issues that the IG reported on in its report, also in addition to what Mr. Campbell said, is that those standards apply only to the bulk electricity supply, but there further only apply to those assets that the entities within that sector have designated as a critical asset. And so if the entity has not identified any critical assets, then those standards would not necessarily apply.

And the IG report also indicated that back in 2009, the former chief information security officer of NERC did a survey and identified that about, I think it was 36 percent of the power generators, or those entities with power generation and about 67 percent of those responsible for transmitting bulk power had identified only—at least one critical asset. So that left a fair number of—or at least a fair percentage of entities that produce power or transmit it that did not identify any critical assets.

Mr. GINGREY. Mr. Trimble?

Mr. TRIMBLE. I would just—my expertise is not cyber, so I will—so to simplify that, the issue as I sort of have come to understand it is the NERC CIP standards apply to—for critical infrastructure protection but it is limited because it is just bulk power and it is just those that the industry have identified as being critical assets. But industry self-identification has not been exactly—has been identified as comprehensively as it could be.

The NIST standards that we are talking about for cyber pursuant to ISA are voluntary, primarily focused on interoperability and cyber threats. The limitation there is that FERC's sort of bailiwick is, again, bulk power so it doesn't get into anything beyond sort of interstate transmission, if you will. If you are getting into the State level, those guidelines, those standards, even though voluntary, don't kick in. If you get down to the city level, like New York, they don't kick in. So you have got this patchwork where there is a whole bunch of places with no standards that kick in.

Mr. GINGREY. My time is expired, but I just want to say that, you know, it is pretty much green eyeshades sort of stuff, but hugely important, and of course, you are bringing important information to us, the members of the subcommittee, and I think this is very beneficial. I deeply appreciate you being here today, and thank you for your testimony.

Mr. Chairman, I yield back.

Mr. STEARNS. Thank the gentleman and we are getting ready to conclude the hearing, and I, as chairman, have the opportunity to give a closing remark. I would say it has been brought up here and also I remember in our July hearing. Department of Homeland Security fields all this information dealing with cybersecurity and then gives it to U.S. Cert agency, and they offer the documentation, as I understand it, to the private industry, so it sort of filters down that way. Is that correct?

Mr. WILSHUSEN. I believe it is, yes.

Mr. STEARNS. Well, my concern is, just like the 9/11 Commission said, there was not full communication between all the government agencies as well as private industries on what—to alert them of possible information it could have thwarted and stopped the 9/11 attack. I see it is clear here today in the conversation that there

is not really full adequate communication between the private sector and the government sector dealing with utilities with cybersecurities, and I think this is a warning that we should all take into effect or we might be sitting here at a later date with something that is very serious.

I want to thank the witnesses for their time and effort, and the subcommittee is adjourned.

[Whereupon, at 11:37 a.m., the subcommittee was adjourned.]