S. HRG. 112–529

ELECTRIC GRID SECURITY

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

TO

EXAMINE THE STATUS OF ACTION TAKEN TO ENSURE THAT THE ELECTRIC GRID IS PROTECTED FROM CYBER ATTACKS

JULY 17, 2012

Printed for the use of the
Committee on Energy and Natural Resources

U.S. GOVERNMENT PRINTING OFFICE

75–809 PDF WASHINGTON : 2012

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 NATURAL RESOURCES

JEFF BINGAMAN, New Mexico, *Chairman*

RON WYDEN, Oregon
TIM JOHNSON, South Dakota
MARY L. LANDRIEU, Louisiana
MARIA CANTWELL, Washington
BERNARD SANDERS, Vermont
DEBBIE STABENOW, Michigan
MARK UDALL, Colorado
JEANNE SHAHEEN, New Hampshire
AL FRANKEN, Minnesota
JOE MANCHIN, III, West Virginia
CHRISTOPHER A. COONS, Delaware

LISA MURKOWSKI, Alaska
JOHN BARRASSO, Wyoming
JAMES E. RISCH, Idaho
MIKE LEE, Utah
RAND PAUL, Kentucky
DANIEL COATS, Indiana
ROB PORTMAN, Ohio
JOHN HOEVEN, North Dakota
DEAN HELLER, Nevada
BOB CORKER, Tennessee

ROBERT M. SIMON, *Staff Director*
SAM E. FOWLER, *Chief Counsel*
MCKIE CAMPBELL, *Republican Staff Director*
KAREN K. BILLUPS, *Republican Chief Counsel*

CONTENTS

STATEMENTS

APPENDIX

ELECTRIC GRID SECURITY

TUESDAY, JULY 17, 2012

U.S. SENATE,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The committee met, pursuant to notice, at 10 a.m. in room SD–366, Dirksen Senate Office Building, Hon. Jeff Bingaman, chairman, presiding.

OPENING STATEMENT OF HON. JEFF BINGAMAN, U.S. SENATOR FROM NEW MEXICO

The CHAIRMAN. OK. Why don't we go ahead and get started?

I am advised that Senator Murkowski is on her way, but urged us to proceed. This morning's hearing is to examine the status of actions taken by the Federal Energy Regulatory Commission or FERC, and the North American Electric Reliability Corporation or NERC, and the States to protect the electric grid from computer attacks on their facilities and control systems.

I don't think we need to talk much about the serious nature of this issue. Last week, we experienced a week-long outage in much of this region. It was a weather-related outage, but it demonstrates how important reliable service on the electric grid is.

We read every day of newly discovered attacks or threats on computer systems in this country and around the world. According to the Director of National Intelligence, there's been a dramatic increase in the frequency of malicious cyber activity, targeting U.S. computers and networks, including a more than tripling of the volume of malicious software, since 2009. So, the threat is real, and it is serious.

In 2005, we gave FERC the authority to name an entity to develop and enforce standards to protect the reliability of the grid. I believe that there are two things that we can say about the system that has emerged since then.

First, the current reliability system does have a mandatory character, so the electric grid is the only critical infrastructure in this country that has some form of an enforceable standard for cybersecurity.

Second, the current reliability system that has emerged is cumbersome and overly complicated. This may be adequate to deal with reliability concerns like, standards for trimming trees so that they do not fall on transmission lines, but when it comes to cyber attacks, I am concerned that the current system is not adequate.

The process to develop standards started in earnest in 2006 when NERC filed a series of reliability standards with NERC; a

number of them related to cybersecurity and FERC found them wanting. In a series of filings since then, NERC has corrected some of the shortcomings that the FERC highlighted.

As recently as April, version 4 of the cyber standards was approved, with the provision that NERC address the remaining inadequacies by the end of the first quarter of next year. That means that we are here today in this committee, 7 years after we passed the law, and we are still waiting for this process to produce the full set of adequately protective standards that we need. That cumbersome process has to address a threat, whose nature is rapidly changing. The standards that are in place may not be flexible enough to deal with emerging threats, and we still do not have an effective system in place to require action in the face of an imminent cyber attack.

NERC has developed a system of alerts to help the industry with newly discovered threats. I will have some questions about that system, how that system is working in practice.

The concerns that have prompted this hearing are ones that have resulted in bipartisan cybersecurity legislation that we have reported from this committee, both this Congress and in the last Congress. In 2010, Senator Murkowski and I agreed on an expedited approach to cybersecurity standards that was centered at FERC and that passed the committee unanimously. That bill was hotlined for passage in the Senate at the end of the last Congress. It ran into holes from two of our colleagues and, perhaps, more.

Last year, Senator Murkowski and I reworked the proposal into one that featured a greater role for NERC, but allowed FERC to set effective deadlines for action and also gave the Secretary of Energy emergency cybersecurity authority. Once again, that bill passed this committee unanimously.

I don't believe that the cyber threat facing the electric grid has gotten any less serious since last year, when we acted on a bipartisan basis to pass our legislation out of the committee.

In the testimony for today's hearing, there are suggestions that there are additional cyber issues that also need focused attention, particularly with respect to the implementation of smart grid technologies. We need to address these vulnerabilities that are clearly before us. The bill that passed this committee unanimously would be an excellent place to start. It did a good job of balancing the need to avail ourselves of the expertise in industry on these issues, with the need to act expeditiously. Nothing since then has changed the need for clear authority to deal with immediate emergencies and longer-term vulnerabilities.

As we all agreed last year, processes that take years to bear fruit, may be sufficient for less urgent reliability issues, but not for the challenges we face in cybersecurity. So, I look forward to hearing from the witnesses.

Let me defer to Senator Murkowski for any opening statements she would like to make.

STATEMENT OF HON. LISA MURKOWSKI, U.S. SENATOR FROM ALASKA

Senator MURKOWSKI. Thank you, Mr. Chairman. Welcome, to all the witnesses this morning. I appreciate the hearing today.

Of course, the purpose of this morning's hearing is to take another—and, perhaps, a closer—look at the ongoing efforts to protect our Nation's grid from cyber attacks. I do think it is important that we recognize the tremendous amount of work that has already gone into safeguarding the grid's reliability.

Back in 2005, Congress directed FERC to select an electric reliability organization, now known as the NERC, and tasked it with establishing and enforcing mandatory reliability standards, including cyber standards.

I think it has been a difficult, time-consuming process, but I would like to commend NERC for the professional and balanced way that it has consistently met its responsibilities.

There is no question, Mr. Chairman, as you point out, that cybersecurity is an absolutely critical issue. It should be addressed by this Congress. I am certain that every member of this body is concerned that our Nation may be vulnerable to cyber attacks that could have severe economic and security ramifications.

We see stories about this just about every day, on individuals, on companies, on the Government—these cyber incursions. It is time for us to take steps to protect ourselves from a very real and emerging threat.

Last year, as you point out, Mr. Chairman, the Energy Committee did report out a sector-specific cybersecurity bill. This action was taken in response to the majority leader's directive to the various committees with cyber jurisdiction to produce their own bills. At which point, they would all be stitched together into a single piece of cybersecurity legislation.

I think, Mr. Chairman, that the Energy Committee was the only committee to have actually done just exactly that. But since that time, now over a year ago, circumstances have evolved. I think there is near agreement that we need a comprehensive approach to the cybersecurity problem. Some would have us believe that only the Department of Homeland Security and a host of new Federal regulations will protect us from persistent cyber threats.

But I don't think that heavy-handed static requirements from yet another Federal regulator will address the very real threat that we face. I think, instead, that we need a much more nimble approach to deal with cyber-related threats that are constantly growing and always changing.

I have joined with a number of other Ranking Member colleagues to introduce, what we're calling, the Secure IT Act. This is S. 3342. I think it's a pragmatic approach to this issue. We focus on 4 areas that, I believe, we can draw bipartisan support for. That is within the area of information sharing. We have got FISMA reform, criminal penalties, additional research.

But what the Secure IT Act does not do, I think, is equally important. It does not add new layers of bureaucracy and regulation that will serve little purpose and achieve meager results. I think it is a pretty straightforward approach to cybersecurity that can go a long ways in addressing our problem.

Mr. Chairman, I thank you for convening this hearing. I look forward to hearing what the witnesses have to say on the actions that have been taken to date, as well as the ongoing efforts to secure the grid at both the transmission and the distribution level.

The CHAIRMAN. Thank you very much. I would just point out that the Majority Leader has advised, I think, everyone who's—listens to his statements that he hopes we can move to cybersecurity legislation on the Senate floor between now and the time we adjourn in August, and so, I think this hearing is particularly timely for that reason.

Let me introduce our 4 witnesses.

First is, Mr. Joseph McClelland, Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission.

Next is, Mr. Gregory C. Wilshusen, who is the Director of Information and Technology, with the Government Accountability Office.

Third is, Mr. Gerry Cauley, who is President and Chief Executive Officer with the North American Electric Reliability Corporation, NERC. Thank you very much for being here.

Mr. Todd Snitchler, who is the Chairman of the Public Utility Commission of Ohio. Thank you very much for being here.

Mr. McClelland, why don't you start. If each of you could take 5 or 6 minutes and give us the main things you think we need to understand about the issue. We will then have some questions.

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

Mr. MCCLELLAND. Thank you, Mr. Chairman.

Mr. Chairman, Ranking Member, and members of the committee, thank you for the privilege to appear before you today to discuss the security of the electric grid. My name is Joe McClelland, and I am the Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission.

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

The Commission is committed to protecting the reliability of the Nation's bulk power system. Nevertheless, limitations in Federal authority do not fully protect the grid against physical and cyber threats. My testimony summarizes the Commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act, and the Commission's implementation of that authority, with respect to cyber-related reliability issues, primarily through Order 706

In the Energy Policy Act of 2005, Congress entrusted the Commission with a major new responsibility, to oversee mandatory enforceable reliability and cybersecurity standards for the Nation's bulk power system. This authority is in new section 215 of the Federal Power Act.

Under the new authority, FERC cannot author or modify reliability standards, but must select an Electric Reliability Organization, or ERO, to perform this task. The ERO develops and proposes reliability standards or modifications for the Commission's review, which it can then either approve or remand.

If the Commission approves the proposed reliability standard, it applies to the users, owners, and operators of a bulk power system and becomes mandatory in the United States. If the Commission

remands a proposed standard, it is sent back to the ERO for further consideration.

The Commission selected the North American Electric Reliability Corporation, or NERC, as the ERO. It is important to note that FERC's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, which excludes Alaska and Hawaii distribution systems, and can exclude transmission facilities in certain large cities, such as New York.

In addition to the reliability authority, FERC is also charged with oversight of the cybersecurity of the bulk power system. As is the case with non-security issues, FERC's authority under 215 of our cybersecurity is exercised through the reliability standards developed by the ERO and approved by FERC. Pursuant to this duty, FERC approved 8 cybersecurity standards known as the Critical Infrastructure Protection standards, or CIP standards, proposed by NERC, while concurrently directing modifications to them in January 2008.

Three sets of modifications, responding to the Commission's directives, have been received from the ERO, and the last was approved earlier this year.

Although the CIP standards are approved, full compliance with these revised standards will not be mandatory until 2014. More importantly, in approving the latest revision of the CIP standards, the Commission recognized that they are an interim step and raised its concern that the newly revised standards do not provide enough protection to satisfy the Commission's January 2008 Order. Thus, the Commission established a deadline for the end of the first quarter of 2013, for NERC to file standards in compliance with the outstanding directives in that Order.

Physical attacks against the power grid can cause equal or great destruction than cyber attacks. One example of a physical threat is an electromagnetic pulse, or EMP, event.

In 2001, Congress established a commission to assess the threat from EMP. In 2004 and, again, in 2008, the Commission issued its reports. Among the findings in the reports were that a single EMP attack could seriously degrade or shut down a large part of the electric power grid. Depending upon the attack, significant parts of the electric infrastructure could be, "Out of service for periods measured in months to a year or more."

In addition to man-made attacks, EMP events are also naturally generated, caused by solar flares and storms, disrupting the Earth's magnetic field. Such events can be powerful and can also cause significant and prolonged disruptions to the power grid.

The standards development system utilized under FPA 215 develops mandatory reliability standards, using an open and inclusive process, based on consensus. Although it can be an effective mechanism with dealing with the routine requirements of the power grid, it is inadequate when addressing threats to the power grid that endanger national security.

Despite its active role in approving reliability standards, FERC's current legal authority is insufficient to assure direct, timely, and mandatory action to protect the grid, particularly where certain information should not be publicly disclosed.

Any new legislation should address several key concerns. First, legislation should allow the Federal Government to take action before a cyber or physical national security incident has occurred.

Second, any legislation should ensure appropriate confidentiality of the sensitive information submitted, developed, or issued under this authority.

Third, if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would not authorize Federal action to mitigate cyber or other national security threats to reliability that involve certain critical facilities in major population areas.

Finally, it is important that entities be able to recover costs that they incur to mitigate vulnerabilities and threats.

Thank you for your attention today. I am available to address any questions that you may have.

[The prepared statement of Mr. McClelland follows:]

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

Mr. Chairman, Ranking Member and Members of the Committee:

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

The Commission is committed to protecting the reliability of the nation's bulk electric system; nevertheless, the Commission's current authority is not adequate to address cyber or other national security threats to the reliability of our transmission and power system. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our government and economy and helps ensure the health and welfare of our citizens.

I will describe how limitations in Federal authority do not fully protect the grid against physical and cyber threats. My testimony also summarizes the Commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act (FPA) and the Commission's implementation of that authority with respect to cyber related reliability issues primarily through Order No. 706.

BACKGROUND

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

The Commission may approve proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." The Commission itself does not have authority to modify proposed standards. Rather, if the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or

modification on a specific matter but it does not have the authority to modify or author a standard and must depend upon the ERO to do so.

Limitations of Section 215 and the Term "Bulk Power System"

Currently, the Commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any federal installations located therein. The current interpretation of "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas. The Commission directed NERC to revise its interpretation of the bulk power system to eliminate inconsistencies across regions, eliminate the ambiguity created by the current discretion in NERC's definition of bulk electric system, provide a backstop review to ensure that any variations do not compromise reliability, and ensure that facilities that could significantly affect reliability are subject to mandatory rules. NERC has recently filed a revised definition of the term bulk power system, and the Commission has solicited comments on its proposal to accept NERC's revised definition. However, it is important to note that section 215 of the FPA excludes local distribution facilities from the Commission's reliability jurisdiction, so any revised bulk electric system definition developed by NERC will still not apply to local distribution facilities.

Critical Infrastructure Protection Reliability Standards

An important part of the Commission's current responsibility to oversee the development of reliability standards for the bulk power system involves cyber related reliability issues. In August 2006, NERC submitted eight proposed cyber standards, known as the Critical Infrastructure Protection (CIP) standards, to the Commission for approval under section 215. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "Bulk Electric System." Under NERC's implementation plan for the CIP standards, full compliance became mandatory on July 1, 2010.

On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards while concurrently directing NERC to develop significant modifications addressing specific concerns. The Commission set a deadline of July 1, 2009 for NERC to resolve certain issues in the CIP reliability standards, including deletion of the "reasonable business judgment" and "acceptance of risk" language in each of the standards. NERC concluded that this deadline would create a very compressed schedule for its stakeholder process. Therefore, it divided all of the changes directed by the Commission into phases, based on their complexity. NERC opted to resolve the simplest changes in the first phase, while putting off more complex changes for later versions.

NERC filed the first phase of the modifications to the CIP Reliability Standards (Version 2) on May 22, 2009. In this phase, NERC removed from the standards the terms "reasonable business judgment" and "acceptance of risk," added a requirement for a "single senior manager" responsible for CIP compliance, and made certain other administrative and clarifying changes. In a September 30, 2009 order, the Commission approved the Version 2 CIP standards and directed NERC to develop additional modifications to certain of them. Pursuant to the Commission's September 30, 2009 order, NERC submitted Version 3 of the CIP standards which revised Version 2 as directed. The Version 3 CIP standards became effective on October 1, 2010. This first phase of the modifications directed by the Commission in Order No. 706, which encompassed both Version 2 and Version 3, did not modify the critical asset identification process, a central concern in Order No. 706.

On February 10, 2011, NERC initiated the second phase of the Order No. 706 directed modification, filing a petition seeking approval of Version 4 of the CIP standards. Version 4 includes new proposed criteria to identify "critical assets" for purposes of the CIP reliability standards. On April 19, 2012, the Commission issued Order No. 761, approving the Version 4 CIP standards, which introduced "bright line" criteria for the identification of Critical Assets. The version 4 CIP standards do not go into effect until April 1, 2014. The currently effective CIP reliability standards allow utilities significant discretion to determine which of their facilities are "critical assets and the associated critical cyber assets," and therefore are subject to the requirements of the standards. It is important to note that although "critical assets" are used to identify subsequent "critical cyber assets," only the subset of "critical cyber assets"—which are self-determined by the affected entities—are subject to the CIP standards. As the Commission stated in Order No. 706, the identi-

fication of critical assets is the cornerstone of the CIP standards. If that identification is not done well, the CIP standards will be ineffective at maintaining the reliability of the bulk power system.

In the order approving NERC's Version 4 standards, the Commission recognized that Version 4 is an interim step and stated its concern that Version 4 does not provide enough protection to satisfy Order No. 706. Thus, the Commission established a deadline of end of first quarter of 2013 for NERC to file standards in compliance with the outstanding directives in Order No. 706.

The remaining CIP standards revisions to respond to the Commission's directives issued in Order No. 706 are still under development by NERC. It is important to note that the majority of the Order No. 706 directed modifications to the CIP standards have yet to be addressed by NERC. Until they are addressed, there are significant gaps in protection.

THE NERC PROCESS

As an initial matter, it is important to recognize how mandatory reliability standards are established. Under section 215, reliability standards must be developed by the ERO through an open, inclusive, and public process. The Commission can direct NERC to develop a reliability standard to address a particular reliability matter. However, the NERC process typically requires years to develop standards for the Commission's review. In fact, the CIP standards approved by the Commission in January 2008 took approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for stakeholder comment, are open, and are generally based on the procedures of the American National Standards Institute. The NERC process is intended to develop consensus on both the need for, and the substance of, the proposed standard. Although inclusive, the process is relatively slow, open and unpredictable in its responsiveness to the Commission's directives. This process requires public disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments. NERC-approved standards are then submitted to the Commission for its review.

The procedures used by NERC are appropriate for developing and approving routine reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process can be a strength of the process. However, it can be an impediment when measures or actions need to be taken to address threats to national security quickly, effectively and in a manner that protects against the disclosure of security-sensitive information. The current procedures used under section 215 for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations. Certain circumstances, such as those involving national security, may require immediate action, while the reliability standard procedures take too long to implement efficient and timely corrective steps. On September 3, 2010, FERC approved a new reliability standards process manual filed by NERC. While this manual includes a process for developing a standard related to a confidential issue, the new process is untested and it is unclear how the process would be implemented.

FERC rules governing review and establishment of reliability standards allow the agency to direct the ERO to develop and propose reliability standards under an expedited schedule. For example, FERC could order the ERO to submit a reliability standard to address a reliability vulnerability within 60 days. Also, NERC's rules of procedure include a provision for approval of "urgent action" standards that can be completed within 60 days and which may be further expedited by a written finding by the NERC board of trustees that an extraordinary and immediate threat exists to bulk power system reliability or national security. However, it is not clear NERC could meet this schedule in practice. Moreover, faced with a national security threat to reliability, there may be a need to act decisively in hours or days, rather than weeks, months or years. That would not be feasible even under the urgent action process. In the meantime, the bulk power system would be left vulnerable to a known national security threat. Moreover, existing procedures, including the urgent action procedure, could widely publicize both the vulnerability and the proposed solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, a reliability standard submitted to the Commission by NERC may not be sufficient to address the identified vulnerability or threat. Since FERC may not

directly modify a proposed reliability standard under section 215 and must either approve or remand it, FERC would have the choice of approving an inadequate standard and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. Under either approach, the bulk power system would remain vulnerable for a prolonged period.

This concern was highlighted in the Department of Energy Inspector General's January 2011 audit report on FERC's "Monitoring of Power Grid Cyber Security." The audit report identified concerns regarding the adequacy of the CIP standards and the implementation and schedule for the CIP standards, and concluded that these problems exist, in part, because the Commission's authority to ensure adequate reliability of the bulk electric system is limited. This report emphasizes the need for additional authority to ensure adequate cyber security over the bulk electric system.

Finally, the open and inclusive process required for standards development is not consistent with the need to protect security-sensitive information. For instance, a formal request for a new standard would normally detail the need for the standard as well as the proposed mitigation to address the issue, and the NERC-approved version of the standard would be filed with the Commission for review. This public information could help potential adversaries in planning attacks.

PHYSICAL SECURITY AND OTHER THREATS TO RELIABILITY

The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks and the Federal government should have no less ability to act to protect against such potential damage. One example of a physical threat is an electromagnetic pulse (EMP) event. EMP events can be generated from either naturally occurring or man-made causes. In the case of the former, solar magnetic disturbances periodically disrupt the earth's magnetic field which in turn, can generate large induced ground currents. This effect, also termed the "E3" component of an EMP, can simultaneously damage or destroy bulk power system transformers over a large geographic area. Regarding man-made events, EMP can also be generated by weapons. Equipment and plans are readily available that have the capability to generate high-energy bursts, termed "E1", that can damage or destroy electronics such as those found in control and communication systems on the power grid. These devices can be portable and effective, facilitating simultaneous coordinated attacks, and can be reused, allowing use against multiple targets. The most comprehensive man-made EMP threat is from a high-altitude nuclear explosion. It would affect an area defined by the "line-of-sight" from the point of detonation. The higher the detonation the larger the area affected, and the more powerful the explosion the stronger the EMP emitted. The first component of the resulting pulse E1 occurs within a fraction of a second and can destroy control and communication electronics. The second component is termed "E2" and is similar to lightning, which is well-known and mitigated by industry. Toward the end of an EMP event, a third element, E3, occurs. This causes the same effect as solar magnetic disturbances. It can damage or destroy power transformers connected to long transmission lines. It is important to note that effective mitigation against solar magnetic disturbances and non-nuclear EMP weaponry provides effective mitigation against a high-altitude nuclear explosion.

In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure. In 2004, the EMP commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.[2] Both electrical equipment and control systems can be damaged by EMP.

An EMP may also be a naturally-occurring event caused by solar flares and storms disrupting the Earth's magnetic field. In 1859, a major solar storm occurred, causing auroral displays and significant shifts of the Earth's magnetic fields. As a result, telegraphs were rendered useless and several telegraph stations burned

[1] Graham, Dr. William R. et al., Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (2004).

[2] Dr. John S. Foster, Jr. et al., Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (2008).

down. The impacts of that storm were muted because semiconductor technology did not exist at the time. Were the storm to happen today, according to an article in Scientific American, it could "severely damage satellites, disable radio communications, and cause continent-wide electrical black-outs that would require weeks or longer to recover from."[3] Although storms of this magnitude occur rarely, storms and flares of lesser intensity occur more frequently. Storms of about half the intensity of the 1859 storm occur every 50 years or so according to the authors of the Scientific American article, and the last such storm occurred in November 1960, leading to world-wide geomagnetic disturbances and radio outages. The power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced currents. The damage or destruction of numerous transformers across the country would result in reduced grid functionality and even prolonged power outages.

In March 2010, Oak Ridge National Laboratory (Oak Ridge) and their subcontractor Metatech released a study that explored the vulnerability of the electric grid to EMP-related events. This study was a joint effort contracted by FERC staff, the Department of Energy and the Department of Homeland Security and expanded on the information developed in other initiatives, including the EMP commission reports. The series of reports provided detailed technical background and outlined which sections of the power grid are most vulnerable, what equipment would be affected, and what damage could result. Protection concepts for each threat and additional methods for remediation were also included along with suggestions for mitigation. The results of the study support the general conclusion that EMP events pose substantial risk to equipment and operation of the Nation's power grid and under extreme conditions could result in major long term electrical outages. In fact, solar magnetic disturbances are inevitable with only the timing and magnitude subject to variability. The study assessed the 1921 solar storm, which has been termed a 1-in-100 year event, and applied it to today's power grid. The study concluded that such a storm could damage or destroy up to 300 bulk power system transformers interrupting service to 130 million people for a period of years.

On April 30, 2012, the Commission held a technical conference to discuss issues related to reliability of the bulk power system as affected by geomagnetic disturbances. The conference explored the risks and impacts from geomagnetically induced currents to transformers and other equipment on the bulk power system, as well as options for addressing or mitigating the risks and impacts. The Commission is considering the comments filed after that conference.

The existing reliability standards do not address EMP vulnerabilities. Protecting the electric generation, transmission and distribution systems from severe damage due to an EMP-related event would involve vulnerability assessments at every level of electric infrastructure.

THE NEED FOR LEGISLATION

In my view, section 215 of the Federal Power Act provides an adequate statutory foundation for the ERO to develop most reliability standards for the bulk power system. However, the nature of a national security threat by entities intent on attacking the U.S. through vulnerabilities in its electric grid stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and protective relay maintenance practices. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as endanger the health and safety of millions of citizens. Given the national security dimension to this threat, there may be a need to act quickly to protect the grid, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure.

The Commission's current legal authority is inadequate for such action. This is true of both cyber and physical threats to the bulk power system that pose national security concerns. Section 215 of the FPA excludes all facilities in Alaska and Hawaii and all local distribution facilities from the Commission's reliability jurisdiction, which may leave significant facilities vulnerable to the threat of a cyber or physical attack. In addition, although the NERC standards development process as envisioned in section 215 can be fine for routine reliability matters, it is too slow, too open and too unpredictable to ensure its responsiveness in the cases where national security is endangered. This process is inadequate when measures or actions

[3] Odenwald, Sten F. and Green, James L., Bracing the Satellite Infrastructure for a Solar Superstorm, Scientific American Magazine (Jul. 28, 2008).

need to be taken to address threats to national security quickly, effectively and in a manner that protects against the disclosure of security-sensitive information.

These shortcomings can be solved through a comprehensive, government-wide approach to cyber security issues or through a sector-specific approach. If a government-wide course is pursued, care should be taken to ensure that the two approaches complement each other, preserving FERC's ability to regulate electric reliability effectively. Any new legislation should address several key concerns. First, to prevent a significant risk of disruption to the grid, legislation should allow the federal government to take action before a cyber or physical national security incident has occurred. In particular, the federal government should be able to require mitigation even before or while NERC and its stakeholders develop a standard, when circumstances require urgent action. Second, any legislation should ensure appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Without such confidentiality, the grid may be more vulnerable to attack. Third, if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would not authorize Federal action to mitigate cyber or other national security threats to reliability that involve certain critical facilities and major population areas. Fourth, it is important that entities be able to recover costs they incur to mitigate vulnerabilities and threats.

CONCLUSION

The Commission's current authority is not adequate to address cyber or other national security threats to the reliability of our transmission and power system. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our government and economy and helps ensure the health and welfare of our citizens. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

The CHAIRMAN. Thank you very much.

Mr. Wilshusen, go right ahead.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION AND TECHNOLOGY, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Mr. Chairman, Ranking Member Murkowski, members of the committee. Thank you for the opportunity to testify at today's hearing on actions to secure the electricity grid.

As you know, the electric power industry, which is composed of electricity generation, transmission, distribution, and system operations, is increasingly incorporating information technology systems and networks into its existing infrastructure, as it modernizes the electricity grid.

The use of IT can provide many benefits, such as greater efficiency and reliability, and lower costs to consumers. However, this increased reliance on computer systems and networks also introduces cyber-based risk to the grid if the systems and networks are not properly protected.

For nearly a decade, GAO has identified the protection of systems supporting our Nation's critical infrastructure, which includes the electricity grid, as a Government-wide, high risk area.

Today, I will discuss the cyber threats to the electricity grid and several of the actions taken and challenges remaining to secure the grid. But, first, if I may, Mr. Chairman, I would like to recognize several members of my team who were instrumental in developing this statement and also conducting the work on which it is based.

With me today is Anjalique Lawrence, seated behind me. Back at the office: Mike Gilmore, Lee McCracken, David Trimble, Jon Ludwigson, and Paige Gilbreath, all played significant roles and made significant contributions.

Mr. Chairman, the threats to systems supporting the electricity grid are evolving and growing. They include both unintentional and intentional threats, and may come in the form of equipment failures, as well as targeted and untargeted attacks from our adversaries.

The interconnectivity between industrial control systems, computer networks, and the Internet can amplify the impact of these threats and expose the grid to known and unknown cybersecurity vulnerabilities, potentially affecting the operations of critical infrastructures, the security of sensitive information, and the flow of commerce. Several reported incidents illustrate the potentially serious impact of these threats.

To address such concerns, State and Federal authorities play key roles in overseeing grid reliability, which involves the security of the grid. State regulators generally oversee the reliability of local distribution system; whereas, NERC has developed and enforced mandatory standards intended to ensure the reliability of the bulk power system, which includes certain generation facilities and the high voltage electricity transmission network.

FERC has approved and, thus, made mandatory, 8 critical infrastructure standards developed by NERC to help ensure the secure electronic exchange of information and to prevent unauthorized physical and logical access to critical cyber assets.

In addition, NIST has identified guidelines on how to securely implement smart grid systems and identified an initial set of interoperability and cybersecurity standards for the smart grid. However, FERC has not yet adopted these standards, citing a lack of consensus for them.

GAO has previously reported on a number of key challenges to securing the modernized electricity grid; for example, aspects of current regulatory environment may complicate matters. Specifically, jurisdictional issues and the difficulties associated with responding to continually evolving cyber threats were a key regulatory challenge to ensuring the cybersecurity of the grid.

We also reported other challenges affecting industry efforts to secure the smart grid. Specifically, the electricity industry had not consistently built security features for certain smart grid devices, established an effective mechanism for sharing cybersecurity information, and created a set of metrics for evaluating the effectiveness of cybersecurity controls.

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

In summary, Mr. Chairman, the evolving and growing threat from cyber-based attacks highlights the importance of securing the electricity industry's systems and networks. A successful attack could result in wide-spread power outages, significant monetary losses, and extensive property damage.

More needs to be done to meet the challenges facing the industry and enhancing security. In particular, Federal regulators and other stakeholders will need to work closely together with the private sector, to address cybersecurity challenges, as the generation, transmission, and distribution of electricity come to rely more on emerging and sophisticated technologies.

Mr. Chairman, Ranking Member, this completes my statement. I would be happy to answer any questions.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION AND TECHNOLOGY, GOVERNMENT ACCOUNTABILITY OFFICE

WHY GAO DID THIS STUDY

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). This use of IT can provide many benefits, such as greater efficiency and lower costs to consumers. However, this increased reliance on IT systems and networks also exposes the grid to cybersecurity vulnerabilities, which can be exploited by attackers. Moreover, GAO has identified protecting systems supporting our nation's critical infrastructure (which includes the electricity grid) as a governmentwide high-risk area.

GAO was asked to testify on the status of actions to protect the electricity grid from cyber attacks. Accordingly, this statement discusses (1) cyber threats facing cyber-reliant critical infrastructures, which include the electricity grid, and (2) actions taken and challenges remaining to secure the grid against cyber attacks. In preparing this statement, GAO relied on previously published work in this area and reviewed reports from other federal agencies, media reports, and other publicly available sources.

WHAT GAO RECOMMENDS

In a prior report, GAO has made recommendations related to electricity grid modernization efforts, including developing an approach to monitor compliance with voluntary standards. These recommendations have not yet been implemented.

WHAT GAO FOUND

The threats to systems supporting critical infrastructures are evolving and growing. In testimony, the Director of National Intelligence noted a dramatic increase in cyber activity targeting U.S. computers and systems, including a more than tripling of the volume of malicious software. 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, 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 electricity grid's reliance on IT systems and networks exposes it to potential and known cybersecurity vulnerabilities, which could be exploited by attackers. The potential impact of such attacks has been illustrated by a number of recently reported incidents and can include fraudulent activities, damage to electricity control systems, power outages, and failures in safety equipment.

To address such concerns, multiple entities have taken steps to help secure the electricity grid, including the North American Electric Reliability Corporation, the National Institute of Standards and Technology (NIST), the Federal Energy Regulatory Commission, and the Departments of Homeland Security and Energy. These include, in particular, establishing mandatory and voluntary cybersecurity standards and guidance for use by entities in the electricity industry. For example, the North American Electric Reliability Corporation and the Federal Energy Regulatory Commission, which have responsibility for regulation and oversight of part of the industry, have developed and approved mandatory cybersecurity standards and additional guidance. In addition, NIST has identified cybersecurity standards that support smart grid interoperability and has issued a cybersecurity guideline. The Departments of Homeland Security and Energy have also played roles in disseminating guidance on security practices and providing other assistance.

As GAO previously reported, there were a number of ongoing challenges to securing electricity systems and networks. These include:

- A lack of a coordinated approach to monitor industry compliance with voluntary standards.
- Aspects of the current regulatory environment made it difficult to ensure the cybersecurity of smart grid systems.

- A focus by utilities on regulatory compliance instead of comprehensive security.
- A lack of security features consistently built into smart grid systems.
- The electricity industry did not have an effective mechanism for sharing information on cybersecurity and other issues.
- The electricity industry did not have metrics for evaluating cybersecurity.

Chairman Bingaman, Ranking Member Murkowski, and Members of the Committee:

Thank you for the opportunity to testify at today's hearing on the status of actions to protect the electricity grid from cyber attacks.

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). This use of IT can provide many benefits, such as greater efficiency and lower costs to consumers. Along with these anticipated benefits, however, cybersecurity and industry experts have expressed concern that, if not implemented securely, modernized electricity grid systems will be vulnerable to attacks that could result in widespread loss of electrical services essential to maintaining our national economy and security.

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

In my testimony today, I will describe (1) cyber threats facing cyber-reliant critical infrastructures,[2] which include the electricity grid, and (2) actions taken and challenges remaining to secure the grid against cyber attacks. In preparing this statement in July 2012, we relied on our previous work in this area, including studies examining efforts to secure the electricity grid and associated challenges and cybersecurity guidance.[3] (Please see the related GAO products in appendix I.) The products upon which this statement is based contain detailed overviews of the scope of our reviews and the methodology we used. We also reviewed documents from the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, the Department of Energy, including its Office of the Inspector General, and the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, as well as publicly available reports on cyber incidents. 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.

Utilities own and operate electricity assets, which may include generation plants, transmission lines, distribution lines, and substations—structures often seen in resi-

---

[1] GAO's biennial high-risk list identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a government-wide high-risk area since 1997; 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. These include, for example, banking and finance, communications, public health, and energy. The energy sector includes subsectors for oil and gas and for electricity.

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

dential 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.

MODERNIZATION OF THE ELECTRICITY INFRASTRUCTURE

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

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

The use of smart grid systems may have a number of benefits, including improved reliability 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 developing and enforcing mandatory standards to ensure the reliability of the bulk power system—i.e., facilities and control systems necessary for operating the transmission network and certain generation facilities needed for reliability. NERC develops reliability standards collaboratively through a deliberative process involving utilities and others in the industry, which are then sent to FERC for approval. These standards include critical infrastructure protection standards for protecting

[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).

electric utility-critical and cyber-critical assets. FERC has responsibility for reviewing and approving the reliability standards or directing NERC to modify them.

In addition, the Energy Independence and Security Act of 2007[6] established federal policy to support 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 the Department of Energy. With regard to cybersecurity, the act required NIST and FERC to take the following actions:

- NISTwas 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. However, according to FERC officials, the statute did not provide specific additional authority to allow FERC to require utilities or manufacturers of smart grid technologies to follow these standards. As a result, any standards identified and developed through the NIST-led process are voluntary unless regulators use other authorities to indirectly compel utilities and manufacturers to follow them.

THE ELECTRICITY GRID IS POTENTIALLY VULNERABLE TO AN EVOLVING ARRAY OF CYBER-BASED 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.[9] 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. Table 1 shows common sources of cyber threats.

TABLE 1: SOURCES OF CYBERSECURITY THREATS

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).

[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] 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).

TABLE 1: SOURCES OF CYBERSECURITY THREATS—Continued

Threat source	Description
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.

TABLE 1: SOURCES OF CYBERSECURITY THREATS—Continued

Threat source	Description
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

These sources of cyber threats make use of various techniques, or exploits that may adversely affect computers, software, a network, an organization's operation, an industry, or the Internet itself. Table 2 shows common types of cyber exploits.

TABLE 2: TYPES OF 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 bombs	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.

TABLE 2: TYPES OF CYBER EXPLOITS—Continued

Type of exploit	Description
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or 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.
Structured Query Language (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 timeframe between public discoveries of both makes it difficult to defend against

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

ELECTRICITY GRID FACES CYBERSECURITY VULNERABILITIES

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. In addition, the increased reliance on IT systems and networks also exposes the electric grid to potential and known cybersecurity vulnerabilities. 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.

In May 2008, we reported that the corporate network of the Tennessee Valley Authority—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.[10] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing the Tennessee Valley Authority's critical infrastructures and 73 recommendations to address specific weaknesses in security controls. The Tennessee Valley Authority concurred with the recommendations and has taken steps to implement them.

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.[11] Further, in 2007, the Department of Homeland Security, in cooperation with the Department of Energy, ran a test that demonstrated that a vulnerability commonly referred to as "Aurora" had the potential to allow unauthorized users to remotely control, misuse, and cause damage to a small commercial electric generator. Moreover, in 2008, the Central Intelligence Agency reported that malicious activities against IT systems and networks have caused disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multicity power outage.[12] As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

REPORTED INCIDENTS ILLUSTRATE THE POTENTIAL IMPACT OF CYBER THREATS

Cyber incidents continue to affect the electricity industry. For example, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team recently noted that the number of reported cyber incidents affecting control systems of companies in the electricity sector increased from 3 in 2009 to 25 in 2011. In addition, we and others have reported[13] that cyber incidents can affect the operations of energy facilities, as the following examples illustrate:

- Smart meter attacks.—In April 2012, it was reported that sometime in 2009 an electric utility asked the FBI to help it investigate widespread incidents of power thefts through its smart meter deployment. The report indicated that the miscreants hacked into the smart meters to change the power consumption recording settings using software available on the Internet.
- Phishing attacks directed at energy sector.—The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team reported that, in 2011, it deployed incident response teams to an electric bulk provider and an electric utility that had been victims of broader phishing attacks. The team found three malware samples and detected evidence of a sophisticated threat actor.
- 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 con-

[10] GAO, Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks, GAO-08-526 (Washington, D.C.: May 21, 2008).
[11] GAO-07-1036.
[12] The White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, D.C.: May 29, 2009).
[13] GAO-07-1036 and GAO-12-92.

trol 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.

ACTIONS HAVE BEEN TAKEN TO SECURE THE ELECTRICITY GRID, BUT CHALLENGES REMAIN

Multiple entities have taken steps to help secure the electricity grid, including NERC, NIST, FERC, and the Departments of Homeland Security and Energy. NERC has performed several activities that are intended to secure the grid. It has developed eight critical infrastructure standards for protecting electric utility-critical and cyber-critical assets.

The standards established requirements for the following key cybersecurity-related controls: critical cyber asset identification, security management controls, personnel and training, electronic "security perimeters," physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets. In December 2011, we reported that NERC's eight cyber security standards, along with supplementary documents, were substantially similar to NIST guidance applicable to federal agencies.[14]

NERC also has published security guidelines for companies to consider for protecting electric infrastructure systems, although such guidelines are voluntary and typically not checked for compliance. For example, NERC's June 2010 Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets is intended to assist entities in identifying and developing a list of critical cyber assets as described in the mandatory standards. NERC also has enforced compliance with mandatory cybersecurity standards through its Compliance Monitoring and Enforcement Program, subject to FERC review. NERC has assessed monetary penalties for violations of its cyber security standards.

NIST, in implementing its responsibilities under the Energy Independence and Security Act of 2007 with regard to standards to achieve interoperability of smart grid systems, planned to identify cybersecurity standards for these systems. In January 2011, we reported[15] that it had identified 11 standards involving cybersecurity that support smart grid interoperability and had issued a first version of a cybersecurity guideline.[16] NIST's cybersecurity guidelines largely addressed key cybersecurity elements, such as assessment of cybersecurity risks and identification of security requirements (i.e., controls); however, its guidelines did not address an important element essential to securing smart grid systems—the risk of attacks using both cyber and physical means.[17] NIST officials said that they intended to update the guidelines to address this and other missing elements they identified, but their plan and schedule for doing so were still in draft form. We recommended that NIST finalize its plan and schedule for incorporating missing elements, and NIST officials agreed. We are currently working with officials to determine the status of their efforts to address these recommendations.

FERC also has taken several actions to help secure the electricity grid. For example, it reviewed and approved NERC's eight critical infrastructure protection standards in 2008. Since then, in its role of overseeing the development of reliability standards, the commission has directed NERC to make numerous changes to standards to improve cybersecurity protections. However, according to the FERC Chairman's February 2012 letter in response to our report on electricity grid modernization, many of the outstanding directives have not been incorporated into the latest versions of the standards. The Chairman added that the commission would continue to work with NERC to incorporate the directives. In addition, FERC has authorized NERC to enforce mandatory reliability standards for the bulk power system, while retaining its authority to enforce the same standards and assess penalties for viola-

[14] GAO-12-92.
[15] GAO-11-117.
[16] 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.
[17] GAO-11-117.

tions. We reported in January 2011 that FERC also had begun reviewing initial smart grid standards identified as part of NIST efforts. However, in July 2011, the commission declined to adopt the initial smart grid standards identified as a part of the NIST efforts, finding that there was insufficient consensus to do so.

The Department of Homeland Security has been designated by federal policy as the principal federal agency to lead, integrate, and coordinate the implementation of efforts to protect cyber-critical infrastructures and key resources. Under this role, the Department's National Cyber Security Division's Control Systems Security Program has issued recommended practices to reduce risks to industrial control systems within and across all critical infrastructure and key resources sectors, including the electricity subsector. For example, in April 2011, the program issued the Catalog of Control Systems Security: Recommendations for Standards Developers, which is intended to provide a detailed listing of recommended controls from several standards related to control systems.[18] The program also manages and operates the Industrial Control Systems Cyber Emergency Response Team to respond to and analyze control-systems-related incidents, provide onsite support for incident response and forensic analysis, provide situational awareness in the form of actionable intelligence, and share and coordinate vulnerability information and threat analysis through information products and alerts. For example, it reported providing on-site assistance to six companies in the electricity subsector, including a bulk electric power provider and multiple electric utilities, during 2009-2011.

The Department of Energy is the lead federal agency which is responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in the energy sector, including the electricity subsector. In this regard, we have reported that officials from the Department's Office of Electricity Delivery and Energy Reliability stated that the department was involved in efforts to assist the electricity sector in the development, assessment, and sharing of cybersecurity standards.[19] For example, the department was working with NIST to enable state power producers to use current cybersecurity guidance. In May 2012, the department released the Electricity Subsector Cybersecurity Risk Management Process.[20] The guideline is intended to ensure that cybersecurity risks for the electric grid are addressed at the organization, mission or business process, and information system levels. We have not evaluated this guide.

CHALLENGES TO SECURING ELECTRICITY SYSTEMS AND NETWORKS

In our January 2011 report, we identified a number of key challenges that industry and government stakeholders faced in ensuring the cybersecurity of the systems and networks that support our nation's electricity grid.[21] These included the following:

- There was a lack of a coordinated approach to monitor whether industry follows voluntary standards.—As mentioned above, under the Energy Independence and Security Act of 2007, 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, which had discussed the standards-setting process in general terms. Nevertheless, according to officials from FERC and the National Association of Regulatory Utility Commissioners, 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

[18] DHS, National Cyber Security Division, Control Systems Security Program, Catalog of Control Systems Security: Recommendations for Standards Developers (April 2011).
[19] GAO-12-92.
[20] U.S. Department of Energy, Electricity Subsector Cybersecurity Risk Management Process, DOE/OE-0003 (Washington, D.C.: May 2012).
[21] GAO-11-117.

and other regulators to know whether a voluntary approach to standards setting is effective or if changes are needed.[22]

- Aspects of the current regulatory environment made it difficult to ensure the cybersecurity of smart grid systems.—In particular, jurisdictional issues and the difficulties associated with responding to continually evolving cyber threats were a key regulatory challenge to ensuring the cybersecurity of smart grid systems as they are deployed. Regarding jurisdiction, experts we spoke with expressed concern that there was a lack of clarity about the division of responsibility between federal and state regulators, particularly regarding cybersecurity. While jurisdictional responsibility has historically been determined by whether a technology is located on the transmission or distribution system, experts raised concerns that smart grid technology may blur these lines. For example, devices such as smart meters deployed on parts of the grid traditionally subject to state jurisdiction could, in the aggregate, have an impact on those parts of the grid that federal regulators are responsible for—namely the reliability of the transmission system.

  There was also concern about the ability of regulatory bodies to respond to evolving cybersecurity threats. For example, one expert questioned the ability of government agencies to adapt to rapidly evolving threats, while another highlighted the need for regulations to be capable of responding to the evolving cybersecurity issues. In addition, our experts expressed concern with agencies developing regulations in the future that are overly specific in their requirements, such as those specifying the use of a particular product or technology. Consequently, unless steps are taken to mitigate these challenges, regulations may not be fully effective in protecting smart grid technology from cybersecurity threats.
- Utilities were focusing on regulatory compliance instead of comprehensive security.—The existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity. Specifically, experts told us that utilities focus on achieving minimum regulatory requirements rather than designing a comprehensive approach to system security. In addition, one expert stated that security requirements are inherently incomplete, and having a culture that views the security problem as being solved once those requirements are met will leave an organization vulnerable to cyber attack. Consequently, without a comprehensive approach to security, utilities leave themselves open to unnecessary risk.
- There was a lack of security features built into smart grid systems. Security features are not consistently built into smart grid devices.—For example, experts told us that certain currently available smart meters had not been designed with a strong security architecture and lacked important security features, including event logging[23] and forensics capabilities that are needed to detect and analyze attacks. In addition, our 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 lack the capability to detect and analyze attacks, increasing the risk that attacks will succeed and utilities will be unable to prevent them from recurring.
- The electricity industry did not have an effective mechanism for sharing information on cybersecurity and other issues.—The electricity industry lacked an effective mechanism to disclose information about cybersecurity vulnerabilities, incidents, threats, lessons learned, and best practices in the industry. For example, our experts stated that while the electricity industry has an information sharing center, it did not fully address these information needs. In addition, President Obama's May 2009 cyberspace policy review also identified challenges

[22] 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.

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

related to cybersecurity information sharing within the electric and other critical infrastructure sectors and issued recommendations to address them.[24] According to our experts, information regarding incidents such as both unsuccessful and successful attacks must be able to be shared in a safe and secure way 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 cyber attacks and their methods, which could help grid operators better defend against them. If the industry pursued this end, it could draw upon the practices and approaches of other industries when designing an industry-led approach to cybersecurity information sharing. Without quality processes for information sharing, utilities will not have the information needed to adequately protect their assets against attackers.

- The electricity industry did not have 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[25] are difficult to develop, they could help compare the effectiveness of competing solutions and determine what mix of solutions combine to make the most secure system. Furthermore, our experts said 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, there is increased risk that utilities will not invest in security in a cost-effective manner, or have the information needed to make informed decisions on their cybersecurity investments.

To address these challenges, we made recommendations in our January 2011 report. To improve coordination among regulators and help Congress better assess the effectiveness of the voluntary smart grid standards process, we recommended that the Chairman of FERC develop an approach to coordinate with state regulators and with groups that represent utilities subject to less FERC and state regulation to (1) periodically evaluate the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards and (2) develop strategies for addressing any gaps in compliance with standards that are identified as a result of this evaluation. We also 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 these recommendations.

Although FERC agreed with these recommendations, they have not yet been implemented. According to the FERC Chairman, given the continuing evolution of standards and the lack of sufficient consensus for regulatory adoption, commission staff believe that coordinated monitoring of compliance with standards would be premature at this time, and that this may change as new standards are developed and deployed in industry. We believe that it is still important for FERC to improve coordination among regulators and that consensus is reached on standards. We will continue to monitor the status of its efforts to address these recommendations.

In summary, the evolving and growing threat from cyber-based attacks highlights the importance of securing the electricity industry's systems and networks. A successful attack could result in widespread power outages, significant monetary costs, damage to property, and loss of life. The roles of NERC and FERC remain critical in approving and disseminating cybersecurity guidance and enforcing standards, as appropriate. Moreover, more needs to be done to meet challenges facing the industry in enhancing security, particularly as the generation, transmission, and distribution of electricity comes to rely more on emerging and sophisticated technology.

Chairman Bingaman, Ranking Member Murkowski, and Members of the Committee, this concludes my statement. I would be happy to answer any questions you may have at this time.

APPENDIX I: RELATED GAO PRODUCTS

Cybersecurity: Threats Impacting the Nation. GAO-12-666T. Washington, D.C.: April 24, 2012.

Cybersecurity: Challenges in Securing the Modernized Electricity Grid, GAO-12-507T. Washington, D.C.: February 28, 2012.

---

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

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

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. GAO-12-92. Washington, D.C.: December 9, 2011.
High-Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.
Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed. GAO-11-117. Washington, D.C.: January 12, 2011.
Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. GAO-11-865T. Washington, D.C.: July 26, 2011.
Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. GAO-10-628. Washington, D.C.: July 15, 2010.
Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606. Washington, D.C.: July 2, 2010.
Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats. GAO-10-834T. Washington, D.C.: June 16, 2010.
Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO-10-296. Washington, D.C.: March 5, 2010.
Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. GAO-10-338. Washington, D.C.: March 5, 2010.
Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats. GAO-10-230T. Washington, D.C.: November 17, 2009.
Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets. GAO-10-147. Washington, D.C.: October 23, 2009.
Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment. GAO-09-969. Washington, D.C.: September 24, 2009.
National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.
Electricity Restructuring: FERC Could Take Additional Steps to Analyze Regional Transmission Organizations' Benefits and Performance. GAO-08-987. Washington, D.C.: September 22, 2008.
Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.
Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.
Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. GAO-07-705. Washington, D.C.: June 22, 2007.
Meeting Energy Demand in the 21st Century: Many Challenges and Key Questions. GAO-05-414T. Washington, D.C.: March 16, 2005.

The CHAIRMAN. Thank you very much.
Mr. Cauley.

STATEMENT OF GERRY CAULEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. CAULEY. Thank you, and good morning, Chairman Bingaman, and Ranking Member Murkowski, and members of the committee, and fellow panelists. My name is Gerry Cauley. I am the President and CEO of the North American Electric Reliability Corporation.

When we go about our business for reliability and security of the power grid, we think, first, of the customers and rate payers and citizens that we serve. When I do that, we think about 4 principles. First of all, focus on really big important reliability problems find solutions, and fix them.

Second, we apply principles of using risk-based approaches to make sure that we are prioritizing effectively and that we are coming up with cost-effective solutions.

Third, we focus on the learning industry. So, we are continually adapting and developing reliability solutions and learning from experience.

Finally, we hold the industry accountable, as well as ourselves, to produce reliability results.

This approach works really well in conventional risks, such as storm outages, equipment failures, human factors, errors, and those kinds of things. I think the approach also works well in the arena of cyber and physical security.

One of the big differences, however, in security is we are often challenged by the lack of information, and this is where, in cyber, the partnership between industry and Government, in terms of information sharing, to help us understand those risks and be able to adapt to them, is very important.

So, our strategy for security recognizes that a perfect defense against the bad guys is not achievable nor necessarily affordable. So what we have to do is combine defense strategies, such as through our standards, as well as resilience, and adapting and enhancing the existing resilience of the bulk power system.

So, our strategy includes several activities. The first is in the—having a base set of standards that ensure the protection of the grid. We promote and are involved in active information sharing between industry and Government, and among industry, and among critical infrastructure sectors. We are focused on training and exercising and testing our ability to perform well under security challenges. We are continually assessing the reliability and security of the system, looking at emerging issues and emerging threats. We are working with Government agencies to develop solutions for security and also addressing cross-sector dependencies.

I did previously testify in front of the committee in May 2011, and I would just like to briefly review some of the changes and some of the activities that we have completed since that time.

First, in the area of standards—and I appreciate the Chairman pointing out that the electric power industry and the nuclear power industries are the only two critical infrastructures that do have mandatory standards and enforceable standards that are in place and that are working.

It was mentioned that we—the Commission just recently approved version 4, which includes a bright-line criteria, in terms of which facilities are required to be included within those standards. We are currently working on what I believe will be a plateau of security for us in version 5, where we are adopting NIST's risk controls into our standards, and we will have those completed and filed with the Commission by the end of the first quarter in 2013.

In addition to the standards, we also have a very rigorous program on compliance. Since 2008, we have conducted over 500 audits of individual companies, sending teams onsite, finding various findings and recommendations and things that need to be corrected. We also have the industry under a very aggressive program to monitor the remediation of those issues.

A third area is in the area of information sharing and analysis. This is our way of addressing near-term issues and risks that emerge continuously. There is a parallel that—if you look at—Microsoft essentially publishes on the second Tuesday of each

month for patches and vulnerabilities that have been identified over the previous month. That is essentially an approach that we need to take in terms of emerging risks and threats that come in that might be—need to be addressed on a matter of hours or days.

We use our information sharing process, issue alerts. We were able to get an agreement signed with Homeland Security to gain us access to the National Cybersecurity and Communications Integration Center, the NCCIC, and we have a secure portal up and running that allows the sharing of information. We have got over 500 companies that are actively engaging, in terms of posting and using that information. Our alerts that we're able to issue go to all 1,900 companies that are affected by the bulk power system.

Another area where we work actively is in the area of partnering with Federal partners. We have developed best practices guidelines, based on NIS practices with Department of Energy. We also worked on the White House Initiative to develop a risk management maturity model, and we recently issued 4 reports on resilience, severe cyber attack, and GMD.

So, in conclusion, I think our framework of standards, information sharing, and partnering with Government is the approach that will be most successful in cybersecurity.

Thank you.

[The prepared statement of Mr. Cauley follows:]

PREPARED STATEMENT OF GERRY CAULEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

INTRODUCTION

Good morning Chairman Bingaman, Ranking Member Murkowski, members of the Committee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). NERC was designated the Electric Reliability Organization (ERO) by the Federal Energy Regulatory Commission (FERC) in accordance with Section 215 of the Federal Power Act (FPA), enacted by the Energy Policy Act of 2005. NERC's reliability standards are mandatory and enforceable within the US for the bulk power system and include Critical Infrastructure Protection (CIP) Standards. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States. NERC's mission is to ensure the reliability of the bulk power system of North America and promote reliability excellence with accountability for standards and compliance, risks to reliability and continued coordination and collaboration with public and private sector partners. I testified on this subject before this Committee in May 2011, and I appreciate the opportunity to update the Committee on NERC's activities related to cybersecurity. These activities include, but are not limited to:

1. Receiving FERC approval of NERC's Critical Cyber Asset Identification standards (CIP-002 version 4);
2. Beginning work on a comprehensive revision to the cybersecurity standards, leveraging lessons learned from previous versions;
3. Issuing eight additional alerts related to cybersecurity concerns;
4. Developing a risk management process guideline to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks;
5. Completing the first phase of the High-Impact Low-Frequency Task Force reports identifying recommendations for owners and operators with respect to addressing severe impact resilience, cyber attacks, spare equipment, and geomagnetic disruptions;
6. Facilitating the first-ever Grid Security Exercise (GridEx) for the Electricity Sub-sector in North America; and
7. Participating in government partnership initiatives, including the Department of Homeland Security's (DHS) National Level Exercise series and various

cybersecurity forums and briefings with Canadian government agencies, as well as the White House-initiated, Department of Energy (DOE)-led Electricity Subsector Cybersecurity Risk Management Maturity Model, which will support ongoing development and measurement of cybersecurity capabilities within the sub-sector;

THE CYBERSECURITY CHALLENGE FOR THE GRID

As a result of society's growing dependence on electricity, the electric grid is one of the Nation's most critical infrastructures. The bulk power system in North America is one of the largest, most complex, and most robust systems ever created. As CEO of the organization charged with ensuring the reliability and security of the North American grid, I remain deeply concerned about the changing risk landscape from conventional risks, such as extreme weather and equipment failures, to new and emerging risks where we are left to imagine scenarios that might occur and prepare to avoid or mitigate the consequences. Some of those consequences could be much more severe than we have previously experienced. I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures. These threats differ from conventional risks in that they result from intentional actions by adversaries and are not simply random failures or acts of nature.

To explore the impacts of this changing risk landscape from the view of the newer emerging risks, NERC has worked with industry and government to better understand cybersecurity risks and manage those risks. Based on all of the work NERC has been involved in to date, it is clear that the most effective approach against adversaries exploiting the newer risk landscape is through thoughtful application of resiliency principles. Resiliency requires proactive readiness for whatever may come our way and includes robustness; the ability to minimize consequences in real-time; the ability to restore essential services; and the ability to adapt and learn.

NERC MEASURES TO ADDRESS CYBERSECURITY THREATS AND VULNERABILITIES

NERC has incorporated these resiliency elements in our strategic approach to ensuring reliability of the bulk power system. This strategic approach includes: 1) developing mandatory and enforceable standards; 2) ensuring compliance and audit oversight; 3) sharing and analyzing information and issuing Alerts from the Electricity Sector Information Sharing and Analysis Center (ES-ISAC); 4) engaging in private-public partnerships; and 5) conducting outreach, training, and education activities within and external to the bulk power system. Only through these critical infrastructure protection components can we achieve a balanced approach to guard against advanced persistent threats to grid cybersecurity and mitigate vulnerabilities.

RELIABILITY STANDARDS

In 2007, FERC designated NERC the ERO in accordance with Section 215 of the Federal Power Act, enacted by the Energy Policy Act of 2005. Upon FERC's approval, NERC's reliability standards became mandatory within the US. These mandatory reliability standards include CIP Standards 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the US. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, developed with substantial input from industry and approved by FERC, to accomplish our mission to ensure the reliability of the electric grid.

NERC's nine mandatory CIP standards address the following areas:

- Standard CIP-001: Covers Sabotage Reporting.
- Standard CIP-002: Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.
- Standard CIP-003: Requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
- Standard CIP-004: Requires that personnel with access having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

- Standard CIP-005: Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
- Standard CIP-006: Addresses implementation of a physical security program for the protection of Critical Cyber Assets.
- Standard CIP-007: Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
- Standard CIP-008: Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.
- Standard CIP-009: Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

In December 2010, NERC approved an enhancement to its Critical Cyber Asset Identification standard (CIP-002 version 4) that establishes bright-line criteria for the identification of critical assets. This enhanced standard was filed with the Federal Energy Regulatory Commission (FERC) in February 2011, and FERC approved the standard on April 19, 2012. The implementation of the CIP standards under the bright-line approach is currently underway.

In addition, industry is currently developing a comprehensive revision to the cybersecurity Standards. The revision leverages experience with existing CIP standards to enhance the industry's protections against cyber threats and vulnerabilities, including transitioning the classification of critical assets to a "low-medium-high" impact-based system. The revised CIP standards will also provide greater flexibility in implementing solutions to emerging cyber threats. The revised CIP standards have been improved to remove technology-specific requirements by replacing them with a risk-based approach to implementing appropriate and changing technologies. That is, rather than specifying how to implement a requirement, the revised requirements specify the risk-based result that must be achieved, which enables industry to implement new and emerging technologies to address the risk.

NERC can use an emergency standards development process if circumstances warrant. In addition, FERC can order NERC to develop or modify a reliability standard to address a specific matter.[1] Finally, the NERC Board of Trustees can direct NERC to develop and adopt a standard in response to a FERC directive and timetable if the Board determines that the regular standards process is not sufficiently responsive to the Commission.

Under the emergency standards process, FERC has authorized NERC to use an expedited standards development process to meet urgent reliability issues. These special standards can be developed on an expedited, confidential basis to address imminent or longer-term national security threats. NERC has practiced using this expedited, confidential process as part of GridEx.

In addition to developing mandatory reliability standards, NERC supports the ERO's Regional Entities to improve the consistency of compliance program results, improve risk-based approaches for auditing and spot checking, and promote a culture of security and compliance through education, transparency, and incentives. Specifically, we conduct audit oversight of the Regional Entities' compliance audit teams during audits of registered entities, and maintain oversight throughout the entire audit process (pre-audit, on-site, and post audit) in accordance with the audit oversight program. During this process, NERC seeks to capture compliance applications, positive observations, lessons learned, and recommendations. NERC's audit oversights are designed to perform a thorough evaluation of the processes and criteria used by all Regional Entities in their determination of registered entities' compliance with the NERC Reliability Standards, including the CIP Standards.

Compliance with the NERC CIP standards is an important threshold for properly securing the bulk electric system. However, no single security asset, technique, procedure, or standard—even if strictly followed—will protect an entity from all potential cyber threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best-practices call for additional processes, procedures, and technologies beyond those required by the CIP standards.

---

[1] FERC can order NERC to develop a proposed reliability standard or a modification to a reliability standard to address a specific matter (such as a cyber threat or vulnerability) under FPA Section 215(d) (5).

THE ES-ISAC AND NERC ALERTS

Not all vulnerabilities can or should be addressed through a reliability standard. In such cases, NERC Alerts are a key element in critical infrastructure protection. To address cyber challenges not covered under the CIP Standards, NERC works through its ES-ISAC to inform the industry and recommend mitigation actions.

The ES-ISAC gathers information from disparate electric industry participants about security-related events, disturbances, and off-normal occurrences within the Electricity Sub-sector and shares that information with key governmental entities. In turn, these governmental entities provide the ES-ISAC with information regarding risks, threats, and warnings which the ES-ISAC is then responsible for disseminating throughout the Electricity Sub-sector. The two functions that the ES-ISAC supports, information sharing and analytics, are vitally important to all other critical infrastructures and key resource sectors that have active ISACs. Effective collaboration and communication is essential to addressing infrastructure protection and resilience within each sector, as well as the important interdependencies that exist among sectors.

NERC staff with appropriate security clearances often work with cleared personnel from Federal agencies to communicate unclassified sensitive information to the industry. As defined in NERC's Rules of Procedure, the ES-ISAC developed the following three levels of Alerts for formal notice to industry regarding security issues:

- Industry Advisory.—Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- Recommendation to Industry.—Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the Alert.
- Essential Action.—Identifies actions deemed to be "essential" to bulk power system reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the Alert.

The risk to the bulk power system determines selection of the appropriate Alert notification level. Generally, NERC distributes Alerts broadly to users, owners, and operators of the bulk power system in North America utilizing its Compliance Registry. Entities registered with NERC are required to provide and maintain up-to-date compliance and cyber security contacts. NERC also distributes the Alerts beyond the users, owners and operators of the bulk power system, to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., Balancing Authorities, Transmission Operators, Generation Owners, etc.).

Alerts are developed with the strong partnership of Federal technical organizations, including DHS and DOE National Laboratories, and bulk power system subject matter experts, called the HYDRA team. NERC has issued 22 CIP-related Alerts since January 2010 (20 Industry Advisories and two Recommendations to Industry). Those Alerts covered items such as Aurora, Stuxnet, Night Dragon, and the reporting of suspicious activity. Responses to Alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders. In addition, NERC released one Joint Product CIP Awareness Bulletin in collaboration with DOE, DHS and the Federal Bureau of Investigation (FBI) titled, "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPN)."

The NERC Alert system is working well. It is known by industry, handles confidential information, and does so in an expedited manner. The information needed to develop the Alert is managed in a confidential and expedited manner and does not require a NERC balloting process. Information sharing through the ES-ISAC is the greatest asset we have to combat emerging threats to cybersecurity and help ensure the reliability of the bulk power system. As a result, NERC has been enhancing the ES-ISAC's capabilities by building out a private, secure portal to receive voluntary reports from industry members and working with various organizations (both industry and government) to obtain the data and mechanisms necessary to conduct these information sharing activities.

Anything Congress can do to further facilitate information sharing between the public and private sector would add greatly to these efforts. Some actions may include: making more clearances available to industry, identifying alternative methods to communicate classified information to our Canadian partners, and encouraging increased information sharing by US Government departments and agencies with asset-owners.

NERC'S PUBLIC-PRIVATE PARTNERSHIPS TO ENHANCE GRID CYBERSECURITY

As mentioned, NERC has developed several strong relationships with industry and government entities. As chair of the Electricity Sub-sector Coordinating Council (ESCC), I work with industry CEOs and our partners within the government, including the Department of Defense, DOE, and DHS, to identify, discuss, and resolve critical infrastructure protection policy, process, and resource issues. This type of public-private partnership is essential to effective cybersecurity protection by facilitating information sharing about cyber-related vulnerabilities and threats.

Last year, NERC signed a Cooperative Research and Development Agreement with DHS that provides ES-ISAC staff with access to DHS' National Cybersecurity and Communications Integration Center (NCCIC). Access to the classified NCCIC facilitates a significantly improved bi-directional sharing of critical infrastructure protection information between the US government and the Electricity Sub-sector in North America. NERC has also recently established a protected communications corridor for the ES-ISAC in part to facilitate this bi-directional information sharing between the DHS NCCIC and BPS entities.

NERC also provides leadership to three significant DHS-affiliated public-private partnerships. These groups are:

- Partnership for Critical Infrastructure Security, the senior-most policy coordination group between public and private sector organizations comprised of the chairs or co-chairs of all 18 critical infrastructure and key resources sectors and their Government Coordinating Council counterparts;
- Cross-Sector Cyber Security Working Group, which was established to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services; and
- Industrial Control Systems Joint Working Group, which is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, and coordinated efforts to develop better vendor focus on security needs for industrial control systems.

NERC also collaborates with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability, and security incident information.

As part of NERC's outreach and awareness efforts to engage industry and government in addressing some of the key cybersecurity challenges we face, NERC facilitated the first-ever Grid Security Exercise (GridEx) for the Electricity Sub-sector in North America. This distributed play exercise, which was held in November 2011, was designed to validate the readiness of the Electricity Sub-sector to respond to a cyber incident, strengthen utilities' crisis response functions, and provide input for internal security program improvements. Seventy-five industry and government organizations from the US and Canada participated in GridEx. BPS entities included generation and transmission owners, reliability coordinators, independent system operators, and balancing authorities. Key government agencies, such as DHS, FBI, and DOE, were also heavily involved. GridEx provided a realistic environment for organizations to assess their cyber response capabilities. The biennial exercise was viewed across industry and government as a training success in preparing the BPS for a disruptive security event. NERC issued a final report in March 2012, and is applying the GridEx recommendations to further strengthen the bulk power system's preparedness and response mechanisms.

Given the heightened awareness of security in the Electricity Sub-sector, NERC hosts an annual Grid Security Conference (GridSecCon) to discuss emerging threats, industry best practices, and provide cutting edge training to the industry. NERC will again host this conference in October 2012, and will bring together cyber and physical security thought leaders from government and industry to discuss securing industrial control systems, social engineering attacks, and security event response management, among other topics.

CONCLUSION

As outlined today, NERC has many tools available, including critical infrastructure protection standards and processes and the ES-ISAC, to address imminent and non-imminent threats and vulnerabilities. We work with multiple government, industry, and consumer partners to support a coordinated comprehensive effort to address cybersecurity.

We appreciate this opportunity to discuss NERC's activities on cybersecurity with the committee related to cybersecurity protection of the grid.

The CHAIRMAN. Thank you very much.

Mr. Snitchler, go right ahead.

STATEMENT OF TODD A. SNITCHLER, CHAIRMAN, PUBLIC UTILITIES COMMISSION OF OHIO

Mr. SNITCHLER. Good morning. Chairman Bingaman, Ranking Member Murkowski, and members of the committee, I want to thank you for the opportunity to appear before you today as we examine the status of actions taken to ensure that the electric grid is protected from cyber attacks. My name is Todd Snitchler, and I am the Chairman of the Public Utilities Commission of Ohio.

Our State agency is responsible for assuring residential and business customers access to adequate, safe, and reliable utility service at fair prices, ensuring the financial integrity and service reliability of the Ohio utility industry and, among other things, promoting utility infrastructure investments, including investments in IT infrastructure. I am pleased to have the opportunity to discuss cybersecurity issues for the electric grid; because, often times, we take that grid for granted.

Should Congress decide to pass legislation on cybersecurity, however, it is my view that we must distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be addressed and resolved more deliberately. Particularly, regarding the electricity grid, one-size solutions for cybersecurity may not be the most effective means to mitigate and reduce known vulnerabilities.

Additionally, the desired outcome from such legislation should be the establishment of a foundation that contemplates 4 basic considerations. First, we need to protect diamonds like diamonds and apples like apples. That is, we must prioritize accordingly to ensure that the appropriate level of security is provided to all areas that require protection.

Second, States and the owners of critical infrastructure that we regulate cannot protect the infrastructure to the maximum extent possible, unless the relevant Federal agencies provide the actionable information necessary to identify and address the threat or vulnerability. In other words, true information sharing between those who have the information and those who need the information to protect their systems.

Third, our utilities can provide a gold-plated, or even a platinum-plated, system which is ultra-cyber secure. However, this raises the question of just how much do we want a kilowatt hour of electricity to cost.

Fourth, preparedness should not focus solely on response capabilities, but should also ensure that resilience is built into the infrastructure. Our Nation's utilities—municipal-, cooperative-, and investor-owned—have done this country proud in responding to the greatest calamities and catastrophes, quickly, and capably restoring power after significant storms, earthquakes, wildfires, or even acts of terrorism.

As a State regulator, my fellow commissioners and I, as well as our staff, have many responsibilities. Some items of significance today are resolved and become less significant down the road, and other items that are less significant today may become a issue of paramount importance in the near future, with a major change, for instance, in weather or technology. This is true for many things,

including the provision of electricity in a safe, reliable, and economic fashion.

Just as utilities cannot protect against all threats, neither can they eradicate all susceptibilities. We must recognize there are different parts of these systems that require different levels of protection. This is why we must ensure there is adequate protection of the grid, especially its most valuable parts, while we must not expend undue levels of resources protecting other less important parts of the system.

Another point of consideration that must be recognized is that State agencies, like the PUCO, along with owners of that critical infrastructure, are unable to provide the full measure of protection necessary to help secure the critical infrastructure if the relevant agencies are not providing that actionable information to address imminent threats.

State regulators take the reliability and security of the bulk power system very seriously. Through strong, Federal, State, public, and private partnerships, we have consistently maintained and improved reliability and security of the grid.

Cybersecurity is an emerging area of risk for our utilities and for State commissions as well. Although, it is unique in some respects, this is not the first time that our State utility systems have faced reliability threats. Through a strong, public-private partnership, we have overcome past risks. It is my belief that this emerging of information systems into the electric and other utility sectors will improve the resilience, reliability, and efficiency.

Cooperation and acceptance of responsibility is a must. With modern threats becoming apparent to us in the last several years, we understand that our traditional responsibility to ensure reliable service must include the need to ensure security, both physical and cyber.

Over the past several years, State commissions have begun to probe the cyber preparedness of our utility companies in the realm of the smart grid. In concept, the smart grid has the potential to provide many improvements in situational awareness, prevention, management, and restoration. In spite of introducing new weaknesses, smart grid fundamentally makes the electric system more secure.

In each of the areas that I have identified in my testimony, steps are being taken to manage the risk. The issue is how much money should be put into this effort when it is virtually impossible to stop all attacks, but vitally important to stop some.

Smart grid poses an additional and particularly thorny policy issue, as well. Through NARUC's collaborative with FERC on smart grid and other activities, State commissions have begun to identify key areas to assure the smart grid investments boast the highest, most sophisticated levels of security. Commissions, therefore, have had to become more expert in our understanding of the prudent smart grid and cybersecurity investments.

In Ohio, for instance, an extensive audit was recently performed on one of our utilities that complied with the NISTIR 7628, and industry best practices that were to identify potential areas of improvement were set forth. This effort was massive and will become

a best practices model for other commissions and utilities in their cybersecurity analyses and efforts.

My testimony also lists a significant number of activities that have been undertaken by the Ohio Commission, in our effort to become more advanced in our understanding of cybersecurity issues. I also identify several other States, including, Pennsylvania, Texas, Missouri, and New York, who are also making active steps to try and increase their understanding, as well.

A long-standing mission of every State public utility is to ensure the physical viability of the utility plan under our supervision. A less traditional responsibility, that of cybersecurity and information systems standards and development, is increasingly being thrust into the mix, and this newer responsibility clearly envelops a broader range of industries and specific expertise.

I see that I'm out of time, and the rest of my comments are in our written testimony.

Thank you.

[The prepared statement of Mr. Snitchler follows:]

PREPARED STATEMENT OF TODD A. SNITCHLER, CHAIRMAN, PUBLIC UTILITIES COMMISSION OF OHIO

Chairman Bingaman, Ranking Member Murkowski, and Members of the Committee, thank you for this opportunity to appear before you today as you examine the status of action taken to ensure that the electric grid is protected from cyber attacks. My name is Todd Snitchler, and I am the Chairman of the Public Utilities Commission of Ohio (PUCO), the State agency responsible for:

- assuring residential and business consumers access to adequate, safe, and reliable utility services at fair prices;
- ensuring financial integrity and service reliability in the Ohio utility industry;
- promoting utility infrastructure investments (including investments in IT infrastructure); and,
- related items like fostering of competition, safety, and even mediation responsibilities.

I am pleased to have been given this opportunity to discuss cybersecurity issues for the electric grid. We take for granted the reliability of our nation's grid and we are hyper-sensitive when we lose power because we are not generally accustomed to it—nor should we be.

Should Congress decide to pass legislation on cybersecurity, however, it must distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be addressed and resolved more deliberately. Particularly regarding the electric grid, one-size solutions for cybersecurity may not be the most effective means to mitigate and reduce known vulnerabilities. Additionally, the desired outcome for such legislation should be the establishment of a foundation that contemplates at least four basic considerations.

First, let us protect diamonds like diamonds and apples like apples. That is, we must prioritize accordingly to ensure that the appropriate level of security is provided to all areas that require protection.

Second, States and the owners of the critical infrastructure we regulate cannot protect the infrastructure to the maximum extent possible unless relevant Federal agencies provide the actionable information necessary to identify and address the threat and/or vulnerabilities—in other words true information sharing between those that have critical information (the Federal agencies) and those that need such information to protect their systems.

Third, our utilities can provide a "gold-plated" or even a "platinum-plated" system which is ultra-cyber secure. However, this raises the question of just how much more do we want a kilowatt hour of electricity to cost? While we understand that if the lights are not on it does not matter what the cost of the electricity is, do we really want the critical infrastructure to be so expensive that due to cost constraints it is no longer considered critical?

Fourth, preparedness should not focus solely on response capabilities, but should also ensure that resilience is built into our infrastructure—our nation's utilities

(municipal, cooperative, and investor-owned) have done this country proud in responding to the greatest calamities and catastrophes, quickly and capably restoring power after significant storms, hurricanes, earthquakes, wildfires, and even acts of terrorism.

As a State regulator, my fellow Commissioners and I, as well as our Staff, have many responsibilities. Some items of significance today are resolved and become less significant down the road. Other items that are less significant today may become of paramount importance in the near future with a major change in one variable like weather, for instance. This is true for many things, including the provision of electricity in a safe, reliable and economic fashion. Focusing on reliability, there are many factors that impact that aspect—physical infrastructure in place and operational considerations, such as generators, wires, substations, transformers, and meters. Also greatly impacting reliability is equipment failure. Equipment may fail due to its age, its overuse or underuse, physical vulnerabilities, and as we are aware, perhaps due to cyber vulnerabilities. Many of these vulnerabilities have existed and are known, while other weaknesses are more recently being better understood. Just as the electric utilities cannot protect against all threats, neither can they eradicate all susceptibilities. But we must recognize there are different parts of these systems that require different levels of protection. This is why we must ensure that there is adequate protection for the electric grid, especially the most valuable parts, while we must not expend undue levels of resources in protecting other, less important parts of the system.

Another important point of consideration that must be recognized is that State agencies like the PUCO, along with the owners of our critical infrastructure, are unable to provide the full measures of protection necessary to help secure our nation's critical infrastructure if the relevant Federal agencies do not provide actionable information to address imminent threats. State regulators take the reliability and security of the bulk-power system very seriously. Through strong Federal, State, public, and private partnerships, we have consistently maintained and improved reliability and security of the grid. As times and technologies have changed, new risks and vulnerabilities have emerged. The transition to a smarter, more efficient grid—while full of promise—carries with it unforeseen concerns and unintended consequences. As Congress considers legislation in this area, it should build on existing Federal-State coordination and result in a framework where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion.

However, identification of vulnerabilities is only one part of the main equation; equally, or even more importantly, is a need by the States and especially by the asset owners to recognize the threats to the nation's grid. We hear consistently from asset owners who provide information about their systems to Federal agencies in the spirit of cooperation, all the while seeking reciprocity, yet they never receive truly meaningful, actionable, timely information in return. They cannot protect all of their systems against everything; none of us can. They have to target their defenses and we have to help them understand the actionable threats so that they may bolster their defenses where needed.

As with most sectors of the economy, information systems are rapidly merging with utility systems, potentially heightening the risks of service disruption. Cybersecurity is an emerging area of risk for our utilities and for State Commissions as well; although it is unique in some respects, this is not the first time our utility systems have faced new reliability threats. Through a strong public-private partnership, we have overcome past risks, and it is my belief that this merging of information systems into the electric and other utility sectors improves their resilience, reliability and efficiency.

National security roles and responsibilities have been subject to the purview of Emergency Management Agencies, State Police, and Departments of Homeland Security. However, the lines defining and separating roles in critical infrastructure protection between the Federal government, State agencies, and the private sector owners of critical infrastructure are necessarily overlapping now. Cooperation and acceptance of responsibility is a must. With modern threats becoming apparent to us in the last several years, we understand that our traditional responsibility to ensure reliable service must include the need to ensure security—both physical and cyber. Breaches of security, obviously, can have extremely serious reliability consequences. From my vantage point, State commissions can identify certain key areas of concern about cybersecurity. The first concern focuses on business process systems—email, office computing, databases, etc.—that are not unique to utilities. In fact, commissions in recent years have improved their own security, along with everyone else, as attacks on these systems become more sophisticated and we become more dependent on them for our operations.

A second vulnerability is more specific to regulated utilities: control systems. Supervisory Control and Data Acquisition (SCADA) systems have been and remain an inextricable part of utility operations, and have served to improve the efficiency and reliability of our system operations in every system throughout the country. In recent years, susceptibilities in these SCADA systems have been repeatedly highlighted.

Over the past several years, State commissions have begun to probe the cyber-preparedness of our utility companies in the realm of smart grid. With tens of billions of dollars in investment on the line, commissions want to know that the investments are not going to introduce new and unmanageable risks. In concept, the smart grid has the potential to provide many improvements in situational awareness, prevention, management, and restoration. In spite of introducing new weaknesses, smart grid fundamentally makes the electric system more secure. Still, this technology brings with it new vulnerabilities and points-of-access to create intentional disruption, which should be taken extremely seriously. "Guns-gates-and-guards" analogs of password protection and "security through obscurity" must be augmented with a framework of maximum system resilience and next-generation safeguards that allow the network to be impregnable, even if devices connected to it are compromised.

In each of these areas, steps are being taken to manage the risk. The regulated companies that we oversee, through the North American Electric Reliability Corporation (NERC), are continuously in a process of developing and updating standards for cybersecurity that we believe are a good step in the right direction for SCADA and business process systems. NERC, for example, has adopted a cyber-security standard for the bulk electric system. NERC's cybersecurity ("CIP") standards are extensive and thorough. Over the past five years electric utilities across the country have requested significant additional staffing and dollars for CIP standard compliance activities in their transmission rate case filings at FERC. The CIP standards already in place are adequate for both physical security and cyber-security. However, extending the applicability of those standards to lower voltage facilities raises the question of how much more we are willing to pay for a marginal increase in cybersecurity. The issue of how much more money should be put into this effort when it is virtually impossible to stop some cyber attacks (e.g., hackers getting into the Pentagon's computer system) needs to be addressed.

Smart grid poses an additional, and particularly thorny, policy issue as well. Through NARUC's collaborative with FERC on smart grid and through other activities, State commissions have also begun to identify key areas to assure that smart grid investments boast the highest, most sophisticated levels of security. Recent Federal funding support for smart-grid investments has incentivized the deployment of hardware in advance of the development of standards for cybersecurity, among other issues. Commissions may be confronted with expenditures on cybersecurity for which no specific standard has yet been reached. This draws commissions into specific areas of review in order to determine the prudence of expenditures—a review that would be unnecessary if the expenditure would be made in compliance with recognized standards.

Commissions, therefore, have had to become more expert in their understanding of prudent smart grid and cybersecurity investments. Because we are driven by our obligation to assure the reliability of service for our ratepayers, we must better understand the prudence of the costs in ensuring reliability (including expenditures for cyber-security) that goes into their rates. As a result, our agency has expended significant time and resources to become better educated regarding cybersecurity. Over the past several years, as the electric industry aptitude has grown regarding cybersecurity, so too has that knowledge base grown across State commissions.

In Ohio, for instance, regarding the smart grid discussion above, an extensive audit was conducted to assess the degree to which Duke Energy Ohio's Smart Grid system complied with the NISTIR 7628 and industry best practices and identify potential areas of improvement, which was a precursor to the action items in the stipulation. An internal audit was also provided during the audit and included penetration testing on a number of Smart Grid assets. An extension stipulation was reached regarding Duke's cybersecurity plan and the implementation of that plan, including the role of the Commission. This effort was massive and will become a best practices model for other commissions and utilities in their cybersecurity analyses and efforts.

We have been very involved in the NIST's and now the Smart Grid Interoperability Panel's (or SGIP's) Cyber Security Working Group. My agency has been very active in pursuing cybersecurity training opportunities with Idaho National Labs, NIST & NIST's ITL Computer Security Division, the SGIP, EnerNex, NERC's Grid Security Conference, and others, as well as participating in the development of the

initial NIST-IR 7628, the most recent version being a multi-volume compendium of Smart Grid Cyber Security Strategy and Requirements. We have actively participated in the National Association of Regulatory Utility Commissioners (NARUC) Cybersecurity Boot Camps. Additionally, our Staff participates in two different sets of regular, twice-monthly conference calls with our colleagues from across the country. These calls address critical infrastructure protection issues, cybersecurity issues for utilities, as well as smart grid development and implementation issues. Our Staff participates in monthly threat briefings for both the electric sector as well as the oil and natural gas sector. Also, our Staff regularly participates in weekly briefings with Ohio Homeland Security. Through this partnership, our agency has a permanent seat at the State of Ohio's Strategic Analysis and Information Center (or SAIC), just as it does in our State of Ohio Emergency Operations Center. Presently, the State of Ohio has developed a Statewide Cybersecurity Strategy and our Staff has been actively engaged in both the development as well as the on-going implementation of that strategy. Over a year ago, my agency conducted a cybersecurity workshop for our utilities as well as for our State and Federal partners. Leading part of that workshop was a representative from the U.S. Department of Energy's Cybersecurity for Energy Delivery Systems program. Also participating was Ohio's Homeland Security Advisor, as well as representatives from the cyber squads from both of the FBI divisions in Ohio. In addition, the two U.S. Department of Homeland Security (DHS) Protective Security Advisors stationed in and serving Ohio addressed not only their physical protective security program, but also DHS's cybersecurity advisor program and the related cyber resources and tools available from DHS for asset owners. Our efforts in strengthening the cybersecurity posture of Ohio's utilities continue.

Ohio also has one of the premier military bases in the country—Wright-Patterson Air Force Base. Located in the south-western portion of the state, this base employs a significant number of personnel and performs mission-critical work for the Department of Defense. My agency has worked with this base in the past, and will do so in the future, to ensure that it has what it needs to accomplish its objectives.

While I am not an expert on what other States are doing with regard to cybersecurity, I am aware of a few examples of activity that State commissions have engaged in, to ensure that companies are focused on this issue. In most instances these activities are coordinated with other State agencies that also have a jurisdictional responsibility for safety and/or security.

Since 2005, the Pennsylvania Public Utility Commission has required all jurisdictional utilities to have a written cyber security plan to complement their emergency response, business continuity and physical security protocols, each of which are tested on an ongoing basis. The Pennsylvania PUC has issued orders on cybersecurity in reaction to media reports of grid infiltration by international hackers. Pennsylvania also issued a secretarial letter to its utilities encouraging them to be active in the NIST Standards development process by reviewing and commenting on the NIST Framework and the Cyber Security Coordination Task Group documents and to participate in various related working groups. Pennsylvania has also incorporated cyber-security review in its management audits process. Pennsylvania performs management and efficiency audits at least once every five years on all electric, gas, and water utilities with over $10 million of plant in service.

Another State taking action is Missouri. Missouri requires all of its utilities to have in place reliability plans and has queried its utilities about steps taken or planned regarding cybersecurity as it relates to company operations. The Missouri Commission required the utilities to furnish Staff with a verified statement affirming whether the company is in compliance with NERC Order No. 706 or what remedial actions are to be taken and how long it will take the company to become compliant. The Commission also asked what other organizations, groups, industry groups or other organizations these companies participate with, such as local FBI or State agencies, regarding security issues.

In New York, they are sharing the responsibility for critical infrastructure protection at the Department of Public Service. Since 2003, when it was created, the New York State Public Service Commission Office of Utility Security has carried out a regular program of oversight of both physical security and cybersecurity practices and procedures at the regulated utility companies in the energy, telecommunications and water sectors. Staff of this office is devoted full time to this security audit responsibility. Generally, that office utilizes the existing NERC CIP standards as benchmarks to form its own judgments about the quality of cybersecurity measures in place at New York's regulated utilities. Its Staff adheres to a schedule that calls for visiting each regulated electric utility company four times a year to audit compliance with some portion of the CIP standards, with the goal of measuring compliance with all of the standards at each company over the course of a year.

The Public Utility Commission of Texas has established a stakeholder working group (comprised of utilities and ERCOT Staff) designed to work on issues specific to cybersecurity. This effort is lead by Texas Commission Staff. The group meets regularly to discuss the cybersecurity assessments performed on Smart Meter Texas, which is the common portal that provides end-user access to energy usage data sourced from the AMI that was deployed by the respective utilities. Each utility is responsible for securing its own AMI and cybersecurity assessments are required of the utilities by rulemaking once deployment of AMI and other smart grid technology is approved. Regulations include requirements for end-to-end assessments, performed independently and annually of the utility system. These results are kept confidential but shared with the Staff.

In addition commission staff participates in the discussions at the ERCOT ISO Critical Infrastructure Protection Working Group (CIPWG), in which NERC CIP issues are discussed. While this concerns the bulk electric system, other topics related to cybersecurity that are broached include: newly discovered vulnerabilities; emerging threats to critical infrastructure; cybersecurity standards development from outside NERC; mission assurance for the military; and any cybersecurity training opportunities, conferences, workshops, or exercises.

A long-standing mission of State public utility commissions is to ensure the physical viability of the utility plant under their supervision. A less traditional responsibility, that of cybersecurity and information systems standards and development, is increasingly thrust into the mix, yet this newer responsibility clearly envelops a broader range of industries and specific expertise. Utility regulators recognize the dependence of sound cybersecurity practices and cyber reporting on sound construction practices and utility-outage reporting, and vice versa.

A concern that I wish to leave with you for consideration is that protocols intended to distinguish between disruptions to critical infrastructure related to cyber events and those related to physical events, for example, a distributed-denial-of-service (DDOS) attack as opposed to a fiber-optic cable failure, have not kept up with the fast-emerging nature of cyber threats. Such protocols are easier to craft than to implement. The first evidence of disruption is the disruption itself, and such events do not often present themselves with the root cause clearly visible.

In the critical "golden hours" after a possible new developing threat is detected, or immediately following an event, it may not always be clear what is actually happening or why. For this reason, close coordination between the utility sector and the cyber sector is essential to the response. As the State public utility commissions have traditionally served as the gateway to the utility sector and have their own independent core of expertise and relationships key to understanding, in real-time, events affecting that plant, close coordination among the operators of our cyber networks, the Federal government, and State homeland security partners, including State utility commissions, is essential. Resolving cybersecurity issues will require significant efforts on the parts of all of us, not just one or two of us. We all are part of the solution. Working with the asset owners and with our Federal partners, the States have been successful in the past in enhancing the overall reliability of our nation's electric grid. Our Federal government possesses significant assets that can provide States and the critical asset owners with timely and actionable threat information necessary to better secure these assets. We are partners in this struggle to maintain and enhance the reliability of our electric grid and to increase its resiliency, and we must all work together to achieve our collective goal.

Mr. Chairman and members of the Committee, this concludes my testimony. We at the Public Utilities Commission of Ohio take the issues of cybersecurity and reliability very seriously. As such, we believe a Federal-State, public-private partnership is essential to meeting these challenges over the long term.

Thank you again for the opportunity to provide testimony here today and I would be happy to answer any questions that you or members of the Committee may have.

The CHAIRMAN. Thank you. Thank you, all, very much for your testimony. I will start with a few questions.

Mr. Cauley, let me ask you first, Could you describe what happens when a vulnerability is discovered, vulnerability to a cyber attack, for example. If you issue an alert to utilities about that vulnerability, is there any requirement that they follow your advice on that alert?

Mr. CAULEY. Thank you. We produce the report with intelligence information from the Government, with cleared experts. We create a document that we can then issue to industry, which is unclassi-

fied. We have 3 levels that we can issue. One is an informational heads-up. One is a recommendation, which we can track the results and performance of the recommendations. The third is an essential action, if we feel that it is imperative that the industry implement that. Then, our board can approve it, and it is a required action, and the industry is required to report back the results of that performance.

The one area I pointed out last year in testimony was the—even though the industry is required to report back and they are required to implement the action, there is not an enforcement mechanism for that. I appreciate that in the discussion of that legislation, there was an inclusion to deal with that gap.

The CHAIRMAN. So, at the current time, if you issue an alert and you say, "Take the following action," and the utility does not do so, you have no ability to enforce that?

Mr. CAULEY. The industry is required to respond by our rules and by rules that FERC has approved, so the—we are limited at this point to a civil action, but not within our current rules and our current framework.

The CHAIRMAN. So, you can take them to court?

Mr. CAULEY. We could.

The CHAIRMAN. But there is no immediate penalty or immediate remedy available to you.

Aurora, I guess, is the most famous cyber vulnerability that has sort of gotten a lot of publicity. It was on CNN for several days back in 2007. You issued an advisory for that vulnerability, I believe; is that correct?

Mr. CAULEY. That is correct.

The CHAIRMAN. Are you able to track how many utilities still have not complied with the recommendations in that advisory?

Mr. CAULEY. We were able to—one of the first things I came—did when I came back to NARC as CEO in the beginning of 2010, as I recognized that the information that the industry had from 2007 was insufficient, unclear, and, essentially, not actionable—so, we worked to issue another alert in 2010, which, I think, points out the importance of information sharing and access to information. So, we were able to put out a meaningful alert in 2010. We are tracking on a twice-yearly basis. We are tracking on the completion of mitigation. We have that information, and we file it with the Commission. It is sensitive information because of the nature of the vulnerability, but we do track that and file that with the Commission.

The CHAIRMAN. It seems to me—and you can just respond and tell me if I am misstating the situation. But it seems to me that the way the standard-setting process works, standards should be developed as a general framework for exercising authority to require mandatory actions in the case of a vulnerability being discovered. In fact, the way the system is working is that you are required to issue a new standard, with all of the accompanying delay, for any new threat that comes along, or if you don't do that, then you are left only with the ability to make non-binding recommendations. Now, is that a fair statement of where things stand?

Mr. CAULEY. I think, Mr. Chairman, not every risk or challenge or vulnerability requires a standard. We get a lot of things cor-

rected with information and just explaining to the industry what the issues are. There is a lot of problem-solving going on every day.

Alerts give us an opportunity to deal with emerging issues or issues that need a timely response. Whether or not we could develop—we could develop a standard on Aurora. The difficulty with that is, it is more of an equipment manufacturing-type standard, which is more applicable to an IEEE, the Institute of Electronic and Electrical Engineers, and I understand that they are committed to looking at that issue as a technical standard on equipment.

If the Commission felt that there was a vulnerability that had been out there and had been out there too long, my belief is that, within the current section 215, the Commission could issue an order to the ERO to produce that standard, if it was a priority over other risks that we are dealing with.

The CHAIRMAN. Senator Murkowski.

Senator MURKOWSKI. Thank you, Mr. Chairman.

I am going to ask a little bit more about information sharing. It is something that each of you has addressed. Clearly, the NERC plays a role here with the Electricity Sector Information Sharing and Analysis Center, where you share and analyze the information. You have mentioned some of that. But it sounds like even from NERC's point of view, you would urge Congress to do what it can to facilitate further information sharing.

Mr. Snitchler, you have indicated how important it is that the Federal agencies provide the actionable information, too, to help address or identify threats or vulnerabilities. GAO has also mentioned that.

So, let me start with you, Mr. McClelland. Does the FERC think that the private sector has the information that it needs today to take action to address the cybersecurity threats and vulnerabilities from the information sharing perspective; do you have in place what you need?

Then, if I could ask each of you to just further address this, because I think this really goes to the heart of what we are talking about here today.

Mr. MCCLELLAND. Thank you, Senator.

I think, in general, the security practices are well-documented. I think there are protocols to standards. There are alerts and advisories that detail specific security protocols to improve the security posture of the utilities.

But, specifically, no, there are circumstances where there may be a specific actor that has targeted a particular piece of equipment or an operating practice. In those cases, it is important that those individual entities, and the industry at large, perhaps to a lesser degree if they don't have that specific equipment, is brought in, counseled, shown the threat, and then, any particular mitigations that could be applied are explained to that entity.

Senator MURKOWSKI. So, then, to the rest of you. How do we do a better job of the information sharing?

Mr. Wilshusen.

Mr. WILSHUSEN. One is to make sure that there is an appropriate mechanism in which—in place to actually share information on a timely, actionable basis.

We did a review a couple of years ago at the Department of Homeland Security, of its lead role promoting the private-public partnership in securing our critical infrastructures, which include the electricity grid. We found that, to a large extent, the information that DHS provided through its alerts and threat information was not meeting the expectations of its private sector partners.

In many cases, the information was not actionable, not timely. So, one of the means that would have to take place is to ensure that the information that is being provided is current, timely, and also anonymized. That has been one of the problems, is making sure that the information is sufficiently anonymous, so as not to identify any particular company or organization, but gets the information out to the individuals who actually put fingers on keyboards and secure the systems.

Senator MURKOWSKI. Mr. Cauley.

Mr. CAULEY. Senator Murkowski, I fully agree with the suggestion that the most important thing that legislation could do would be to foster a robust information sharing between Government and industry.

Today, it is happening, but it is sort of like sipping from a lawn hose. We just need more. Also, the information sources are ad hoc across agencies, so we work out individual relationships with agencies to get information. We have a very limited access to clearances within the industry, particularly on the top secret side. The value of that is, only industry experts can really, fully understand the impacts. Often, our limited folks that we have that do have clearances are explaining back to the intelligence folks what might be the impacts for a particular threat. So, I think getting more clearances, having a more unified system for sharing of information would be very beneficial.

Senator MURKOWSKI. Mr. Snitchler.

Mr. SNITCHLER. Senator, what we hear from the utilities that we regulate is, often, that there is—they perceive a one-way information street, and they provide information and don't feel that they are getting a reasonable amount of information in return. By that, as already mentioned by other panelists, some of the specific data that could be helpful to them.

There is also, I think, often times, the fear of disclosure will result in practices that maybe impact one utility, as opposed to all of them equally. So, there is a reluctance, perhaps, to share granular detail that might be helpful.

Again, the anonymized information that was previously referenced, I think, would be helpful for that, because then it would ensure that we could have better disclosure of information in both directions.

The critical component that we hear from utilities, without exception, is the need for security and that information not to find its way out into the public realm because of the potential implications, both to them and to the utility system.

Senator MURKOWSKI. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. Mr. Chairman, thank you for holding this hearing. I think it is extremely timely, in light of the leader's desire to bring cyber legislation to the floor.

I want to review with the 4 of you, essentially, where things are, on a couple of key questions.

Now, as Chairman Bingaman noted, there are already rules in place that include cyber threats to the electric grid, and that, of course, was launched years ago. Now, this exercise seems to have produced another division in what I call the "growing cyber industrial complex." For years now, the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation, private companies, and lots of lawyers have shuffled paper back and forth, grants have been dispensed by the Department of Energy, and this has produced a product that has left few satisfied.

So, let me start with you, Mr. McClelland, in terms of some of the concerns that would be helpful to have addressed this morning. Do you believe that because the standards don't require a physical separation, between the energy company networks that run the business operations and the critical infrastructure—the substations and the transmission—that despite all of this paper shuffling, this shortcoming is still a significant factor in making the electric grid vulnerable to attack?

Mr. MCCLELLAND. I will answer that and then maybe add a little to it, is that one of the CIP standards, CIP 5, requires an Electronic Security Perimeter around a critical cyber asset. Only critical cyber assets, which are self-designated by the entity that is captured by the standard, are covered by the standards themselves. So, if an entity decides it has critical cyber assets, then it designates an Electronic Security Perimeter around those assets. If the business systems are connected to the critical cyber asset, via the SCADA systems, or whatever the control systems are, then those business systems, theoretically, fall within that Electronic Security Perimeter.

So, if they are interconnected, if they work together, if they can't be separated, the assumption I would have is that they would be within—they would both be included within that ESP and physically protected.

Senator WYDEN. But the bottom line is, the networks don't have to be separate, is that correct?

Mr. MCCLELLAND. That is correct.

Senator WYDEN. OK. The second question I would like to ask of you is, that, for purposes of the legislation that is being considered for the floor of the Senate here before August, some companies are asking, that for purposes of this bill, they should be legally protected—legally protected through indemnification provisions when they report vulnerabilities in any cyber network.

Now, it is my understanding that, with respect to the 2005 law, there is no such legal protection; is that correct? If so, is the absence of that kind of legal protection or indemnification processes—has that caused any problem in your view?

Mr. MCCLELLAND. Under the cyber standards or any of the reliability standards, one of the considerations under the violation severity level is whether or not an entity self-reports its problem. That is taking into consideration, as far as the enforcement provision, the penalties, how willing they are to admit that they have a problem, what the mitigation plan looks like, how timely they could be. So, self-reporting is an important aspect, as far as mitiga-

tion of the enforcement aspects, even under the existing network or the framework.

Senator WYDEN. But the question is, Are there indemnification procedures now? My understanding is there are not.

Mr. MCCLELLAND. Right.

Senator WYDEN. Is the absence of these provisions causing any problem? The reason I am asking is because this is going to be a big issue in the discussion, is whether or not there ought to be these indemnification processes when companies come forward and report problems. What I would like to know is, if there are any problems today, as a result of the lack of reporting requirements. Could you answer that?

Mr. MCCLELLAND. I guess I would answer it by saying that, the self-reporting requirements—you know, the enforcement provisions under the existing standards are important, and if it is not a standard that compels action, then it is not something that you can assure happens.

You know, information exchange, alerts, advisories, essential actions can be helpful. But, at the end of the day, if there is no enforcement provision, it—there is no teeth behind these issues.

Senator WYDEN. I will try one more time. Do you think——

[Laughter.]

Senator WYDEN. Do you think indemnification procedures are needed for purposes of this bill that is going to be considered for the floor before August, yes or no?

Mr. MCCLELLAND. I am just not prepared to comment on that. I'm sorry.

Senator WYDEN. OK. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Franken.

Senator FRANKEN. Yes, Mr. McClelland, do you think—no, I'm not good at that——

[Laughter.]

Senator FRANKEN. But this question is for you, and for anyone who wants to pick up on it. Deploying a smart grid is crucial for integrating distributed and renewable energy resources, but a 2011 GAO report noted that, while FERC has authority to adopt smart grid standards, it does not have any specific enforcement authority to implement these.

What are your recommendations for ensuring that standards are properly developed and enforced? Is this issue adequately addressed in any of the cyber security bills before the Senate?

Mr. MCCLELLAND. The GAO did find—they did echo FERC's finding from its policy statement on smart grid, that it lacked enforcement authority under the EISA that was passed by Congress. So, we do not have enforcement authority, even if we find that cybersecurity standards, as recommended by NIST, achieve sufficient consensus.

The Commission's authority, however, does lie under 215. So, pursuant to that authority, the Commission has been an active participant in NIST's SGIP and Cybersecurity Working Group. Our staff attends those meetings. They are regular participants. They bring that information then back to the NERC 215 process when they actively engage in the standards development teams under the cybsersecurity standards. In fact, the Commission most re-

cently, in approving version 4, even reminded NERC that it needs to consider those NIST provisions and incorporate those NIST provisions, as appropriate, in version 5 of the standards.

So, I can't speak to the pending legislation. I'm sorry, Senator. I'm just not current with it. But I can say that the Commission is actively engaged in the NIST process, is actively working to incorporate the relevant aspects of that NIST process into the NERC standards.

Senator WYDEN. Mr. Wilshusen——

Mr. WILSHUSEN. Yes——

Senator WYDEN. You helped prepare this report, so do you have any comment?

Mr. WILSHUSEN. Right. I would just add that what Mr. McClelland is referring to with section 215 is their ability to enforce mandatory standards established by NERC over the bulk power system. But under the Energy Independence and Security Act, which deals primarily with the implementation of smart grid technologies, much of those technologies are implemented and deployed at the distribution level, which is more under the purview of the State regulatory commissions and others.

I believe FERC does not have the enforcement capability at that level, under EISA or——

Senator WYDEN. Mr. Snitchler, that is fine with you?

Mr. SNITCHLER. Senator, we——

Senator WYDEN. From what I am hearing?

Mr. SNITCHLER. Correct. We think we have got an adequate handle. Ohio has approached the smart grid deployment than other States—each of us has approached it in a different fashion—where we have rolled it out in a series of pilot projects with one utility that is now moving toward full deployment, others who are further behind the curve, but are moving forward. We have been able to work closely with those utilities to make sure that they are operating in a way that gives us a level of comfort, that they have a sufficient amount of security going forward.

We actually have had a couple of open dockets at the Commission, in an effort to determine where companies are at, what steps are being taken. But, like other State commissions, it is sometimes a challenge to have our utilities come in and disclose the weaknesses in their system. So, the issue of confidentiality, again, rears its head, even at the State level, as we try to protect that information and prevent it from becoming part of the public domain.

Senator WYDEN. Taiwan, Singapore, China, South Korea are among the largest manufacturers of semi-conductors and microprocessors for these smart devices.

There are concerns that if a cyber criminal gained access to such devices, especially during a manufacturing process, they could covertly insert code in the devices to impair its function.

For any of you, are we testing these purchased devices to mitigate potential vulnerabilities?

Mr. WILSHUSEN. I guess I will take that question first. IT supply chain has been a key vulnerability into systems and the critical infrastructures of this Nation. We issued a report earlier this year that dealt with IT supply chain and dealt specifically with some of the microprocessing chips.

We looked at several agencies, including DHS, Energy, Department of Defense. To a large extent, we found that the procedures for reviewing the vulnerabilities on IT supply chains and the types of equipment that are being acquired, agencies really have not established effective mechanisms to adequately address that vulnerability.

To some extent, it needs to be done at the national level, because the risks are more national in scope. The administration has recently developed an IT supply chain strategy. We are in the process of looking at that strategy as part of our ongoing work.

Senator WYDEN. My time is up. Does anyone have another comment? I saw Mr. McClelland be nodding.

Mr. MCCLELLAND. I would only add that, you know, hardware is one component. Any time there is two-way electronic communication, there is a chance for compromise, and there are some very sophisticated entities out there that employ various mechanisms, including hardware compromise, to accomplish that task. So, it is a critical aspect of network security.

Senator WYDEN. OK. Thank you, gentlemen.

Mr. Chairman, thank you.

The CHAIRMAN. Mr. McClelland, you mentioned this problem of electromagnetic pulse events. I gather our former Congressman and Speaker, Newt Gingrich, had a op-ed in the "Washington Post" this last week, where he argued that we need to pass legislation to protect against electromagnetic pulse events, and you seem to say the same thing in your testimony as I read it.

Is there anything being done, just at the current time, to deal with this problem?

Mr. MCCLELLAND. The Commission recently held a technical conference on this very subject. It invited NERC and industry experts, and it compared the Commission's report through the Oak Ridge National Laboratory, to the NERC report. It asked for comments and sought consensus.

So, the Commission does have the industry's comments. We are reviewing what can be done, where there is areas of agreement and disagreement. But one thing that was encouraging from the conference is that we thought we heard, regardless of the scale of destruction or damage to the equipment itself, there would be a widespread grid collapse, and everyone agrees that that must be prevented.

So, coordinated studies need to be done among the entities. There are, likely, standards that need to be passed, not necessarily NERC standards, but industry standards, to prevent, you know, damage to vulnerable equipment. There is a subset of critical and vulnerable equipment that should be protected—no regrets actions that should be pursued to protect the public against this issue.

The CHAIRMAN. I guess one obvious question is, What kind of timeframe are we talking about here? I have the distinct impression we may be studying this issue while the electric grid collapses. What is your understanding of the timeframe to get something done?

Mr. MCCLELLAND. The Commission is moving through completion of reviewing those comments, and under existing authority, it can address the geomagnetic disturbance issue through reliability

standards. So, the Commission is now informing itself from the NERC study, from the Oak Ridge study, and from the public comments, and it is moving to review its options under its existing authority to address the issue.

The CHAIRMAN. So, does that mean this year something is going to be done?

Mr. MCCLELLAND. I'm sorry, I just can't speak to the timing of Commission action.

The CHAIRMAN. Whenever people talk about, "We're moving to review our options," that doesn't sound like anything imminent to me.

Mr. Cauley, did you have a point of view on this issue? What is NERC doing to solve this problem of the threat from electromagnetic pulse attacks?

Mr. CAULEY. Thank you, Mr. Chairman.

We issued a report in February, which put the engineering and science behind the characteristics of what kind of failures and things we might see, and we have initiated a number of actions. We issued an alert to industry. We have been working with NASA and NOAA in terms of enhancing the alert system, so we can let industry know if there is an issue impact coming, and that we can put the system in a more conservative position to withstand an event.

We are also working with EPRI, Electric Power Research Institute, in terms of locating monitors on—Earth current monitors, as well as equipment monitors, so we can understand and see the behavior of the impacts and know what we need to do to address that.

This is a long-term effort. I realize that we could have impacts near-term, but really there is a lot to learn and develop. We are also looking at doing testing on transformers, in terms of inducing Earth-type simulated currents in them and seeing how they behave and how they react.

So, there is a lot of working on them on multiple fronts. We are not waiting for standards. We are actually moving on the engineering and the modeling and the operational——

The CHAIRMAN. When you say you issued an advisory—or an alert, I guess—what did you refer to it as, an advisory or an alert?

Mr. CAULEY. It was a NERC alert, yes.

The CHAIRMAN. An alert. Was that a set of directions to utilities to take particular action, or was this just basically saying, "Here's a problem"?

Mr. CAULEY. This one was informative, sir, so it gave actions that could be taken if there was a impact full storm that was going to come toward the Earth, actions that would be recommended to be taken. But it was not issued as a required set of actions.

The CHAIRMAN. So, no required actions have been——

Mr. CAULEY. Not in this particular——

The CHAIRMAN. Recommended——

Mr. CAULEY. That is correct.

The CHAIRMAN. At this or put forward?

Senator Murkowski, did you have other questions?

Senator MURKOWSKI. This is more of a general question to all of you. I think Mr. Wilshusen, you mentioned that, perhaps, stand-

ards should not be spelled out too specifically or utilities kind of get in this compliance mode of trying to meet the standards, instead of safeguarding the systems.

We want to push everybody to be one step ahead of the guys that are trying to disassemble things, and so, we don't want to get them focused on just checking the boxes off; we need them to be thinking ahead every single day. This whole issue of flexibility within a system, as opposed to a prescriptive set of standards concerns me. My concern is that the legislation that is being considered right now, not the secure IT, but what is coming out of Homeland, is a more prescriptive approach.

Can I ask each of you to speak just to that issue, as to the need for flexibility in this area that allows us to be a little more nimble, rather than just complying with a set of standards?

We'll just go from you, Mr. McClelland, on down.

Mr. MCCLELLAND. Thank you, Senator.

I agree. I think all of the panelists would, too, that the individual entities have to have the latitude to have the directive, but not be so prescriptive as to tie them into any singular response.

On the other hand, though, someone needs to make certain that the Mitigation Act is effective. Back to that question about Aurora, you know, it's not enough just to collect survey data; it is important to verify the mitigation. So, I agree; I think the standard needs to compel action, but provide the latitude that the individual entities might need to address the issue on their systems.

Mr. WILSHUSEN. Yes, definitely, I think standards need to be flexible. They should not be overly prescriptive, because you want them to stand the test of time. You don't want to necessarily change your standard every time there is a new threat or a new technology that emerges that presents additional vulnerabilities.

As a parallel, in the Federal Government, NIST issues Federal information processing standards, which are mandatory requirements. In addition, though, it has issued lower levels of guidance, usually through special publications and guidelines that provide increasingly more detailed actions that can be taken to secure systems in cybersecurity. But they are more prescriptive, and they are at a greater level of detail than the actual Government-wide standards. This greater level of detail is needed to effectively secure systems.

So, it is good NIST had that flexibility and multiple layers of guidance—standards, guidelines, and instructions, if you will, to provide to organizations to secure their systems.

Senator MURKOWSKI. Mr. Cauley.

Mr. CAULEY. Senator Murkowski, I agree, as well. The most effective standards will be based on risk controls, setting up systems to catch issues that need to be identified, not on a prescriptive, line-by-line, rule-based-type standards. We are adopting those risk controls in the version 5 standards. We are looking at the NIST model. We have extracted from their set of standards, the ones that we think would work in the power system, and we are flushing those out within those standards.

There is an added factor within—in the security arena, is that you really want to incent people to report issues. Because part of the intelligence is finding out what are the bad guys doing and

what information are we finding, and lots of little pieces mean something when you roll it all up together.

So, if we are going in with a checklist style of compliance, it is not going to be helpful that. We want people reporting information, actively. I think we are on the right track for that.

Senator MURKOWSKI. Mr. Snitchler.

Mr. SNITCHLER. Senator, at the risk of saying, me, too, I would agree with the comments made by the prior panelists. I think the flexibility that you have suggested, necessarily, moves into that resiliency that can be developed by the multiple utilities that we regulate, taking a different approach to achieve to same objective. That diversity of approach to solving a problem also potentially has the ability to keep an entire system from being knocked down, because, instead of targeting one set of security concerns, you are looking at more than one set and ways that that problem may have been solved, and has the ability to require far more effort on the part of those that will do ill-will to the electric grid or to those who may be seeking to try and damage the country.

I think, also, by moving away from a prescriptive, check-the-box, as you describe it, list is helpful, and that we are then charging the utilities that we regulate with being as far as they can, one step ahead of, in evaluating all the threats, whatever they may be.

I know that I have been to at least one utility in Ohio's command center where they are doing just that and have retained security folks to deal with those issues, in an effort to ensure that they are viewing all the potential sources of entry and all the potential manners in which they can respond and block those out, at various levels within their system.

Senator MURKOWSKI. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Udall.

Senator UDALL. Thank you, Mr. Chairman.

Good morning to all of you. Thanks for joining us on this important topic.

Mr. McClelland, if I could, I will start with you. This may be a tangent—a slight tangent, more accurately. I don't know if any of the witnesses have addressed work force issues in their written testimonies, but I realize one of NERC's standards refers to personnel training requirements.

I am curious whether you believe we have the right people with the right training in place at FERC, at NERC, at the utilities, or elsewhere, to develop and implement the standards to keep the grid secure and respond to threats and vulnerabilities.

Do you think we would be more secure with additional and better training to cyber warriors?

Mr. MCCLELLAND. I would say, yes. We do have—the Commission is fortunate to have—it is a small staff, but it is a very talented staff that we have mostly drawn from other agencies, and they have spent their entire careers in cybsersecurity. I think NERC is also gifted with some of the employees that they have in place. But these folks are as scarce as hen's teeth, and it is difficult to find them. In many cases, we steal them from each other.

That said, we have been able to—and I know NERC has also taken advantage of this. We have leveraged the intel agencies with some of the best, probably—well, undoubtedly, the best skill sets

in the world. So, we leverage those intel agencies to help us understand what the issues are and to address the threats. But, certainly, more and well-trained cybersecurity people are something that we all need.

Senator UDALL. Others on the panel, care to comment?

Mr. Cauley.

Mr. CAULEY. Gerry Cauley, NERC. I believe that is an opportunity for us, and I think we do need to expand and grow our work force in terms of capabilities. It is another example of an opportunity to partner between Government and industry. There is a training program at the Pacific Northwest Lab, and we have been running as many industry folks as we can through that. It is a very good, week-long program. It is very intense. But, we need more of that.

Mr. WILSHUSEN. I would——

Senator UDALL. Mr. Wilshusen.

Mr. WILSHUSEN. Yes, thank you. I would just add that, not only just within NERC and FERC, but throughout the Federal Government. We have issued a report earlier this year, too, about human capital challenges within the Federal Government, securing Federal systems. Indeed, that is an area that is a prime consideration and concern.

Mr. SNITCHLER. Good morning, Senator.

Senator UDALL. Mr. Snitchler.

Mr. SNITCHLER. One of the issues that we have found, anecdotally, in talking with our utilities in Ohio, is that they have actively recruited from within the military, and have had good success with folks who are used to dealing with top secret clearance and higher on issues that involve issues of this nature at the utility. They have found that to be helpful.

That being said, they are also at a premium, and it is very difficult to find sufficient staff. I would agree with the prior comments about this being an opportunity for specific work force development that has long-term implications for the country.

Senator UDALL. Mr. Wilshusen, let me turn to you for the next question.

You talk about the difficulties in the industry of sharing information on cybersecurity. Could you describe some ways that you think the electricity industry could improve in this area?

Mr. WILSHUSEN. Yes, I think there are a couple of areas. One would be to have a mechanism in place in which the industry can collect actionable intelligence—or information about security incidents and vulnerabilities that may be present within the industry and then being able to share it with other members, but after it is been anonymized.

Before you came, we talked about the need to anonymize certain threat information, alert information, so as not to put other companies in peril. Then, those companies may be more willing to share information that they may have of any incidents occurring at their organizations. So, that will be one key area.

Another is, to receive information from Federal sources and through NERC and FERC; particularly, getting additional information through the intelligence community, through Department of Homeland Security, on threats that are occurring and

vulnerabilities that are happening within those particular industries.

Senator UDALL. Let me follow that up. In Colorado, we have the Western Cyber Exchange, which is a public-private partnership, and it works on a regional geographic basis, both on improving cybersecurity, and then on incident response.

Do you think regional cross-sector models like this are something we could encourage and should encourage?

Mr. WILSHUSEN. I think they serve their place. You know, regional would help. But many of the threats are international in scope and come from other sources from which regional utilities—or groups may not have that information. That is why it is important at the Federal level, at least, threat information, alert information from the intelligence community, through DHS, be shared with those particular groups.

Senator UDALL. Mr. Cauley or Mr. Snitchler, would you care to comment on that question, as well?

Mr. CAULEY. Yes, sir. We have the Information Sharing Analysis Center, and what I think we are trying to create is hubs of information connected to other hubs. So, ours is focused on the power system in North America, but we are connected to intelligence agencies, U.S.-served and other—the NCICs, who are plugged into these other sources, and we share information with our members in North America.

I think the one other thing that we could do better is to have more access to clearances, and to create what I would call "fusion centers," perhaps in cooperation with the FBI local offices, regional offices, where we can quickly get very detailed information at the classified level to people in industry who can understand, at a very granular level, what is the threat, and what actions should I take. That is an opportunity for us to think about.

Mr. SNITCHLER. Senator, I think I would echo the comments from the GAO, where actionable information that has been sufficiently anonymized would be helpful, because the issue that we often hear is the question of, If I provide information, will this later be used against me? If it is, obviously, they are reluctant to share that information.

Frankly, if we get into a situation where we have a better way to exchange information, we can be implementing best practices and avoiding each individual company's having to uncover and discover the same problem and work their own solution, but would then have, in effect, a clearinghouse of known issues. Then, they could work to solve that with the flexibility within the standard that may be required.

Senator UDALL. Thank you all, again, for appearing and discussing this very important topic.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Coons.

Senator COONS. Thank you, Chairman Bingaman.

Senator Bingaman, you have been beating the drum on this issue for some time now, and I was happy to join you last year in supporting the Grid Cyber Security Act.

I am grateful to you and to Senator Murkowski for convening this panel into taking another look at where we stand and what

we and Congress have to do in order to raise the baseline for cyber defense in this most important sector for the American economy and the American people.

Since we met on this topic a year ago, cybersecurity has become one of the most talked about challenges facing our Nation. Everyone, from the Secretary of Defense, who has said the next Pearl Harbor will be in cyberspace and is coming, to individual business leaders, have warned that the Nation as a whole faces a real threat, which Members of Congress need to work together to address.

There is very few issues I lose more sleep about than our cyber vulnerabilities, and when I speak to experts, they simply cause me to lose even more sleep. So, I appreciate the opportunity to reduce my sleep opportunities further today.

To Mr. Wilshusen of GAO; forgive me. Your written testimony said that when the GAO looked at the security of utilities, you concluded that, overall, they were focusing on regulatory compliance, more than a comprehensive security. I think that's a quote.

Can you elaborate about more—more on what about the existing approach, in fact, leads to standards becoming a ceiling, instead of a floor, for the level of cybersecurity, and what we could do in terms of standard-setting and internal partnerships that would strengthen an approach to comprehensive security, rather than mere compliance?

Mr. WILSHUSEN. I think that one of the dangers when organizations just focus on mere compliance is that they don't take an overarching view and develop a comprehensive program for assessing the risks and taking the appropriate steps to assure that they cost-effectively address those risks and mitigate them to an acceptable level.

I think it is still important, though, that you do have standards or minimum baselines of security controls that can be consistent across a wide group of similar organizations, perhaps, an industry, taking into account that each entity may have separate risks and controls in place to help mitigate those risks.

So, it is going to be important that each agency have an effective program for assessing the risk and then taking the appropriate steps to implement the appropriate controls to mitigate that. That would include, not only just assuring compliance with standards, but also taking other actions as determined necessary in the facts and circumstances.

Senator COONS. If there were to be standards that were negotiated—that were agreed to between industry and regulatory agencies, for an area like cyber, where the threat seems to be rapidly evolving, how would you update, routinely, those standards in a way that contributed to actual comprehensive security; how would you do that in a way that balances the economic impact, the cost, with promoting and achieving actual security?

Mr. WILSHUSEN. I think one way is, first off, with the standards. They need to be at a sufficiently high level to where they are flexible enough to allow for movement in the implementation of controls to address emerging threats and vulnerabilities that occur.

So, it really gets back to each agency or organization being able to determine what its risks are, and then take the appropriate con-

trols to mitigate them. At the same time, there needs to be a level of standards, such as the CIP standards, and probably have those evolve as going through the current process, to address new technologies and vulnerabilities that occur.

Senator COONS. Mr. Cauley, at NERC, you discussed that your biggest concern is a coordinated, actual physical and cyber attack, and that, perhaps, the combination of a terrorist attack in the physical world, followed by an attack that then takes down some critical infrastructure, such as the electric grid. I happen to agree that a cyber attack of this kind would be particularly dangerous. I would be interested in what sorts of public-private partnerships NERC is engaging in to prepare with or promote relationships with local and State responders to help mitigate those threats, and I would interested in where you hope to expand on those partnerships in the future.

Mr. CAULEY. Thank you, Senator.

We do work closely with State and local agencies, in terms of informing them what we are doing on the system and vulnerabilities. One of the most concerns that we have is any challenge that would do any permanent damage to equipment, so we work closely with law enforcement, FBI, in terms of securing the physical assets and investigating issues that come up with breaches and entry into substations and equipment, things like that.

So, I think there is an opportunity to continue working on that and expand that, in terms of types of scenarios—of attack scenarios we might see and run through drills and sort of understand our communications: who has responsibilities; how do we need to move personnel from point A to point B and move equipment; and those kinds of things. So, it's still an opportunity for us to continue working and developing.

Senator COONS. Broadly, how would you appraise the capabilities and the preparedness of State and local first responders, law enforcement, emergency management agencies, to deal with this sort of a combined attack or the emerging threats of cyber?

Mr. CAULEY. I think we certainly see a lot of experience and practice there that gives us some confidence—when we have major storms come through, trees are down, and roads are blocked. A lot of the capabilities that come into play during an attack on the grid would be similar to those kinds of things. So, in terms of securing people, moving people, securing supplies, those kinds of things, I am confident in the capability of the local and regional law enforcement and first responders.

Senator COONS. Thank you.

Mr. Snitchler, at the utility, the PUCO that you are now a chair of, I was heartened in your prepared testimony to hear that you addressed the importance, not only of public-private partnerships, but also Federal-State. I agree, since, in any of the scenarios we have been discussing, it is likely to be State and local responders who bear a lot of the responsibility, are likely to be first on scene, or likely to be leading the recovery effort.

Now, but on an issue like cyber that doesn't respect traditional, internal political boundaries or planning processes, how do you avoid wildly different standards that lead to uncertain and unreliable security situations or potentially to overinvestment in security

that puts too much of a burden, in terms of the operating costs of utilities?

Mr. SNITCHLER. Senator, I think you have hit on the—one of the primary issues that we often face at the Commission, which is, What is the appropriate cost and what can consumers and businesses afford to pay, in order to have the safe, reliable system that they have come to expect? Certainly, we try to approach that, being mindful—as I put in my written testimony—about protecting those critical assets, determining what those are, those are your diamonds, and giving them the appropriate level of protection, and then, having your—I hate to use the term "less valuable", but those that perhaps are, for example, a transformer on a street as opposed to a substation that is going to power several city blocks. You would treat those two differently. As a result, you would make your investments in how you would want those to be treated differently.

To move back to your first question, to address how do you—I think what you are asking is how do you not end up with a litany of ways for States to address these issues, when you have one issue that may be a national security issue or an attack on the country. I think you have to look at threats versus vulnerabilities. I think where you have a threat that has the ability to impact the entire country or a substantial region, then, certainly, there is a definite need for Federal involvement to be able to address those types of concerns.

Where you have got a more localized issue or a vulnerability that could be exploited, then, certainly, there is a role for State commissions—the utilities and the State government, in general—to deal with those concerns. I think it is a little bit fact-specific, depending on exactly what the scenario you are describing is; but, certainly, it is not a good idea to have 51 different ways for us to evaluate a problem. But, I think if you break that problem down into a threat versus vulnerability, and then categorize or prioritize, you can arrive at a more comprehensive way of evaluating those issues.

Senator COONS. Mr. Snitch, excuse me, Mr. McClelland, if I might, for a last question.

I just would be interested in your level of confidence that we have got the information sharing and the collaboration in place to allow State and local operators to distinguish between an unexpected outage, a rolling brownout, an equipment malfunction, and something that, in fact, has originated as a attack on the Nation, and then, to share relevant information in real time.

Mr. MCCLELLAND. Thank you, Senator.

There is certainly room for improvement. I think the important aspect is that the interconnections are very large; there are multiple States within the interconnections. Because it is a network, and a tightly integrated network, the actions or inaction of any particular player can have a substantial impact on the rest of the interconnection.

So, going back to your prior question, I think it is important that the entities communicate, that minimum standards be put into place. A minimum in security is a tricky business.

Now, you mentioned before about, you know, sort of, what are the costs economically to put the standards in place or to put these protocols in place. But the world moves on, and it is a very small

place. What we are seeing is, you know, folks from around the world having access—or potential access to SCADA systems. You can no longer live in isolation.

So, the question would be, What are the adequate security provisions that an entity must have to protect its business, and then, how do those practices compare with other practices? Are we sharing lessons learned? Are we sharing relevant intelligence? Is it actionable intelligence, so that folks can see what is happening, they can learn from their neighbor, and they can put the security in place, because the threats are moving at lightning speed?

So, as with you, it does keep us up at night. It is probably the most significant thing that we deal with. It actually has a potential to become much worse, because, as we add equipment that was previously dumb equipment and make it smart equipment, and give it two-way communication, and then give it the ability to speak with the largest generators on the system or to have a nexus to the largest generators on the equipment, then we have introduced a vulnerability. It would be like on-line banking, without cybersecurity. You really don't want to go there.

So, I think we are at a point now with the grid and the changing grid and the cyber connectivity, where no one can live in isolation. If there is connectivity, there is two-way communication; there has to be some sort of minimum protocols and there needs to be sufficient information sharing so that everyone is able to move ahead with a threat.

Senator COONS. Thank you.

Thank you, Mr. Chairman. Thank you, to the panel.

The CHAIRMAN. Senator Murkowski, do you have additional questions?

Senator MURKOWSKI. I am done, Mr. Chairman. Thank you, though.

The CHAIRMAN. Senator Udall, did you have additional questions?

Senator UDALL. Mr. Chairman, thank you for asking. If I might. I think much of this could be done for the record, but I wanted to ask Mr. Cauley what more can we at the Federal level do to recruit, train, and motivate young people to operate and defend our critical infrastructure, like the electric grid?

Mr. CAULEY. Senator, you know, I think by its—by the very attention and focus that we are putting on this, I think we are creating sort of an attractive arena to go into, and I think, you know, we are seeing that in some of the schools, as well.

But I think, ultimately, one of the other panelists mentioned recruiting military and people from Government. I think we have to recognize that the—sort of, the center of universe intelligence and security state-of-the-art is in the Government and in the military, and to the extent that it is not just the hiring of the people, but to do training and development programs and cooperative programs.

You know, I think information sharing and partnering between Government and industry are the two most important things we can do, and this is one area where we could do a lot more, in terms of Government sharing practices, the art and skill of security man-

agement. I think those kinds of things would be very useful for industry.

Senator UDALL. Mr. Snitchler, would you care to comment?

Mr. SNITCHLER. I would echo the comments from the other panelists.

Ohio is blessed to have the Wright-Patterson Air Force Base near Dayton, where we have a substantial military presence, of course. As a result, we have a large number of military folks who may be being discharged from the Service and who are able to move into those positions. But, as I previously noted, even with that, we still find that there is a shortage. These skilled professionals, and they are exactly that, are in short supply and in high demand, and companies are working very hard to try and find them.

I think one of the other panelists said, we typically end up raiding somebody else's cupboard to find someone to be able to fit that need. That has been my experience in talking with the utilities that we regulate is, that is often times where they find them. I think a more concerted effort to demonstrate that when you have completed your time of Service, if you want to move into the private sector, these are some of the avenues that you can pursue to have a long-term viable career, because these issues are not going to go away. The skills that they bring to the table make them immediately valuable to an organization, and I think that has tremendous value.

Senator UDALL. I would note, as I conclude, that I sit on the Armed Services Committee. We are having some of these same discussions with the Department of Defense, and they are also concerned about recruiting young cyber warriors, if you will. So, I think we have got to really focus on growing the pie, growing the sense that this is an important career path and work together, not only with the private sector and the public civilian sector, but also the Department of Defense.

I look forward to working with all of you in that regard.

Thanks, again, for your testimony. It is very helpful. Thanks.

The CHAIRMAN. Yes, thank you very much. I think it has been a useful hearing.

We will conclude the hearing with that. Thank you.

[Whereupon, at 11:30 a.m. the hearing was adjourned.]

APPENDIX

RESPONSES TO ADDITIONAL QUESTIONS

RESPONSE OF GERRY CAULEY TO QUESTION FROM SENATOR BINGAMAN

NERC registered entities are required under the currently effective NERC Critical Infrastructure Protection Standards (specifically Standard No. CIP-007-3, Requirement 4) to have a malicious software prevention program to protect critical assets supporting the electric grid. The standard specifically requires a NERC registered entity to "use anti-virus software and other malicious software ("malware") prevention tools" (emphasis added) to "detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware."

Due to the use of the term "and", the use of antivirus technology in a registered entity's malware prevention program appears to be a minimum requirement for[sic]. However, there are other technologies, such as whitelisting, that are superior to antivirus in the protection of these critical assets, but if antivirus is a minimum requirement, this standard appears to present a roadblock to registered entities using those newer, superior technologies in malware prevention.

Question 1. Please explain why registered entities should be at risk for noncompliance and penalties for using a malware prevention tool other than antivirus.

Answer. NERC has not processed violations for a case as described. The focus during NERC audits is on assessing how the entities are handling and mitigating the virus or cyber intrusion risk, and not strictly on having both methods. NERC's focus is on securing virus and malware no matter the tools.

Antivirus software is a well-understood protection method, but it is only one method to detect, prevent, deter, and mitigate the introduction, exposure and propagation of malware. CIP-007-3 R 4 allows for and does not prevent the use of additional and alternative methods. When used, antivirus technologies should be used in conjunction with other methods, such as whitelisting, file integrity checking, and computer and network behavior analysis.

Version 5 of the CIP Standards, currently being finalized, requires that entities "deploy method(s) to deter, detect, or prevent malicious code" and "mitigate the threat of identified malicious code," thus allowing flexibility by entities to implement the current anti-virus and/or anti-malware paradigm, implement whitelisting, or choose any other method so long as it meets the requirement to deter, detect, prevent, and mitigate threats posed by malicious code.

RESPONSES OF GERRY CAULEY TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. A few months ago the White House and the Department of Homeland Security staged a mock scenario for Senators featuring a cyber-attack on the grid in New York City. I was disappointed to learn that neither FERC nor NERC was invited to participate in this exercise, particularly since at no time during the briefing did the Administration ever inform members that the utility sector is already subject to mandatory cyber standards to protect the Bulk Power System (BPS). Why was FERC not invited to participate in the Administration's grid cyber-attack exercise? How does FERC interact with DHS in the cyber arena currently? Is DHS aware of the cybersecurity standards currently in place for the BPS?

Answer. NERC is unaware of the circumstances regarding why FERC was not invited to the DHS exercise; NERC is also unaware of FERC's interaction with DHS in the cyber arena. NERC was not invited to participate in the White House/DHS/Senate briefings and thus could not brief Members and staff on the action that Congress took in the Energy Policy Act of 2005 to address mandatory standards for cybersecurity for the BPS, and how that authority has been implemented.

DHS is aware that BPS owners and operators are subject to mandatory cybersecurity standards. In November 2011, NERC hosted the first-ever sector-specific distributed play security exercise, GridEx, which involved NERC's mandatory

cybersecurity standards. DHS personnel, including representatives from the Industrial Control Systems Cyber Emergency Response Team and the Office of Infrastructure Protection (including the Electricity Sub-sector Specialists), helped plan and execute GridEx, and participated in it.

In addition to awareness of NERC's standards, DHS is also aware of Alerts issued by NERC's Electric Sector Information Sharing Advisory Council (ES-ISAC). NERC and DHS agreed to have ES-ISAC employees staff the National Cybersecurity and Communications Integration Center, where the ES-ISAC has access to actionable intelligence, including classified contextual information available to appropriately cleared staff within the BPS community. NERC also provides anonymous situational awareness to DHS analysts to supplement the information DHS received from the intelligence community. This effort is crucial to improving the level of threat awareness within the industry and improving information sharing between government and industry.

As I mentioned in my testimony, NERC regularly interacts with DHS, partnering on many efforts, including several industry task forces working to improve security compliance and risk management. Specifically, DHS participates in the NERC Critical Infrastructure Protection Committee and the Electricity Sub-sector Coordinating Council. Additionally, NERC has partnered with DHS for each Cyber Storm exercise to educate federal partners on the BPS and industry's response to security threats.

Question 2. Many of the hearing witnesses noted that you simply cannot protect an entity from all potential cyber-attacks. Mr. Snitchler from the Ohio PUC cautions that while you can try to "gold-plate" or even "platinum-plate" a system, the critical infrastructure we're trying to protect will become too expensive to run. Instead, he suggests we prioritize, using a risk-based approach. Please comment on the issue of cybersecurity costs and the suitability of using a risk-based approach. Do you agree with Mr. Snitchler that we should be protecting "diamonds like diamonds" and "apples like apples"? Is the current FERC/NERC process for addressing cyber security vulnerabilities risk-based? If not, why not?

Answer. Since becoming President and CEO of NERC, I have prioritized incorporating a risk based approach to reliability. We are developing a strong portfolio of standards that address performance, risk containment, and competency. We are applying a defense-in-depth strategy that has proven successful in managing risks in critical sectors, such as nuclear as well as the aerospace industry. I am fully confident that this approach will work well in managing risks to the reliability of the BPS.

The NERC CIP Standards have always approached cybersecurity protection from a risk management basis. Version 4 of the CIP standards (approved by FERC earlier in 2012) established a set of impact-based "bright lines" to remove subjectivity from the process of determining what BPS components are deemed "critical." Under this paradigm, industry resources are focused on protecting the BPS components that have the most impact on reliable operations.

Version 5 of the CIP Standards will have a three-tier approach for the categorization of critical cyber assets. Under Version 5, industry resources will still be focused on protecting the components with the greatest potential to affect the BPS at the highest levels, while recognizing that the remaining components still contribute to reliable operations of the BPS, and thus must be appropriately protected.

Question 3. What are NERC's standard operating procedures once it receives credible threat intelligence that may affect the bulk electric system?

Answer. NERC's Electricity Sector Information Sharing and Analysis Center (ES-ISAC) has developed different Alerts to inform industry about emerging threats. Alerts are different from standards, and can be developed and issued very quickly, depending on the urgency of the situation.

Specifically, the ES-ISAC first reviews classified information with industry subject matter experts (SME) who hold the appropriate level of security clearances. As a part of the vetting process, a preliminary saturation and impact assessment determines the relative significance a compromise of the targeted technology would have on the BPS. Once NERC and the industry SMEs determine how a compromise may occur and the potential impact or significance of the compromise, ES-ISAC staff and industry SMEs develop a draft Alert that contains specific, actionable information that BPS entities can use to establish a defense against the threat or help remediate an already existing impact.

This draft Alert, which should be no more sensitive than "For Official Use Only," is then distributed to a larger technical team of BPS SMEs called the HYDRA Team. The HYDRA Team is a broad coalition of industry volunteers with specialties in fields such as transmission, generation, planning, operations, and cybersecurity of industrial control systems. Typically, the vendor of the targeted technology is also

involved in the Alert review, as is the vulnerability researcher who discovered the underlying vulnerability in the technology. Members of the technical staffs of the DOE, DHS, and the FERC are also members of the HYDRA Team. They receive draft Alerts and contribute to making final Alerts valuable for the industry.

The finalized Alert is then sent to both US (including FERC) and Canadian governmental authorities for their final review and comment. Thereafter, the Director of the ES-ISAC/Chief Cyber Security Officer approves the Alert for release to industry. When the Alert is distributed, it not only goes to NERC's Registered Entities, but also to other Electricity Sub-sector participants. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., Balancing Authorities, Planning Authorities, Generation Owners, etc.). Using this process, NERC has issued an alert in as little as 32 hours after receiving classified information about a threat.

Question 4. On Thursday, July 19, 2012, FERC approved an order that allows the ERO to fine the Southwestern Power Administration up to $19,500 for violating two cybersecurity-related reliability standards in July 2011. Please explain the nature of these cybersecurity violations. I understand that DOE believes the federal government is exempt from such penalties under the Federal Power Act. Please specify for the Committee why the federal government is, in fact, subject to compliance with the FERC/NERC reliability standards, including cybersecurity standards.

Answer. The Southwestern Power Administration (SWPA) violated NERC CIP-004-1 (Cyber Security—Personnel and Training) and CIP-007-1 (Cyber Security—Systems Security Management). CIP-004-1 sets out requirements for personnel that have authorized cyber access or authorized unescorted physical access to Critical Cyber Assets, including requirements related to personnel risk assessment, training, and security (including cyber security). CIP-007-1 sets out requirements related to security systems determined to be Critical Cyber Assets and other assets within an "Electronic Security Perimeter."

Agencies and instrumentalities of the federal government that are users, owners and operators of the bulk power system (such as the Tennessee Valley Authority and the Bonneville Power Administration) are subject to compliance with the FERC/NERC Reliability Standards, including cybersecurity standards. DOE has recognized that such entities are subject to the Reliability Standards, but it has taken the position that neither FERC nor NERC may impose financial penalties on those entities for violation of the standards.

By way of background, Section 215(c) of the Federal Power Act (FPA), 16 U.S.C. § 824o(c), authorizes FERC to certify and oversee an electric reliability organization (ERO) responsible for developing and enforcing mandatory Reliability Standards that are applicable to all users, owners and operators of the Bulk-Power System (BPS). FERC certified NERC as the ERO in 2006,[1] and has since approved over one hundred national Reliability Standards as mandatory and enforceable, pursuant to FPA Section 215(d).

FPA Section 215(b) (1), "Jurisdiction and applicability," describes FERC's reliability jurisdiction as follows:

> The Commission shall have jurisdiction . . . over . . . all users, owners and operators of the bulk-power system, including but not limited to the entities described in section 201(f) . . . for purposes of approving reliability standards established under this section and enforcing compliance with [FPA Section 215]. All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section.

Because they are described in FPA Section 201(f), agencies or instrumentalities of the United States are expressly included within the term "users, owners, and operators of the bulk-power system" in Section 215 and made subject to FERC's jurisdiction to both approve and enforce reliability standards. The requirement in FPA Section 215(b)(1) that all users, owners and operators of the bulk-power system must comply with reliability standards that take effect under Section 215 thus applies to Federal entities.

In orders issued since 2009, FERC has held consistently that a federal entity that uses, owns or operates the Bulk-Power System must comply with mandatory Reli-

[1] North American Electric Reliability Corp., 116 FERC § 61,062, order on reh'g and compliance, 117 FERC § 61,126 (2006), order on compliance, 118 FERC § 61,190, order on reh'g 119 FERC § 61,046 (2007), aff'd sub nom. Alcoa Inc. v. FERC, 564 F.3d 1342 (D.C. Cir. 2009).

ability Standards.[2] Most recently, in its July 19, 2012 order, FERC found that Section 215 explicitly conveys authority to assess a monetary penalty against a federal entity that is a user, owner, or operator of the Bulk-Power System for violations of a mandatory Reliability Standard.[3] FERC rejected arguments that the grant of enforcement authority under FPA Section 215 is limited by the scope of the Commission's general civil penalty authority over federal entities, as set out in FPA Section 316A, and instead found that the separate grant of penalty authority over federal entities under FPA Section 215 is "explicit and unambiguous." FERC found that this penalty authority under FPA Section 215(e) applies to both the ERO and the Commission.

RESPONSE OF GERRY CAULEY TO QUESTION FROM SENATOR BARRASSO

Question 1. In your testimony, you encourage Congress to "facilitate information sharing between the public and private sector." You recommend "making more clearances available to industry, identifying alternative methods to communicate classified information to our Canadian partners, and encouraging increased information sharing by US Government departments and agencies with asset-owners." Would you please expand upon the steps Congress should take to facilitate information sharing between the Federal government and industry?

Answer. The most important action that can be taken to address cybersecurity is improving information sharing. Improved information sharing depends on a fundamental understanding by government that the private sector owners and operators of the BPS need to know as much as possible about a threat, as soon as possible, so that they can take the appropriate action. The owners and operators of the BPS know their systems and the consequences that actions taken in one part of the BPS may have for another part. They cannot merely be told that there is a threat; they must be provided with sufficient information about the threat so that proper mitigation measures can be developed. In NERC's experience, this has been difficult for government security professionals to understand. As I noted in the hearing, it took more than three years to get actionable information from the government on the Aurora vulnerability. Once that information became available in a form that NERC could share with industry, NERC issued an Alert to industry, and industry then began developing mitigation plans.

Any action Congress can take to make more secret-level clearances available to the Electricity Sub-sector would assist in information sharing efforts. Individuals from the Electricity Sub-sector should be able to access and analyze classified information and share it among other cleared partners. In addition, in the instance of a cyber attack, these individuals should be assured that they have access to local secure centers, such as fusion centers or local Federal Bureau of Investigation offices.

Continued support for NERC's existing cybersecurity efforts, including NERC standards and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the Electric Sector Coordinating Council and NERC's grid security exercise and conference, which provide forums for improving information concerning cybersecurity among the public and private sector, is appreciated. NERC's ES-ISAC is one of the most effective tools NERC has to inform industry about emerging cybersecurity threats through Alerts. As I mentioned in my testimony, the ES-ISAC partners with several industry and government organizations to not only share critical cyber information, but to also develop these Alerts.

Also, reflecting the international nature of the BPS, NERC is responsible for ensuring the reliability of the BPS within the US and Canada. Currently, NERC is unable to share sensitive information regarding cyber threats or vulnerabilities with our Canadian partners. We are aware that the government has mechanisms in place to facilitate government-to-government information sharing at classified levels. Further work needs to be done to facilitate information sharing with industry officials in Canada, as well.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. You testify that the majority of the Directives that FERC issued in Order No 706 have yet to be addressed. Could you describe some of the most important of them?

---

[2] North American Electric Reliability Corp., 129 FERC § 61,033 (2009) (2009 Jurisdictional Order), reh'g denied, 130 FERC § 61,002 (2010); North American Electric Reliability Corp., 133 FERC § 61,214 (2010), reh'g denied, 137 FERC § 61,044 (2011).

[3] North American Electric Reliability Corporation, 140 FERC § 61,048 (2012).

Answer. First, the Commission directed NERC to develop a process of external review and approval of critical asset lists in order to ensure that the proper assets were consistently covered by the CIP standards under a system that depends on the entities to self-designate their equipment. In Order No. 761, the Commission stated that the adoption of appropriate, bright line criteria for Critical Asset identification may obviate the need for an external review. However, as stated in that order, whether this development ultimately eliminates the need for an external review process as directed in Order No. 706 will depend on the discretion allowed to individual registered entities to self-identify and characterize assets or systems for critical infrastructure protection to support the nation's bulk-power system. It also will depend on whether the bright line criteria generally include adequate facilities. Second, Order No. 706 directed the ERO to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).

Question 2. Some have argued that FERC has the authority to order NERC to produce a fairly specific standard. Could you do so, and if you did what would be the process then?

Answer. The Commission can direct NERC to develop a reliability standard to address a specific reliability matter. However, the Commission cannot ensure that the content of the standard returned to it by NERC will adequately respond to the specific reliability matter as the Commission may not directly author or modify a reliability standard under section 215. Under section 215, reliability standards must be developed by the ERO through an open, inclusive, and public process. The NERC process is intended to develop consensus on both the need for, and the substance of, the proposed standard. Although inclusive, the process is relatively slow, open and unpredictable in its responsiveness to the Commission's directives.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. A few months ago the White House and the Department of Homeland Security staged a mock scenario for Senators featuring a cyber-attack on the grid in New York City. I was disappointed to learn that neither FERC nor NERC was invited to participate in this exercise, particularly since at no time during the briefing did the Administration ever inform members that the utility sector is already subject to mandatory cyber standards to protect the Bulk Power System (BPS). Why was FERC not invited to participate in the Administration's grid cyber-attack exercise? How does FERC interact with DHS in the cyber arena currently? Is DHS aware of the cybersecurity standards currently in place for the BPS?

Answer. I do not know why the Commission was not involved in this exercise. That question is best answered by those who organized the exercise.

With respect to the Commission's interaction with DHS, Commission staff works closely with the DHS both on an informal basis and through formalized processes such as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the Cyber Unified Coordination Group, and the National Protection and Programs Directorate at DHS. Commission staff meets monthly with the Nuclear Regulatory Commission (NRC), Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) at the Top Secret/ Sensitive Compartmented Information level to discuss events and threats. Meetings with ICS-CERT are also conducted as required to discuss imminent threats and events that could impact the security of the electric grid. The meetings take place so the ICS-CERT can provide guidance to entities on how to address these issues.

Question 2. Many of the hearing witnesses noted that you simply cannot protect an entity from all potential cyber-attacks. Mr. Snitchler from the Ohio PUC cautions that while you can try to "gold-plate" or even "platinum-plate" a system, the critical infrastructure we're trying to protect will become too expensive to run. Instead, he suggests we prioritize, using a risk-based approach. Please comment on the issue of cybersecurity costs and the suitability of using a risk-based approach. Do you agree with Mr. Snitchler that we should be protecting "diamonds like diamonds" and "apples like apples"? Is the current FERC/NERC process for addressing cyber security vulnerabilities-risk based? If not, why not?

Answer. In general, the use of a risk-based approach to identify assets that are critical to the operation of the Bulk Power System can be suitable. The cost of cyber protection must be considered against both the effectiveness of the measures and the impact that the facilities in-question can have on the reliability of the Bulk Power System. However the designation of "diamonds" does not just depend upon the size or expense of the equipment, but also depends upon the connectivity of the equipment, whether it can be compromised and, in turn, be used to compromise

other equipment that may alone or in aggregate successfully compromise the operation of the Bulk Power System or the customers it serves.

The currently applicable CIP standards include a risk-based methodology to determine which facilities are "critical assets and the associated critical cyber assets," and therefore are subject to the requirements of the CIP reliability standards. However these standards allow utilities significant discretion to determine which of their facilities fit that description. The recently-approved Version 4 CIP Reliability Standards, which will go into effect on April 1, 2014, replace this risk-based assessment with "bright line" criteria. Version 4 relies upon the affected entities to self-designate their "Critical Cyber Assets". Only facilities that are self-designated by the regulated entities as "Critical Cyber Assets" are covered under the CIP standards. In order to help guide their decisions, the CIP standards identify categories of "Critical Assets" as a starting point in the process. If the entities have any "Critical Assets" (i.e., such as generating stations at 1500 MW or above, reactive power supplies at 1000 MVAR or above, transmission facilities at 500 kV or above, etc.), they are then required to determine if they have any "Critical Cyber Assets" at these facilities and if they decide that they do, those facilities will fall under the CIP standards. Entities can only designate "Critical Cyber Assets" from the "Critical Asset" list.

In Order No. 761, the Commission supported the application of the tiered-approach in the National Institute of Standards and Technology (NIST) Framework. That framework would, among other things, (1) ensure that all Cyber Systems associated with the Bulk-Power System, based on their function and impact, receive some level of protection; (2) customize protection to the mission of the cyber systems subject to protection; and (3) apply a tiered approach to security controls that specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System. The Commission stated that incorporating these applicable features of the NIST Framework into the CIP Reliability Standards would be a positive step in improving cyber security for the Bulk-Power System. In addition to considering the NIST Framework, the Commission in Order No. 761 stated that the criteria adopted for the purpose of identifying Critical Cyber Assets should include a cyber asset's "connectivity" and its potential to compromise the reliable operation of the Bulk-Power System. Therefore, we expect Version 5 to address these issues. NERC, in its comments to the CIP Version 4 proceeding, stated that it is incorporating into the Version 5 CIP Reliability Standards the NIST risk-based approach.

Question 3. We hear a lot about the potential benefits from smart grid systems, including reduced rates and improved reliability. However, we're starting to hear more about an unintended consequence from smart grid systems—namely that the smart grid's reliance on IT systems and networks exposes the electric grid to cybersecurity vulnerabilities which could be exploited by attackers. In the 2007 energy bill, Congress directed NIST to develop smart grid interoperability standards that FERC would later adopt. I understand that while NIST has developed these standards, FERC has not yet taken action because of a lack of consensus on the standards.

a. The 2009 stimulus bill provided over $4 billion in smart grid funding before these NIST interoperability standards were even developed. In fact, the stimulus bill provided $10 million in funding for NIST to perform the standard development work. What cybersecurity protections were included in the smart grid assets purchased with stimulus money? Doesn't it cost more to implement security after the network is already up and running?

Answer. I do not know what cyber security protections were included in any assets purchased with the stimulus money, since this program was administered by the Department of Energy. Generally, it costs more and may be less effective to implement security after a network is installed.

b. GAO has previously suggested that FERC monitor industry compliance with NIST's voluntary smart grid standards. Has the Commission done so? If not, why not? What is FERC doing in the smart grid arena with regard to cybersecurity standards?

Answer. The Commission has not monitored compliance with NIST's voluntary smart grid standards. Much of the smart grid involves facilities used in local distribution, which are not under the Commission's Federal Power Act (FPA) jurisdiction. However, Commission staff attends and observes meetings of the NIST Cyber Security Working Group, Smart Grid Task Force, and participates in a collaborative with the National Association of Regulatory Utility Commissioners concerning the smart grid. Commission staff also regularly performs outreach to NIST and the

Smart Grid Interoperability Panel and is following the development of smart grid standards. Commission staff also monitors developments of the North American Synchrophasor Initiative (NASPI) relative to applicable cyber security standards. Lastly, pursuant to its FPA 215 responsibilities Commission staff attend and participate in the NERC standards development process—including the CIP standards. Commission staff offers guidance that can include information relevant to the smart grid.

Question 4. You testified that because FERC's Federal Power Act authority does not extend to local distribution facilities there may be some "significant facilities [that are] vulnerable to the threat of a cyber or physical attack." Mr. Snitchler's testimony included a snapshot of state actions, including those undertaken in New York, that demonstrate a proactive stance on cyber security. Are there particular cities or local facilities where FERC is concerned no action has been taken by your state counterparts to protect their distribution system from cyber incursions?

Answer. I cannot identify specific cities or local facilities where no action has been taken by the states but am aware of the types of risks which such facilities might be facing.

Question 5. Throughout your testimony you note your frustration with the time it takes for NERC and its stakeholder process to develop these cybersecurity standards. However, NERC filed its enhanced Critical Cyber Asset Identification Standard (CIP-002 version 4) with the Commission in February 2011 and it took FERC a full 14 months to approve that revision. Why is it taking so long for the Commission to act on such filings and what can the Commission do by way of improvement?

Answer. In general, the Commission could shorten the time to process the NERC filings using an Order versus a Notice of Proposed Rulemaking (NOPR). The NOPR process requires the Commission to propose Commission action on the standard. The Commission must then solicit comments on the NOPR and issue a Final Rule on the proposed standard. Although longer, the NOPR process allows for open communication between the Commission and the commenters including opportunities for meetings between Commission members and individual stakeholders and industry interest groups on the Commission's proposed dispositions. Because the Commission may not directly author or modify a reliability standard under section 215, the NOPR process is the most effective way to detail the Commission's concerns regarding a proposed reliability standard before issuing a final rule regarding that standard. In Order No. 693, the Commission stated that it anticipates that it will address most, if not all, new Reliability Standards proposed by NERC through the more open rulemaking process which has been strongly preferred by industry. Additionally, the CIP cyber security standards are extremely technical and it takes both the Commission time to appropriately analyze them and the industry time to prepare its comments to the Commission proposed rule. These procedures, which ensure the Commission has a sufficient record on which to act on the technical aspects of the cyber security standards, take time to implement.

Specifically with respect to the Version 4 standards, on February 10, 2011, NERC filed a petition seeking Commission approval of the Version 4 CIP Reliability Standards. On April 12, 2011, Commission staff issued a data request to NERC in order to receive supplemental information necessary to understand the filing because the filing lacked information necessary for the Commission to process them. On April 13, 2011, NERC requested an extension of time to respond to a portion of the Commission's April 12, 2011 data request. The Commission granted this request, and NERC provided the information on May 27, 2011 and June 30, 2011. The Commission issued the Notice of Proposed Rulemaking September 15, 2011 and allowed 60 days from publication in the Federal Register for the industry to comment, or November 21, 2011. The Commission then issued the final rule on April 19, 2012, 150 days later, after reviewing comments from 28 entities and reply comments from NERC.

Question 6. The electricity sector has told us that what it needs in the event of a cybersecurity emergency is timely, specific, and actionable information. Does FERC agree? What do the words "timely, specific and actionable" mean to FERC?

Answer. I agree with this statement. I believe that "timely, specific and actionable" means that, to prevent a significant risk of disruption to the grid, the information should allow mitigating action to be taken before a cyber security event. Because cyber events have the ability to compromise multiple systems simultaneously, both prevention and quick intervention are keys. Sufficient and accurate information about both the vulnerability and the targeted systems must be available to develop specific details regarding how to defend, mitigate, or eradicate a cyber attack as quickly as possible, which may require pre-emptive mandatory actions in order to be effective. Specific and actionable means that the information must be detailed

in a manner for the owner/operators to be able to quickly apply the mitigations to the equipment allowing for prevention or mitigation of a cyber attack.

Question 7. On Thursday, July 19, 2012, FERC approved an order that allows the ERO to fine the Southwestern Power Administration up to $19,500 for violating two cybersecurity-related reliability standards in July 2011. Please explain the nature of these cybersecurity violations. I understand that DOE believes the federal government is exempt from such penalties under the Federal Power Act. Please specify for the Committee why the federal government is, in fact, subject to compliance with the FERC/NERC reliability standards, including cybersecurity standards.

Answer. That order is subject to rehearing, so I cannot comment at this time on the issues presented in the proceeding. For your convenience, attached is the Commission's order in that proceeding.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR BARRASSO

In your testimony, you state that "[t]he Commission is committed to protecting the reliability of the nation's bulk electric system." However, I am concerned that the Commission, under Chairman Wellinghoff, has downplayed the cumulative impact of EPA's new and proposed regulations on electric reliability. On May 17, 2011, Senator Murkowski sent a letter to Chairman Wellinghoff inquiring about the impact of EPA's regulations on reliability. Commissioner Norris has testified that he had three conversations last year with Heather Zichal, Deputy Assistant to the President for Energy and Climate Change Policy, "regarding FERC staff's review of EPA regulations." Commissioner Norris testified that Ms. Zichal contacted him on two occasions—in late June or July of 2011—"for information on the timing of the FERC studies on the reliability impact of the pending EPA Rules and the timing of FERC responses to Sen. Murkowski's questions to the Commissioners." Notably, Chairman Wellinghoff and Commissioners Norris and LaFleur did not respond to Senator Murkowski until August 1, 2011—more than two months after receiving the Senator's letter. In their response, the Chairman and Commissioners Norris and LaFleur revealed that your staff had—after almost one year—completed only an "informal assessment" of the impact of EPA's regulations on reliability. Your staff's analysis found that as much as 41 GW of coal-fired generating capacity was "very likely" to retire, with another 40 GW "likely" to retire, on account of EPA's regulations. On September 14, 2011, Chairman Wellinghoff testified before the House Subcommittee on Energy and Power and characterized your staff's analysis as "back-of-the-envelope." However, your staff's analysis, as far as I can tell, is turning out to be a reasonably accurate prediction of the retirements. I am concerned that it took an inquiry from this Committee to bring your staff's analysis to light. I am also concerned about the timing of that analysis.

Question 1. Have you or any member of your staff had any direct or indirect contacts or exchanges, in person, by telephone, electronic mail, or otherwise (e.g., together with or in the company of the Chairman or any Commissioner(s)), with Ms. Zichal or anyone in the Executive Office of the President (EOP) about the potential impact of EPA's regulations on electric reliability or on any other subject (e.g., the "informal assessment" as Chairman Wellinghoff used the term in his correspondence with Senator Murkowski, or "FERC staff's review" or "FERC studies" as Commissioner Norris used the terms in his testimony)? If so, please list the dates the contacts or exchanges took place and provide the names and titles of the individuals involved in these contacts or exchanges.

Answer. To the best of my knowledge, neither I nor my staff has had any direct or indirect contacts with Ms. Zichal or anyone in the Executive Office of the President on these issues, except as noted in the Chairman's response to Senator Murkowski's May 17, 2011 letter.

Question 2. What was the purpose and the subject matter of the contact(s) or exchange(s) you have identified in question 1?

Question 3. Have you or any member of your staff advised or provided any information to the Chairman or any of the Commissioners in connection with any contact or exchange (to include, as in question 1 above, in person, by telephone, electronic mail, or otherwise) that the Chairman or any Commissioner may have had with Ms. Zichal or others in the EOP? If so, (a) what was the purpose and the subject matter of the advice or information you or your staff gave to the Chairman or Commissioner(s) in connection with contacts or exchanges with Ms. Zichal or others in the EOP; and (b) please list the dates the contacts or exchanges took place and provide the names and titles of the individuals involved in these contacts or exchanges.

Answer. No

RESPONSE OF TODD A. SNITCHLER TO QUESTION FROM SENATOR BINGAMAN

Question 1. Mr. Wilshusen has recommended that FERC coordinate with the states and other nonjurisdictional entities (such as Coops or munis) to evaluate the extent to which utilities are complying with voluntary standards and to develop strategies for addressing gaps in compliance. Does that sound like a recommendation that you would welcome? Would it work, given the splits in jurisdiction, differences in state laws and regulations and the fact that many entities are jurisdictional neither at the state or federal level?

Answer. Recognition must be given that voluntary standards are, indeed, voluntary. By requiring utilities to develop strategies for addressing "gaps in compliance", these "voluntary" standards then become ones which are mandatory. I do not believe we are all (FERC, states, utilities) in agreement with respect to mandatory standards or which standards, if any, ought to be mandatory. However, I believe that there could be benefits to having increased coordination between the states, non-jurisdictional entities, jurisdictional utilities, and the federal government in addition to the existing FPA §215 process. A collective meeting of the parties would be useful in sorting out and resolving these issues.

RESPONSE OF TODD A. SNITCHLER TO QUESTION FROM SENATOR MURKOWSKI

Question 1. You note that the Ohio PUC has worked closely with the Wright Patterson Air Force Base. What can you tell us about your state's efforts in working with the military?

Answer. The Public Utilities Commission of Ohio has met with Wright Patterson Air Force Base (WPAFB) representatives on a variety of topics and issues over the years. Our staff addressed WPAFB representatives on energy assurance issues back in 2009. At that time, the PUCO encouraged WPAFB personnel to engage in meaningful discussions with their local electric utility regarding the specific needs and concerns for base operations, enhanced reliability requirements, and mitigating threats to these enhanced reliability requirements (including generation/supply, distribution/delivery, and system security—physical as well as cyber). Also at that time, the PUCO offered to facilitate those discussions, but was assured that appropriate base personnel would work directly with the appropriate utility personnel on these issues. Subsequently, the PUCO extended an invitation to WPAFB representatives to participate in Ohio's Energy Assurance tabletop exercise conducted in June 2011; a major component of the event featured a cybersecurity panel discussion with representatives from: the U.S. Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) program; the Supervisory Special Agents for the Cyber Squads in the Cincinnati and Cleveland Divisions of the U.S. Federal Bureau of Investigation; a Cyber Security Advisor from the U.S. Department of Homeland Security's National Cyber Security Division; the two Protective Security Advisors from the U.S. Department of Homeland Security's Office of Infrastructure Protection which serve the State of Ohio; and Ohio's Homeland Security Advisor. Additionally, the PUCO met with representatives from the electric utility serving WPAFB as early as 2009 to discuss the utility's cybersecurity program and posture.

The PUCO also was instrumental in working with the U.S. Air Force at WPAFB to eliminate our nation's, and especially our military's, dependence on foreign oil. Research into synthetic fuel from domestic coal, shale, biomass, and other sources using the Fischer-Tropsch process in order to reduce our dependence on foreign oil and achieve greater price stability has resulted in the creation of the Assured Aerospace Fuels Research Facility (AAFRF). This lab was created to perform essential research and development of these coal-to liquid, biomass-to-liquid, and shale-to-liquid synthetic fuel technologies. It serves as an excellent research tool for professional researchers from government, academia, and industry as well as training grounds for creating skilled operators, technicians, and researchers for future commercial facilities.

RESPONSES OF TODD A. SNITCHLER TO QUESTIONS FROM SENATOR BARRASSO

Question 1. In your testimony, you state that "one-size solutions for cybersecurity may not be the most effective means to mitigate and reduce known vulnerabilities." Would you expand upon your comments for the Committee?

Answer. Broad-based principles regarding good cybersecurity practices may be more appropriate for utility applications. Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition Systems (SCADA) tend to be very specialized equipment monitoring and controlling extremely complex networks. What may be considered a best-practices approach for one control system may not function as a best-practices approach for a different control system. The existing differences in

approaching cybersecurity utilized by the utilities and also the RTOs actually has a positive effect in that an attack on one utility's system will not necessarily bring down all systems because each has its own method of ensuring their cybersecurity. By allowing disparate approaches to solving the cybersecurity issue, while establishing the broad based, best practices, we potentially strengthen defenses against attacks to the grid.

Question 2. In your testimony, you state that "smart grid [technology] fundamentally makes the electric system more secure." However, you also say that "this technology brings with it new vulnerabilities. . .which should be taken extremely seriously." Would you expand upon the vulnerabilities that smart grid technology brings to our electric grid?

Answer. The "Smart Grid" too often is defined as being synonymous with "smart meters" or advanced metering infrastructure (AMI). Other important portions of the Smart Grid often overlooked include synchrophasors, protective relays, reclosers, and substation automation, among others. These components improve fault-detection capabilities and enable self-healing of the electricity grid. Taken as a whole, these technologies do make the electric system more secure and more reliable. The additional vulnerabilities are introduced by converting previously one-directional flows of power and information to become bi-directional. As additional points of data collection and gathering are introduced, so, too, are there additional points where hackers or other non-native data sources may introduce false information feeds into the network in an attempt to cause disruptions or system actions undesirable to the system operators. Finally, each new potential access point creates a remote source of entry to the system. It is essential to security protocols that proper backstopping from those potential entry points ensure that remote access is denied and the system is able to lock out or compartmentalize the access points to ensure that access, if secured, can be isolated and prevent substantial harm to the system.

Question 3. In your testimony, you explain that state regulators and industry "are unable to provide the. . .protection necessary to help secure our nation's critical infrastructure if the relevant Federal agencies do not provide actionable information to address imminent threats." You go on to say that "asset owners who provide information about their systems to Federal agencies in the spirit of cooperation. . .never receive truly meaningful, actionable, timely information in return."

a. Do you know why the Federal government is not sharing this information with state regulators and industry?

Answer. An often-cited answer is lack of security clearances in order to share specific threat information with state regulators or industry. This is understandable for specific threat information. Present practice provides monthly or intermittent threat briefings to the electricity sector, yet such threat information is often too stale or so non-specific as to be un-actionable. Surely an opportunity exists to provide more timely or actionable information without disclosing classified information. Addressing this fundamental problem would be a tremendous help to state regulators and, I expect, to the electricity industry. For instance, in the case of the "Aurora" situation, the federal government and its regulators in essence told the electric utility sector, "we have a secret problem on our hands and we can't tell you what it is. . . .now go fix it." In this specific case, the government knew of a vulnerability (they created it in a lab), and wanted that vulnerability addressed yet would not or could not disclose that information at that time. There must be a way for the federal government to provide such actionable intelligence in a timely manner so that those that need to take action know what action to take before the vulnerability becomes a threat and a threat becomes a tragedy.

b. Do state regulators and industry lack the security clearances necessary to obtain this information?

Answer. A lack of security clearances by regulators and utilities often is cited as the primary impediment to sharing of information by the federal government. However, granting additional regulatory authority to FERC or another federal agency does nothing to change that fact. Therefore, it would appear that it might be worth some time devising a means for the federal government to share relevant, actionable, and timely information with state regulators and utilities without divulging the methods or sources by which that information has been obtained. Additionally, the federal agencies responsible for providing security clearances should establish a consultative process with those in the electricity sector (state government and industry) to identify to whom or to which positions within the industry and/or state government ought to be provided an opportunity to gain the necessary clearance and at what level. The agencies should then be instructed to establish a procedure to thoroughly review and process these requests. In order to secure timely transfer of

information, select members of state commissions and/or utilities should be considered for security approval and permitted access to information critical to maintenance and protection of the grid.

Question 4. In your testimony, you state that "our utilities can provide a 'gold-plated' or even a 'platinum-plated' system which is ultra-cyber secure." However, you go on to ask "how much more do we want a kilowatt hour of electricity to cost?" Would you discuss the potential impact of new cyber security investments on ratepayers?

Answer. It is difficult to assess a financial cost of cybersecurity investments imposed by a federal regulatory agency not yet granted the authority to order such investments. It also is difficult to ascertain what cybersecurity requirements might be imposed by such a scheme. Yet, nothing is too expensive for one who doesn't have to pay the bill.

My point is this: there are risks these businesses must manage everyday in running their utility systems. Cybersecurity is one more of those risks that must be managed. There is a definite role for the federal and state governments to assist these critical infrastructures in securing their networks. But, as stated above, a best-practices approach for one utility, when applied to another utility, may not have the same positive impact on that second utility's cybersecurity posture. In other words, what may be prudent and necessary cybersecurity infrastructure expenditures for a utility system in Washington, DC, which houses much of our federal government, may not be appropriate in Houston, Texas, which houses petroleum refining. And neither of the appropriate cybersecurity expenditures in those two instances may be prudent to a utility serving Pleasantville, Ohio. The opportunity exists for the federal and state governments to ensure appropriate cost recovery for necessary cybersecurity remediations or enhancements. Undoubtedly, these utility control systems must become more secure and resilient; but most beneficial would be federal guidance to the electricity sector and state regulatory bodies that would assist us in determining how to best direct scarce resources in the most cost-effective appropriate fashion to be directed against the most imminent threats and against the likely vulnerabilities to the electricity sector.

In the end, we cannot, and we should not, expend resources on every known vulnerability: it would just be too expensive. For instance, to use the analogy of physical security, we could place 24-hour manned guardhouses at the base of each major electric transmission tower in order to prevent the vulnerability of a terrorist bringing down the grid with the destruction of multiple towers in several key locations. However this would be a very expensive solution for a low probability vulnerability. We must address the cybersecurity threats and vulnerabilities just as we address the physical security threats and vulnerabilities to our nation's infrastructure.

Question 5. At what point do the costs and vulnerabilities associated with smart grid technology outweigh the value for ratepayers?

Answer. There is no simple answer to the question posed here. The experience of power outages brought on by storm activity is fundamentally no different than a cyber attack that may disable the grid. A cost-benefit analysis must be performed—either explicitly or implicitly—to ascertain if the costs associated with the risk are worth the benefit achieved by implementation of the grid.

The self-healing ability of the smart grid, shorter outage times and increased reliability are all substantial benefits as a result of the use of the smart grid. Further, in restructured markets customers have greater access to options to control their utility usage and control their costs, as well as the increasingly varied pricing options available are all dependent on the utilization of the smart grid tools.

GOVERNMENT ACCOUNTABILITY OFFICE,
Washington, DC, August 2, 2012.

Hon. JEFF BINGAMAN,
Chairman, Committee on Energy and Natural Resources, U.S. Senate.

Subject: Responses to Questions for the Record; Hearing on Status of Action Taken to Ensure that the Electric Grid Is Protected from Cyber Attacks

This letter responds to your July 26, 2012, request that we reply to additional questions arising from the Committee's July 17, 2012, hearing on the status of actions to protect the electricity grid from cyber attacks. At the hearing, we discussed (1) cyber threats facing cyber-reliant critical infrastructures, which include the electricity grid, and (2) actions taken and challenges remaining to secure the grid

against cyber attacks.[1] The enclosure provides our responses, which are primarily based on previously issued products that were performed in accordance with generally accepted government auditing standards.[2]

Should you or your office have any questions on the matters discussed in this letter, please contact me at (202) 512-6244 or wilshuseng@gao.gov or David C. Trimble, Director, Natural Resources and Environment, at (202) 512-3841 or trimbled@gao.gov.

Sincerely yours,

GREGORY C. WILSHUSEN,
Director, Information Security Issues.

[Enclosure.]

RESPONSES TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. You recommend that FERC develop an approach to coordinate with state regulators and entities that are not subject to state regulation to evaluate the extent to which utilities and manufacturers are following voluntary standards, and to develop strategies for addressing gaps in compliance with standards. What encourages you to believe that efforts like this could be successful?

Answer. Electricity industry regulation is fragmented, with oversight responsibility divided among various regulators at the federal, state, and local levels. Such regulatory fragmentation can make it difficult for individual regulators to develop an industry-wide understanding of whether utilities and manufacturers are following voluntary standards. This is due to the large number of regulators in the industry-the Federal Energy Regulatory Commission (FERC), electricity regulators in 50 states and the District of Columbia, and regulators of thousands of cooperative and municipal utilities-and their potentially limited visibility over parts of the grid outside their jurisdiction. This complex reality of electricity regulation led us to believe that a coordinated approach to monitoring whether utilities and manufacturers follow voluntary standards would be more successful than an approach in which one or more regulators attempted such an assessment on its own. We are encouraged by the fact that FERC has previously worked with state regulators and groups representing entities not subject to state regulation on a range of issues. For example, we reported that FERC and the state commissions had already begun initial collaboration on smart grid and demand-response issues,[3] and these and other entities have also collaborated on other topics, including issues related to Regional Transmission Organizations and electric reliability and environmental regulations.

Question 2. I think that you are primarily talking about the NIST smart grid standards that FERC did not adopt because they did not find sufficient consensus in the industry to do so. Do you believe that FERC has the authority to adopt those standards without such consensus?

Answer. Section 1305(d) of the Energy Independence and Security Act (EISA)[4] provides that any time after the National Institute of Standards and Technology's (NIST) work has led to sufficient consensus in FERC's judgment, FERC shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to ensure smart-grid functionality and interoperability. In July 2011, FERC declined to institute a rulemaking procedure to adopt initial smart grid standards identified as a part of the NIST efforts, finding that there was not sufficient consensus to do so. EISA does not give FERC authority to adopt the standards in the absence of a determination by FERC that sufficient consensus has been achieved.

As noted in our testimony statement, smart grid standards identified through the NIST-led process outlined under EISA are voluntary unless regulators use other authorities to indirectly compel utilities and manufacturers to follow them. In this regard, FERC's authority over the rates, terms, and conditions of transmission and wholesale sales in interstate commerce and its responsibility for reliability standards for the bulk-power system may be relevant. For instance, to the extent that

---

[1] GAO, Cybersecurity: Challenges in Securing the Electricity Grid, GAO-12-926T (Washington, D.C.: July 17, 2012).

[2] Including: GAO-12-926T; Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use, GAO-12-92 (Washington, D.C.: Dec. 9, 2011); 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); Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007); and Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks, GAO-08-526 (Washington, D.C.: May 21, 2008).

[3] GAO-11-117.

[4] EISA § 1305(d), Pub. L. No. 110-140, § 1305(d), 121 Stat. 1492, 1788 (Dec. 19, 2007).

smart grid interoperability and cybersecurity standards are deemed necessary by FERC to ensure the reliability of the bulk power system, these standards could be considered through reliability-based authority provided under the Federal Power Act.[5] Under this authority, the North American Electric Reliability Corporation (NERC) can develop standards to protect the reliability of the bulk power system, or be requested by FERC to do so. If approved, such standards would be considered mandatory and enforceable by both NERC and FERC. However, the FERC Chairman has described limitations on FERC's reliability jurisdiction in the context of securing smart grid systems.[6]

RESPONSES TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. Many of the hearing witnesses noted that you simply cannot protect an entity from all potential cyber-attacks. Mr. Snitchler from the Ohio PUC cautions that while you can try to "gold-plate" or even "platinum-plate" a system, the critical infrastructure we're trying to protect will become too expensive to run. Instead, he suggests we prioritize, using a risk-based approach. Please comment on the issue of cybersecurity costs and the suitability of using a risk-based approach. Do you agree with Mr. Snitchler that we should be protecting "diamonds like diamonds" and "apples like apples"?

Answer. We have reported on the importance of using a risk-based approach for securing critical infrastructures, including control systems.[7] Risk management has received widespread support within and outside government as a tool that can help set priorities on how to protect critical infrastructures.[8] Security controls identified through a risk management process should be cost-effective and reduce risk to an acceptable level. In making decisions about risks associated with the electricity grid, other sectors' reliance on electricity should be an important consideration.[9] Due to these interdependencies, the consequences of an attack on the electricity grid could cascade across many sectors, impacting our national economy and security and the health and well-being of citizens.

In relation to the need for risk-based approaches, we testified that, in May 2012, the Department of Energy released the Electricity Subsector Cybersecurity Risk Management Process.[10] The guideline is intended to ensure that cybersecurity risks for the electric grid are addressed at the organization, mission or business process, and information-system levels. We have not evaluated this guide.

Question 2. We hear a lot about the potential benefits from smart grid systems, including reduced rates and improved reliability. However, we're starting to hear more about an unintended consequence from smart grid systems-namely that the smart grid's reliance on IT systems and networks exposes the electric grid to cybersecurity vulnerabilities which could be exploited by attackers. In the 2007 energy bill, Congress directed NIST to develop smart grid interoperability standards that FERC would later adopt. I understand that while NIST has developed these standards, FERC has not yet taken action because of a lack of consensus on the standards.

The 2009 stimulus bill provided over $4 billion in smart grid funding before these NIST interoperability standards were even developed. In fact, the stimulus bill provided $10 million in funding for NIST to perform the standard development work. What cybersecurity protections were included in the smart grid assets purchased with stimulus money? Doesn't it cost more to implement security after the network is already up and running?

---

[5] See §215 of the Federal Power Act, 16 U.S.C. § 824o.

[6] Letters from the FERC Chairman to Chairman Inouye and Ranking Member Cochran and to Chairman Rogers and Ranking Member Dicks on actions taken in response to GAO-11-117 (Feb. 14, 2012).

[7] See GAO, Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

[8] Risk is the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

[9] Federal policy established 18 critical infrastructure sectors, including the energy sector, which has two subsectors for oil and gas and for electricity. Other sectors include: banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; 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.

[10] U.S. Department of Energy, Electricity Subsector Cybersecurity Risk Management Process, DOE/OE-0003 (Washington, D.C.: May 2012).

Answer. We have not conducted the work necessary to answer the question regarding what cybersecurity protections were included in the smart grid assets purchased with stimulus money. However, with respect to the Smart Grid Investment Grant program that received additional funds under the American Recovery and Reinvestment Act of 2009, the Department of Energy Inspector General found that three of the five cybersecurity plans (required to be submitted by grantees) that it reviewed were incomplete, and did not always sufficiently describe security controls and how they were implemented.[11] While this finding cannot be projected across all such grants, it indicates a risk that grantors and grantees were not adequately considering security prior to the issuance of grants.

Generally, implementing information security features after the technology is operating is more difficult and more costly than is designing and developing the technology with security in mind.

RESPONSES TO QUESTIONS FROM SENATOR BARRASSO

Question 1. The President's stimulus bill provided about $3.5 billion for the Smart Grid Investment Grant program. In January of this year, the Department of Energy's Inspector General issued a report about this program. The Inspector General stated that DOE "approved cyber security plans for Smart Grid projects even though some of the plans contained shortcomings." The Inspector General also stated that DOE "was so focused on quickly disbursing [stimulus] funds that it had not ensured [its] personnel received adequate grants management training." In the Department's rush to deploy smart grid technology, has it compromised the security of our nation's electric grid?

Answer. We have not examined the cybersecurity aspects of the smart grid technology deployed through DOE's Smart Grid Investment Grant program and thus cannot comment on its impact to the security of the nation's electric grid.

Question 2. Would you please estimate how much it will cost to secure the smart grid systems that have been deployed as a result of stimulus funding?

Answer. We have not conducted the work necessary to answer this question.

Question 3. Who is likely to bear the costs identified in question 2? Will it be asset-owners? Will it be ratepayers? Will it be Federal taxpayers?

Answer. As noted above, we have not conducted the work necessary to estimate how much it will cost to secure smart grid systems deployed as a result of stimulus funding. As noted in previous questions, some federal taxpayer money is being spent on smart grid systems under the Smart Grid Investment Grant Program. However, it is unlikely that federal taxpayers would be responsible for the costs associated with additional activities to secure these smart grid systems unless additional funds were designated by Congress for that purpose.

In general, however, smart grid investments-like other electricity investments made by utilities-may be paid for in one of a number of ways. The costs of investments in electricity systems may be passed on to ratepayers if they are approved by the relevant regulator according to that regulator's standards for rate recovery. In cases where an investment is not approved by the relevant regulator, the owners of the asset may have to bear the cost of the investment.

○

[11] U.S. Department of Energy, Office of the 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.: January 20, 2012).