RPTS DEAN

DCMN HOFSTAD

PROTECTING THE ELECTRIC GRID: H.R. 2165, THE "BULK POWER SYSTEM PROTECTION ACT OF 2009," AND H.R. 2195, "TO AMEND THE FEDERAL POWER ACT TO PROVIDE ADDITIONAL AUTHORITIES TO ADEQUATELY PROTECT THE CRITICAL ELECTRIC INFRASTRUCTURE AGAINST CYBER ATTACK, AND FOR OTHER PURPOSES"

TUESDAY, OCTOBER 27, 2009

House of Representatives,

Subcommittee on Energy and Environment,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 9:37 a.m., in Room 2322, Rayburn House Office Building, Hon. Edward J. Markey [chairman of the subcommittee] presiding.

Present: Representatives Markey, Inslee, Butterfield,

Matsui, McNerney, Dingell, Baldwin, Matheson, Barrow, Upton, Stearns, Shimkus, Blunt, Pitts, Walden, Sullivan, Burgess, Scalise, and Barton (ex officio).

Staff Present: Bruce Wolpe, Senior Advisor; John Jimison, Senior Counsel; Jeff Baran, Counsel; Caitlin Haberman, Special Assistant; Lindsay Vidal, Special Assistant; Earley Green, Chief Clerk; Mitchell Smiley, Special Assistant; Matt Eisenberg, Staff Assistant; Andrea Spring, Minority Professional Staff; Peter Spencer, Minority Professional Staff; Aaron Cutler, Minority Counsel; Amanda Mertens Campbell, Minority Counsel; and Garrett Golding, Minority Legislative Analyst.

Mr. Markey. Good morning. Welcome to the Subcommittee on Energy and Environment and to this very important hearing.

The Nation Academy of Engineering has called the North American electric grid the "supreme engineering achievement of the 20th century." The grid is one of our greatest strengths, but, if not properly protected, it could become one of our greatest weaknesses.

More than any other technology, the grid is the long pole in the tent of America's economy and national security. All of our Nation's critical systems -- financial services, health care, telecommunications, transportation, water, defense, law enforcement, and so on -- depend on the grid.

Remarkably, 99 percent of the electric energy used to power our military facilities, including critical strategic command assets, come from the commercially operated grid. Our dependence on the grid will only deepen as we move toward greater reliance on automation and information technology.

It has becoming increasingly clear in the last 2 years that the grid is vulnerable to cyber attacks and to other threats from terrorists, criminals, and hostile states. Over 2 years ago, the Department of Homeland Security revealed the so-called "Aurora vulnerability" through which hackers could use communications networks to physically destroy electric generators, transformers, and other critical assets.

We know that the cyber system controlling the grid and other critical infrastructure are continuously probed by outside parties. Just last week, the U.S.-China Commission reported on China's deep involvement in cyber espionage. In addition, new risks are coming to light, such as grid control systems vulnerability, to portable weapons that use high-powered radio frequency, or microwaves to destroy electronic equipment. Some of these vulnerabilities could worsen if we don't implement smart grid technologies in a smart way.

This past Thursday, I was joined by a number of other members of this subcommittee at a classified briefing on grid security. I assure you, the vulnerabilities of the grid are every bit as urgent as the weaknesses in transportation security that were so tragically revealed by the events of September 11th. A coordinated attack on the grid could literally shut down the U.S. economy, putting lives at risk and costing tens of billions of dollars. Moreover, unlike a storm knocking out power lines that can be replaced in a matter of days, an attack on the grid could result in damage requiring months or years to fix.

There is broad agreement that to meet these challenges we need new Federal authorities and mandates. The status quo for Federal regulation in this area, which relies exclusively on industry development or consensus reliability standards through the North American Electric Reliability Corporation, is inadequate.

That said, tough questions remain as to precisely what shape any new authorities and mandates should take. This morning we will consider two bills that address these issues: one sponsored by Mr. Barrow, which Chairman Waxman and I have cosponsored; and a second sponsored by Homeland Security Committee Chairman Bennie Thompson.

[The information follows:]

******** INSERT 1-1 ********

Mr. Markey. I commend Mr. Barrow and Chairman Thompson for their leadership on this critical issue.

I think it is fair to say that the Barrow bill, of which I am a cosponsor, would establish the minimum new authority that all parties, including the utility industry and State regulators, agree is necessary. However, many parties argue persuasively that we must go further in order to adequately address the threats before us. I have kept an open mind on these issues, and I urge the other members of this subcommittee to do likewise.

I am committed to working closely with Mr. Upton and Mr. Barton, along with Mr. Barrow and Chairman Waxman and all the other members of the committee, to move strong grid security legislation as soon as possible. This hearing represents an important first step in that direction.

I thank the witnesses for joining us. I look forward to your testimony.

And now I turn and recognize the ranking member of the committee, Mr. Upton.

Mr. Upton. Well, thank you, Mr. Chairman. And I do want to thank you for holding this very important hearing. We appreciate our witnesses joining us this morning, as well.

The House Homeland Security Committee has examined this issue, focusing on the vulnerability in electric generator control systems which could allow remote access, enabling a bad actor to

remotely destroy a generator. We have also begun to look at these issues here, including classified hearings with the Department of Defense and Homeland Security, FERC, and others just last week.

Today, we will seek additional answers, with a focus on the most productive way to ensure the security of our energy infrastructure. I know we can work together on bipartisan legislation to address this very, very serious issue.

It is my hope that legislation to protect our critical infrastructure will also include Alaska, Hawaii, and our territories. Currently, NERC does not cover those areas, and our critical national security assets, particularly in Alaska and Hawaii, are too important to ignore.

Domestic infrastructure should be protected for cybersecurity generally, in addition to physical and electromagnetic threats. Additionally, I don't think it is enough to just cover the bulk power system; we also must include the distribution system. It has become clear that the distribution system outages and vulnerabilities can lead to problems with the bulk power system, and critical defense facilities are connected at the distribution level.

There is no question that this legislation should be comprehensive. We should seek to fill as many security gaps as possible. The threats that we face are too serious and abundant to only address a small portion of our vulnerability. The stakes could not be higher.

And, as we know, security is not free. There will be a cost to protecting our critical energy and national defense infrastructure. Our legislation should provide a mechanism by which all generators, regardless of whether or not they are rate-regulated by a State PUC, are capable of covering the cost of investments that they are required to make in the name of protecting the national security of the U.S.

The security of our Nation's energy infrastructure from attack is one of the most important issues that our committee will address. It is not an issue that we can take lightly or cover in just one hearing.

Energy has certainly been one of the leading issues debated in Congress this year, rightfully so. Energy literally powers our economy. Even small price spikes and supply disruptions can wreak havoc on the economy. It is imperative that the security of our Nation's energy infrastructure gets the attention it deserves.

I yield back.

Mr. Markey. The gentleman's time has expired.

The Chair recognizes the gentleman from Michigan, chairman emeritus of our committee, Mr. Dingell.

Mr. Dingell. Mr. Chairman, thank you. I commend you for holding this hearing today. The reliability of this Nation's electricity grid in the face of its vulnerabilities to cybersecurity attacks is a matter of the utmost interest and concern.

Mr. Chairman, I would note that the White House has indicated that there will be a significant effort on the part of the administration to address the renewal of the grid. Therefore, this hearing comes at a very important time because, in addition to addressing the questions of efficiency of the grid, we can also see to it that questions relative to the safety and security of the grid are also addressed.

If there were a successful remote cyber attack on a plant's utility control systems, we could face something more serious than a brief brownout or blackout. The Idaho National Laboratory has shown how a hacker can remotely turn a large generator into a smoldering scrap pile in just a few moments. Known as the "Aurora vulnerability," this type of attack could destroy generating equipment and impair the generation and delivery of electricity across the entire area of North America for weeks or months, its consequences cascading on consumers, on our economy, on our health care system, and on our national defense assets, amongst other things.

These concerns are not just theoretical. It has been reported that China, Russia, and other nations have conducted cyber probes of the U.S. grid systems. Moreover, cyber attacks have actually been conducted against critical infrastructure in other countries.

In response to the Department of Homeland Security's worrying about Aurora vulnerability, the North American Electric

Reliability Corporation, NERC, issued an advisory in June 2007 which outlined immediate and longer-term mitigation measures for utilities. An FERC audit of 30 utilities found that, 2 years later, progress had been made but that very significant issues still remain.

As the Electricity Reliability Organization designated under Section 215 of the Energy Policy Act of 2005, NERC has developed reliability standards for critical infrastructure protection. However, there are significant gaps, given the nature of a national security threat. We need to extend Federal authority to take emergency actions as necessary to protect the grid. I look forward to building a bipartisan consensus on legislation which will ensure that the Federal Government has all the necessary powers to intervene when there are emergencies that threaten the Nation's electricity supply.

I also welcome our panel of witnesses. It is my hope that they can inform us on whether emergency power should extend beyond the bulk power system to utility systems in Alaska, Hawaii, Guam, and in other American possessions or areas.

These powers should also be able to reach critical distribution systems in places like the District of Columbia or New York City. We want to be sure that the legislation addresses threats to the electrical system and that the Federal Government is not improperly hobbled by legal and jurisdictional boundaries in the case of emergencies.

Thank you, Mr. Chairman.

Mr. Markey. Great. The gentleman's time has expired.

The Chair recognizes the gentleman from Illinois, Mr. Shimkus.

Mr. Shimkus. Thank you, Mr. Chairman.

I, too, concur that this is a very important meeting, and I appreciate you all coming to help us sort through this.

You know, I had recently retired, about a year ago, from the Army Reserves. I served 3 years actively in West Germany. And, throughout my years here, I have always followed up on comments about the electromagnetic pulse concern, whether from natural occurrences or ships or a nuclear burst.

And we have always talked about smart metering is like the Holy Grail of energy efficiency. I think some people would argue that we set ourselves more at risk on some of this if it is an intentional electromagnetic burst in the atmosphere because of the ability to fry out this smart metering in all these solid-state applications, and the recovery time would be much greater than if we kept it simple.

So that will be my focus to debate, to hear, to try to figure out what is good and how far should we go, but, again, being careful that we don't try to automate so much that we actually decrease our ability to have a quick recovery, whether there be an intentional electromagnetic pulse burst or something that will naturally occur that will cause us great harm.

It was interesting, I heard a story out of St. Louis. I live close to St. Louis, Missouri. The nuclear power plant in Missouri is still on dial-up for its communications, just dial-up communications. And one of the things that they mentioned was, well, they don't really want to be on broadband because they don't want cybersecurity issues, they don't want some other types of concerns.

So it will be interesting to follow -- again, this is all just basically over-the-radio broadcast news, so I look forward to following that up.

Thank you, Mr. Chairman. I yield back.

Mr. Markey. Great. The gentleman's time has expired.

The Chair recognizes the gentlelady from California, Ms. Matsui.

Ms. Matsui. Thank you, Mr. Chairman, and thank you for calling this hearing. I am very pleased to be here today and would just take a couple minutes so we can continue on to the distinguished witnesses.

I would like to thank today's panelists for joining us to discuss the security of our electric grid, with regard to the two pending pieces of legislation. In particular, I would like to welcome my friend and constituent, John DiStasio, general manager and CEO of Sacramento Municipal Utility District, otherwise known as SMUD, to today's hearing.

John has served SMUD most admirably for nearly 30 years. He

originally joined the utility as a buyer for the district's purchasing department. He was promoted to the utility's top post last year, after serving as the assistant general manager since 2000 and being awarded a number of customer service honors.

I look forward to hearing his views on ways in which we can legislatively address cybersecurity issues in relation to protecting our electric infrastructure.

Additionally, I look forward to hearing all of your expert opinions. The expertise you share here will be useful throughout the committee process and in considering these measures.

As we are aware, the world has become critically reliant on digital communications, making military targets, civilian infrastructure, particularly our electric grid, vulnerable to cyber attack. The electric grid is a significant part of our country's infrastructure. Failure to take preventative steps to ensure its protection significantly endangers our economy.

It is critical that we examine the existing regulatory authorities that respond to threats aimed at our power system. And we need to continually examine the expanding risk of cyber attacks and the implications for traditional methods of deterrence. This committee is well-positioned to examine this issue and has already suggested one manner in which to address it. Together, we can ensure that we have the tools and resources necessary to effectively defend our electric infrastructure.

I look forward to hearing from the panelists on the bills

before us today and working with the committee and stakeholders on these important matters. Once again, I thank you, Mr. Chairman, for highlighting this important topic. And I yield back the balance of my time.

Mr. Markey. The gentlelady's time has expired.

The Chair recognizes the gentleman from Florida, Mr. Stearns.

Mr. Stearns. Good morning. And thank you, Mr. Chairman, and thank the ranking member, Mr. Upton, for calling this really important hearing, which basically is addressing the vulnerability of the Nation's electrical grid to cyber attacks and the steps that are needed to be taken to protect this critical infrastructure.

It has become apparent, I think, to all that our electric grid is vulnerable to cyber attacks by terrorists and by other nations. Our Nation's infrastructure systems are heavily, obviously, reliant on computer-based systems that are used to monitor and control sensitive processes and physical functions. These systems were once mostly closed proprietary operations but are increasingly connecting to open networks, like corporate intranets and the Internet.

The transition towards widely used technologies and open connectivity exposes the control system to the ever-present cyber risks that exist in the information technology world in addition to control-system-specific tasks.

Driving such concerns are reports that malicious attacks are

rising on specialized computer control systems that open and shut valves on natural gas pipelines, throw circuit breakers on power lines, and make telecommunications and defense networks, nuclear power plants, and hydro dams do their jobs.

To address these vulnerabilities, the Institute for Human and Machine Cognition, which is part of the Florida Institute of Technology and partnership thereof -- Mr. Chairman, it is located in my hometown of Ocala, Florida -- is creating new processes for better defending supervisory control and data acquisition systems, SCADA, from attack. Such systems, known as SCADA, monitor and report on the functions of closed computerized networks that provide real-time data in the operation of these central facilities.

For example, SCADA networks could track something as simple as a climate control system in an office building or monitor the key workings of something as complex and expansive as a nuclear power plant. SCADA networks are also widely used to control the flow of oil and natural gas through pipelines, dams, and many non-energy-related processes such as water and sewer lines, telecommunication systems, and mass transit systems.

So, Mr. Chairman, I think this is a very good hearing, and I look forward to our witnesses.

Mr. Markey. Great. The gentleman's time has expired.

The Chair recognizes the gentleman from California, Mr. McNerney.

Mr. McNerney. Well, I want to thank you, Mr. Chairman, for calling this meeting on the critical issue that is in front of us and also a very fascinating issue.

I want to thank the witnesses. I have looked at your resumes, and I am very pleased with the caliber of information you are going to bring in front of us.

Mr. DiStasio, from my area in California, I appreciate your coming out here today.

It amazes me that we have a network, a physical network, of electrical system that serves our country that is vulnerable to cyber attack that can bring down large portions of our country. So the question is, what do we do about it? And we need to worry both about how to prevent attacks, how to make ourselves less vulnerable, and also how to plan for contingencies if attacks are successfully carried out, both cyber and physical attacks.

So these are big issues. The issue is complicated, but we look forward to getting some concrete ideas from you.

I want to thank Mr. Barrow for your leadership on this; Bennie Thompson, who is not here, for his leadership. This is what we need, this kind of forward-looking leadership.

So thank you all for coming, and I look forward to your testimony.

Mr. Markey. The gentleman's time has expired.

The gentlelady from Wisconsin, Ms. Baldwin, is recognized.

Ms. Baldwin. Thank you, Mr. Chairman, for holding this

important hearing on protecting the Nation's electric grid from cyber attacks and other threats.

The threat of someone with ill intent attacking and accessing the control systems of electric generators or other equipment presents a substantial concern that must be addressed. These cyber or other forms of attacks, perpetrated with the intent to disrupt services in the short term or wreak long-term havoc by damaging equipment, could have a significant impact not only on our national security but also our economic security. In fact, according to one estimate, if a third of the country lost power for 3 months, the economic price tag would be $700 billion.

The Idaho National Laboratory test, known as Aurora, which has been cited a couple of times already, demonstrated how an attacker could break into a control system and disrupt the grid. This test highlighted the seriousness of a potential threat to our infrastructure and the urgency with which Congress and our Nation's agencies must act to mitigate any consequences.

As we consider the two bills before us, we must remember that we have a responsibility to remain vigilant, to make sure that our agencies have the proper tools to protect against cyber attacks, and to ensure that industry is fully prepared to work in concert with government to prevent any disruptions.

I look forward to hearing from our witnesses today about how we can best address these reliability and security issues.

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

time.

Mr. Markey. The gentlelady's time has expired.

The gentleman from Georgia, the sponsor of this legislation, who I would like to congratulate for his excellent efforts in this area, is recognized for 2 minutes.

Mr. Barrow. Well, thank you, Mr. Chairman. And thank you for moving this legislation forward and for the opportunity to work together on this issue of critical importance to our homeland security.

I am a sponsor of H.R. 2165, the "Bulk Power System Protection Act of 2009," one of the subjects of today's hearing, because I am convinced that the threats to our critical energy infrastructure are every bit as real and every bit as dangerous as any threat we can imagine. I am pleased that this Congress and this committee have given this a high priority and will push forward to pass meaningful legislation.

I obviously think that my bill is on the right track, but I am open to new angles, incorporating new ideas into the mix. I encourage my colleagues to cosponsor H.R. 2165, and let's use it as a foundation for working together on these solutions.

The key to sustainable security is that government and industry identify and address evolving threats against our country together. As our society becomes more and more reliant on technological advances, we actually become more and more vulnerable to debilitating attacks. This hearing is an important

first step toward closing security gaps which threaten us. The time to act is now; the American people expect it, and our national security demands it.

I thank the witnesses for being here today, and I thank the chairman for the time. And I yield back the balance of my time.

Mr. Markey. I thank the gentleman for his work.

All time for opening statements has been completed.

Chairman Bennie Thompson, chairman of the Homeland Security and lead sponsor of H.R. 2195, one of the bills that we are considering today, has submitted a written statement for the record. I would like unanimous consent that that statement be entered into the record.

Without objection, so ordered.

[The prepared statement of Mr. Thompson follows:]

******** INSERT 1-2 ********

Mr. Markey. And all members can introduce their statements for that purpose.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Markey. I would also like to add that Chairwoman Yvette Clarke of the relevant committee on the Homeland Security Committee and Jim Langevin, who was the Chair last year, would also like to have permission to have space reserved in the record for their statements, as well. And I want to congratulate them on their excellent work on this issue.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Markey. I note that the gentleman from Pennsylvania, Mr. Pitts, has arrived; Mr. Scalise has arrived.

Would you like to be recognized, Mr. Scalise?

Mr. Scalise. No, thank you.

Mr. Markey. Then we will turn --

Mr. Pitts. I will submit it for the record, Mr. Chairman.

Mr. Markey. Then the gentleman from Pennsylvania's statement will be included in the record at the appropriate point.

[The prepared statement of Mr. Pitts follows:]

******** COMMITTEE INSERT ********

Mr. Markey. So we will turn to our first witness, Mr. Joseph McClelland, director of the Office of Electric Reliability at the Federal Energy Regulatory Commission. Mr. McClelland has led FERC's efforts to approve and enforce mandatory reliability standards for the electric grid.

We thank you for joining us today. Please begin.

STATEMENTS OF JOSEPH MCCLELLAND, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION; THE HON. PATRICIA HOFFMAN, PRINCIPAL DEPUTY ASSISTANT SECRETARY, OFFICE OF ELECTRICITY, U.S. DEPARTMENT OF ENERGY; THE HON. GARRY A. BROWN, CHAIRMAN, NEW YORK PUBLIC SERVICE COMMISSION; DAVID N. COOK, VICE PRESIDENT AND GENERAL COUNSEL, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION; JOHN DISTASIO, GENERAL MANAGER AND CEO, SACRAMENTO MUNICIPAL UTILITY DISTRICT

STATEMENT OF JOSEPH MCCLELLAND

Mr. McClelland. Mr. Chairman and members of the subcommittee, thank you for the privilege to appear before you today to discuss the security of the power grid.

My name is Joe McClelland, and I am the director of Office of Reliability for 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 Commission or any individual commissioner.

In the "Energy Policy Act of 2005," or EPACT 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 new Section 215 of the "Federal Power Act."

Under the new authority, FERC cannot author or modify cybersecurity standards but must select an industry self-regulatory organization, termed the Electric Reliability Organization, or ERO, to perform this task. The ERO develops and proposes cybersecurity standards or modifications for the Commission's review, which it can then either approve or remand. If the Commission approves a proposed cybersecurity standard, it applies to the users, owners, and operators of the 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 and work.

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, quote, "bulk power system," end quote, as defined in the "Federal Power Act," which excludes Alaska and Hawaii, transmission facilities, and certain large cities such as New York City, and distribution systems.

Pursuant to this duty, in January of 2008 FERC approved eight cybersecurity standards, known as the "Critical Infrastructure Protection Standards," or CIP standards, proposed by NERC while concurrently directing modifications to all of them. Although the existing CIP standards are approved, full implementation of these standards by all entities will not be mandatory until 2010.

The first of several batches of modifications responding to the Commission's directives was approved in September of 2009, although the Commission directed further modifications to the revised standards. It is not yet clear how long it will take for the CIP standards to be modified to eliminate some of the significant gaps in protection within them.

On a related note, as smart grid technology is added to the bulk power system, greater cybersecurity protections will be required, given that this technology provides more access points to attackers and can increase the grid's cyber vulnerabilities. The CIP standards will apply to some but not all smart grid applications.

Physical attacks against the power grid can cause equal or greater 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. And, in 2004 and again in 2008, the EMP Commission issued its reports.

Among the findings of 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 attacks, significant parts of the electric infrastructure could be, quote, "out of service for periods measured in months to a year or more," end quote.

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.

Regardless of whether an EMP event is manmade or occurs naturally, it can cause equal or even greater destruction than a cyber attack, and the Federal Government should have no less ability to protect against it.

In September of this year, FERC initiated a research project with the Oak Ridge National Laboratory to study the events of an EMP event on the United States and to identify mitigation measures to protect against it. DOE and DHS have joined in this study, and we expect to complete it within 6 months.

The standards development system utilized under the "Federal Power Act" 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 too slow, too independent, and too open to address threats to the power grid that endanger national security.

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, FERC should be permitted to take direct action before a cyber or physical national security incident has occurred. Second, FERC should be allowed to maintain the appropriate confidentiality of security-sensitive information. Third, the limitations on the term, quote, "bulk power system," end quote, should be considered, as FERC cannot act to protect attacks involving Alaska and Hawaii, as well as some transmission and all local distribution facilities in large-population areas. Finally, if Congress finds it appropriate, Congress should provide a mechanism allowing entities to recover costs that the utilities incur to mitigate vulnerabilities and threats.

Thank you for attention today, and I look forward to any questions that you may have.

[The prepared statement of Mr. McClelland follows:]

******** INSERT 1-3 ********

Mr. Markey. Great. Thank you, Mr. McClelland, very much.

And I will say to each one of you that you only have 5 minutes for your opening statement. And after I introduce you, you don't have to read that part of your statement again. You can get right to the meat of it, okay, because I will have done it.

Our next witness is Ms. Patricia Hoffman, principal deputy assistant secretary of the Office of Electricity at the U.S. Department of Energy. In this capacity, Ms. Hoffman provide leadership on a national level to modernize the electric grid and enhance the security and reliability of the energy infrastructure.

Thank you for joining us today. Whenever you are ready, please begin.

STATEMENT OF THE HON. PATRICIA HOFFMAN

Ms. Hoffman. Thank you, Chairman Markey and members of the subcommittee, for this opportunity to testify before you today on H.R. 2195 and 2165.

The energy sector's threat analysis encompasses natural events, criminal acts, and insider threats, as well as foreign and domestic terrorism. Because of the diversity of assets in the systems in the energy sector, a multitude of methodologies have been used to assess risks, vulnerabilities, and consequences.

Also, improving the resiliency of the Nation's electric power grid for the purpose of national security will come at a cost. As Congress considers legislation, we recognize there are limited resources. Therefore, we must prioritize our activities, continually assessing risk, the impact to the electric sector, and financial impacts.

Incident response and information sharing still remain foremost our concern. While the United States has had a good deal of experience with physical disruptions to the grid, such as the 2003 Northeast blackout and the hurricanes of 2005 and 2008, it does not have experience-based lessons learned from a cyber incident. While coordination and communication has improved between public and private organizations over the past several years, much more is needed to prevent and respond to an attack that could hamper the U.S. electric power grid.

The 2010 Energy and Water Appropriations Conference Report directs the Department of Energy to develop an independent national energy-sector cybersecurity organization to institute research; development and deployment priorities, including policies and protocols to ensure the effective deployment of tested and validated technology and software controls to protect the bulk power system; and the integration of smart technologies to enhance the security of the electric grid.

Congress assigned the National Institute of Standards and Technology, NIST, with the responsibility to coordinate the development of a framework and a roadmap for interoperability standards, including cybersecurity. The Department has been working closely with NIST and other agencies through this Smart Grid Task Force and the private sector. I am pleased to say significant progress has been made. NIST issued Release 1.0 of the "NIST Framework and Roadmap for Smart Grid Interoperability Standards," as well as Draft NIST Interagency Report 7628, "Smart Grid Cybersecurity Strategy and Requirements."

The Department recognizes the inherent weaknesses associated with driving system effectiveness and risk from a single worst-case scenario. A single worst-case scenario is possible but rarely exists and often exceeds the known and projected adversary capabilities. At the same time, focusing on the worst-case scenario may result in overlooking protection system elements needed to counter more probable, significant, and credible

threats. Consequently, the Department is looking at a more balanced methodology to effectively detect and deter threats.

The Department reviewed the various bills and conducted analysis to evaluate the effectiveness. We also have reviewed the existing cybersecurity standards and the relative effectiveness in addressing high-consequence risks in a rapidly changing threat environment.

The Department provides the committee the following technical comments.

The Federal Energy Regulatory Commission could be authorized to issue an emergency security directive to owners and operators of the bulk power system covering a specific period of time if the Secretary of Energy has determined that a power grid emergency exists.

A power grid emergency could be defined as a situation that poses a high risk to the bulk power system that must be addressed within 60 days without public disclosure. Determination of a power grid emergency in general would require the expertise of the Secretary of Energy, in consultation with the Secretary of Homeland Security, the Office of Attorney General, and the Director of National Intelligence.

In making a determination, the Secretary could consider: a known cyber vulnerability exists that may affect the bulk power system; a threat actor is determined to have known or suspected intent, requisite resources, and capabilities to carry out the

threat with a high likelihood; if exploited, the vulnerability would result in significance consequences, including damage to assets, infrastructure, loss of life, and psychological damage; the situation presents an imminent risk to the bulk power system.

Any directive should have performance objectives and metrics for mitigating the identified threat vulnerability and/or potential consequence. The directive may alternately be in the form of an alert that notify owners or operators of a potentially serious cyber situation. Specific methods for compliance could be left to the discretion of the provider of the bulk electric power, provided the security performance objectives are met.

Any directives should notify private-sector operators of the bulk power system of the nature of the risk, consistent with the proper handling of classified and restricted information, and direct operators to investigate, take appropriate and corrective action, and file report findings back to FERC within a specified time period; and, if required, direct owners and operators of the bulk power system through NERC to develop mitigations to test and validate such mitigations. The Department of Energy could provide technical support.

With this, I will conclude my testimony. I thank you for the opportunity for being here, and I look forward to any questions you have.

[The prepared statement of Ms. Hoffman follows:]

******** INSERT 1-4 ********

Mr. Markey. Thank you, Ms. Hoffman, very much.

Our next witness is Mr. Garry Brown. He is the chairman of the New York State Public Service Commission. Mr. Brown is testifying on behalf of the National Association of Regulatory Utility Commissioners that will henceforth in this committee be referred to as NARUC, which will completely confuse anyone watching on C-SPAN.

So this is your last notice, viewers. It is the National Association of Regulatory Utility Commissioners. So, all 50 States have them. They each decide, kind of, what the electricity and telephone rates are in your State.

Mr. Brown is going to speak for all of them in America. He has 30 years of experience in mastering the arcane language of regulatory law.

And you have 5 minutes, Mr. Brown.

STATEMENT OF GARRY A. BROWN

Mr. Brown. Good morning, Chairman Markey.

As you said, I am the Chair of Electricity Committee at NARUC.

State regulators take the reliability and security of the bulk power system very seriously. However, as technology changed, new risks and vulnerabilities have emerged. The transition to a smarter, digital, more efficient grid carries with it potential concerns.

Do you want me to talk through it?

Mr. Markey. You can continue through.

Mr. Brown. Thank you.

As Congress considerations legislation in this area, it should seek to build on existing --

Mr. Markey. When the bells ring, it tells us with two bells that there is a roll call -- this won't come off of your time -- three bells, that we have a quorum.

When it goes out to six bells and then it goes six bells and then six bells and six bells, you should start running very fast. But that hasn't occurred in my 33 years here. But I just want to notify you that, if it just keeps going through and ringing, that that is not a good thing. But, so far, our reliability counsel up here --

Mr. Shimkus. Mr. Chairman, it is worse when there is no

power, so you hear no bells.

Mr. Markey. So this is maybe the key hearing. Otherwise, we will be reliant upon the same system that my district relied upon in 1775, with Paul Revere riding through and knocking on people's doors and saying, "Get out your gun."

So, anyway, you have 4 minutes and 29 seconds to go, Mr. Brown.

Mr. Brown. Thank you.

As Congress considers legislation in this area, it should seek to build on existing Federal-State coordination that results in a framework where vulnerabilities to the system are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

Our first vulnerability focuses on business process systems -- e-mail, office equipment, databases, et cetera -- that are not unique to utilities but take on special significance given the utilities' economic importance.

A second vulnerability is more specific to utilities, and that is utility control systems. Supervisory control and data acquisition, or SCADA, systems are already inextricably part of our utility operations and have served to improve the efficiency and reliability of our system operations in every system throughout the country.

Regulatory commissions have begun to probe the cyber-preparedness of utility companies in the realm of smart grid. In concept, the smart grid has the potential to provide improvements in situational awareness, prevention, management, and restoration. In spite of introducing new vulnerabilities, smart grid fundamentally makes the electric system more secure. Still, this technology brings with it new vulnerabilities and new points of access to create intentional disruption, which should be taken extremely seriously.

In each of these areas, steps are being taken to manage risk. The regulated companies we oversee have, through the North American Electric Reliability Corporation, developed good cybersecurity standards. The question of how far that standard extends is not yet clear. NERC's cybersecurity standards are extensive and thorough. Over the past 2 years, electric utilities across the country have requested significant additional staffing and significant additional dollars for NERC's standard compliance activities in their transmission rate case filings at FERC.

The standards already in place are adequate for both physical and cybersecurity. Overextending the applicability of those standards to lower-voltage facilities raises the question how much more we are willing to pay for what may be a marginal increase in cybersecurity.

I would like to share three examples of commissions engaged to ensure companies are meeting their responsibilities.

Since 2005, the Pennsylvania Public Utility Commission has required all jurisdictional utilities to have a written cybersecurity plan to complement their emergency response, each of which are tested on an ongoing basis.

Another State taking action is Missouri. The commission requires all of its utilities to have in place reliability plans and, in May 2009, queried its utilities about steps taken or planned regarding cybersecurity as it relates to company operations. The contacts made highlighted NERC order number 706, which mandates that electric companies adhere to eight standards relative to cybersecurity.

Since 2003, the New York Commission's Office of Utility Security has carried out a regular program of oversight of both physical and cybersecurity practices and procedures of the regulated utility companies in the energy telecommunications and water sectors. Staff of this office is devoted full-time to security audit responsibilities.

Generally, we utilize the existing NERC CIP standards as benchmarks to form our own judgments about the quality of cybersecurity measures in place at the regulated utilities. Staff is adhering to a schedule that calls for visiting each regulated utility company four times a year to audit compliance with some portion of CIP standards, with the goal of measuring compliance with all of the standards at each of the companies over the course of the year.

We have the benefit in New York of a close and effective partnership with our State cybersecurity office. The New York Office of Cybersecurity and Critical Infrastructure Coordination directs efforts to maintain cybersecurity practices within State government agencies. We have established an excellent record for being a prompt and reliability source of information. I have personally been in consultation with CCIC and NERC to consider cyber threats and risks to the smart grid.

I want to get to Federal legislation quickly. NARUC believes Congress should build upon existing Federal-State coordination and result in an environment where vulnerabilities are identified, prioritized, and resolved in a timely fashion. Congress needs to distinguish between imminent threats, which require immediate action, and vulnerabilities, which can be resolved more deliberately.

First, a component of any legislation should be the ability for Federal departments and agencies to have information identifying priority vulnerabilities and imminent threats and how this information is communicated to the various electricity providers, State and Federal law enforcement, and State regulatory authorities.

In normal situations, the electric power industry can protect the reliability and security of the bulk power system without governmental intelligence information. However, in the limited circumstances --

Mr. Markey. If you can summarize, Mr. Brown, please.

Mr. Brown. Yes, I can.

In the limited circumstances when the industry does not need governmental intelligence information on a particular threat or vulnerability, it is critical that such information be timely.

NARUC believes H.R. 2165 takes the best approach to the issues that confront cybersecurity in our Nation's electric system. And we thank Representative Barrow, Chairman Waxman, and Chairman Markey for introducing this legislation. There is a need for Federal leadership on these complex cybersecurity issues.

This concludes my remarks, Mr. Chairman.

[The prepared statement of Mr. Brown follows:]

******** INSERT 1-5 ********

Mr. Markey. Thank you, Mr. Brown, very much.

Our next witness is Mr. David Cook. He is the vice president and general counsel of the North American Electric Reliability Council, or NERC. In this role, Mr. Cook helps to lead the development of mandatory and enforceable reliability standards for the electric grid.

Prior to joining NERC in 1999, Mr. Cook worked for 10 years as deputy general counsel of the Federal Energy Regulatory Commission.

So, again, just for our audience, Mr. Cook is speaking for NERC, which is the private sector. Mr. Brown is speaking for NARUC, which are the State regulators. And the first two witnesses speak for the Federal Government, and that would be the Department of Energy, which I think everyone knows, and the FERC, Federal Energy Regulatory Commission.

We have FERC and NERC, and it does get confusing to people, okay, but it is Federal Government, State government, and now the private sector.

Mr. Cook, whenever you are ready, please begin.

STATEMENT OF DAVID N. COOK

Mr. Cook. Thank you, Mr. Chairman and members of the subcommittee.

NERC's overall mission is to ensure the reliability of the bulk power system in North America. Cybersecurity is an important component of that mission. The challenges the grid faces from cybersecurity threats, however, are different from other reliability concerns.

Digital technology changes frequently, and novel potential threats can arise very quickly, requiring rapid and often confidential responses. Threats can arise virtually any time and anywhere across the vast array of communicating devices on the grid. Moreover, cybersecurity threats are more likely to be driven by intentional manipulation of devices rather than weather-related or operational events that regularly occur on the system.

All of these characteristics set cybersecurity apart from other reliability concerns. For these reasons, NERC believes that the U.S. Government needs additional emergency authority to address specific imminent cybersecurity threats.

As the international regulatory authority for the reliability of the bulk power system, NERC is responsible for developing reliability standards applicable to all users, owners, and

operators of the system. The standard-setting process brings together NERC and industry and security experts from the United States and Canada to develop standards that must apply to the international grid.

Developing long-term standards that apply to more than 1,800 diverse entities that own and operate the bulk power system is a complex undertaking. Standards must apply equally to companies with thousands of employees and those with only 20. Additionally, the standards must do no harm.

NERC recognizes that, while the standards in place today provide a sound starting point, they should be and are being improved. NERC is also working in a number of areas to make available the kinds of information that will help the industry better secure critical assets from advanced well-resourced threats and other known cybersecurity activity on an ongoing basis.

In its role as the electricity-sector information sharing and analysis center, NERC analyzes and disseminates threat information and warnings to the electricity industry in the form of voluntary advisories, recommendations to industry, and essential action notifications.

NERC's preparedness and awareness efforts are necessary but not sufficient to protect the system against imminent specific cybersecurity threats. The principal gap that NERC sees in the current law is that the Federal Government lacks sufficient authority to address an imminent and specific cybersecurity

threat. Both H.R. 2165 and H.R. 2195 address that gap.

NERC believes the authority to act in such emergencies should be assigned to a single Federal agency. The legislation should also assure coordination between the Federal agency with that authority and appropriate officials in Canada and Mexico. H.R. 2165 contains important provisions that require such consultation, while H.R. 2195 contains no specific provisions in this area.

The jurisdiction provided by H.R. 2195 would go beyond the scope of existing Section 215 to cover distribution system assets. 2165 would limit its scope to the existing Section 215.

While physical threats are also a concern, NERC believes addressing the present gap and authority to address specific imminent cybersecurity threats is the highest legislative priority at this time.

One of the greatest challenges the industry faces in dealing effectively with the threats we have been discussing is the limited amount of concrete technical information coming from government agencies. Much of the information about threats is classified or otherwise subject to restrictions on disclosure.

Without more specific information being appropriately made available to asset owners, they are unable to determine whether particular cybersecurity concerns exist on their systems or develop appropriate mitigation strategies. A mechanism, therefore, is needed to validate the existence of such threats and

ensure information is appropriately conveyed.

Over the past year, NERC has worked to facilitate this information sharing and stands ready to support further efforts in this area. Both H.R. 2165 and H.R. 2195 contain provisions to address this problem.

To conclude, NERC, the electric industry, and the governments of North America share a mutual goal of ensuring that threats to the reliability of the bulk power system, especially cybersecurity threats, are clearly understood and effectively mitigated. NERC fully supports legislative efforts to provide the Federal Government with emergency authority to address imminent cybersecurity threats as quickly as possible.

Moving forward, NERC is committed to complementing Federal authority to address cybersecurity challenges, regardless of the form that legislation may take.

Thank you.

[The prepared statement of Mr. Cook follows:]

******** INSERT 1-6 ********

Mr. Markey. Thank you, Mr. Cook, very much.

And our final witness is Mr. John DiStasio. He is general manager and CEO of the Sacramento Municipal Utility District, or SMUD; henceforth called "SMUD" for our hearing purposes.

So we will have SMUD, NERC, NARUC, DOE, and FERC. Good luck, C-SPAN viewers, in this hearing.

He will be discussing bulk power as it is differentiated from a distribution system and how we can coordinate.

So welcome, Mr. DiStasio. Whenever you are ready, please begin.

Mr. Markey. And you can see why we should legislate in this area. You can see how it could escape a lot of attention from Congress, in terms of the security of the system.

Welcome, Mr. DiStasio. Whenever you are ready, please begin.

STATEMENT OF JOHN DISTASIO

Mr. DiStasio. Thank you, Chairman Markey, members of the subcommittee. I appreciate the opportunity to explain how the electric industry is addressing cybersecurity challenges and to support narrowly targeted legislation to enhance those efforts.

SMUD supplies electricity to California's capital region. We serve a population of 1.4 million people. We operate 473 miles of transmission lines but nearly 10,000 miles of distribution lines. Our customers include the State of California, the county of Sacramento, companies such as Intel, and other customers critical to public welfare and our local economy.

SMUD is a member of the American Public Power Association, APPA, and the Large Public Power Council, LPPC. They are part of a larger coalition of electricity stakeholders that have been working together on cybersecurity issues for the last 2 years.

The industry coalition includes investors, cooperatively and publicly owned utilities, utility generators, independent generators, Canadian utilities, large industrial consumers, and State PUCs. We often have very different views on policy issues facing our industry, but on the issue of cybersecurity we have been working together to help develop NERC's reliability standards for critical infrastructure protection and, more recently, to identify areas where additional legislation may be needed.

APPA, LPPC, NARUC, the Canadian Electric Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the National Rural Electric Cooperative Association, and the Transmission Access Policy Study Group all support carefully crafted specific legislation to deal with the discrete issue of cybersecurity.

We understand the seriousness of this issue, and we know we need to deal with it. It is in the industry's best interest to protect against cyber attacks. When the lights go out for whatever reasons, we are the ones held responsible. If they do go out, we want to bring them back on as quickly as possible and to minimize potential risk to health, safety, and property and to minimize any adverse impacts to the public.

At the same time, our industry is facing additional regulatory requirements in a number of areas, which all translate to increased costs for our consumers. Therefore, we must use our dollars and workforce wisely to address cybersecurity threats and vulnerabilities that are most likely to occur and have the greatest potential impact.

We need close collaboration between government and industry participants, rather than finger-pointing. Therefore, any cybersecurity legislation Congress adopts should continue the strong industry partnership with government agencies in the United States and Canada.

RPTS JOHNSON

DCMN MAGMER

[10:33 p.m.]

Mr. DiStasio. The interconnected North American electric power industry and NERC work closely with the Department of Homeland Security, DOE, FERC, and Canadian authorities. New legislation should be built on this strong foundation.

We support continued participation in NERC's industry based and FERC-approved standards development process. NERC and the industry have committed significant resources to develop revised and new security standards. We have committed some of our scarcest resources, our subject matter experts in cybersecurity and system operations, to help develop second-generation draft standards.

And it should be limited to the realm of cybersecurity. Some would prefer to include new legislation, other national security threats as well as cyber threats. SMUD and the industry coalition believe that other government entities, both State and Federal, have more direct responsibilities for national security.

The electric utility industry addresses physical threats through communication with local, State, and Federal law enforcement agencies and through our own security measures. SMUD has established a strong and long-term partnership and communication with the FBI, Sacramento County Sheriff's Department, El Dorado County Sheriff's Department, and the

Sacramento Police Department.

SMUD and the industry coalition support H.R. 2165. This bill sets out a process for the Federal Government to interact with the industry in a cybersecurity emergency but does not disrupt the existing reliability regime set out in section 215.

Specifically, the bill provides narrowly targeted authority for FERC to issue emergency orders in response to imminent cybersecurity threat to the bulk power system, specific authority for FERC to issue orders that address the AURORA vulnerability, improved communication flows of timely and actionable information from government to industry, and enhanced responsibility for us to share critical energy infrastructure information, enhanced authority for the electric power industry to protect and keep critical energy infrastructure information confidential and nonpublic and be limited to the bulk power system.

With that, I will conclude my remarks, as time is out. Thank you.

[The prepared statement of Mr. DiStasio follows:]

******** INSERT 2-1 ********

Mr. Markey. Thank you, Mr. DiStasio, very much.

Before I recognize myself, just so everyone understands where we are going here, so we keep these definitions somewhat comprehensible for the audience, we are going to be talking about the bulk power system in the United States. And the Federal Power Act defines that to encompass the large-scale power plants and transmission facilities, but the Bulk Power Act specifically excludes distribution systems. Those are the local systems of lines that bring power from the large transmission facilities, that is, from the bulk power system out to our homes and out to our businesses. And it also specifically excludes the parts of the grid outside the continental United States, Alaska, Hawaii, and Guam. So just so you all understand what we are talking about here as we get into bulk power and distribution systems.

So the Chair will recognize himself; and I would like, Mr. Brown, for you to look at that question of the exclusion of the bulk power system from the distribution systems. Because it is my understanding that there is no clear dividing line dividing the control systems that serve the bulk power system and those that serve the distribution system. So how can we possibly limit the Federal authority to the bulk power system only when it is so interconnected to the distribution system and the fact that that does affect people's homes and businesses?

Mr. Brown. As State regulators, we are concerned with the

whole system from the top to the bottom, including the bulk power system and the distribution system. We have always had this dual jurisdictional aspect to our system whereby the Federal Energy Regulatory Commission oversees the bulk power system, the State regulators oversee the local distribution system. For a hundred years, we have worked together -- or since the Federal Power Act, I guess, 70 years we have worked together in maintaining the reliability.

Mr. Markey. Here is my question. Since Washington, D.C., is not under the bulk power system, since New York is not, since so much of our military is not, how can you separate them? Shouldn't it be integrated as a single authority here to make sure that there is one system put in place?

Mr. Brown. The NERC standards apply to all elements of the system from top to bottom. I think when you are talking about cybersecurity, we would welcome Federal leadership in establishing standards for cyber issues, but I think you need to separate --

Mr. Markey. The NERC standards only apply to the bulk power system. Would you want them extended over to distribution as well?

Mr. Brown. I don't think they need to be.

Mr. Markey. But aren't they intricately entwined with the local distribution system?

Mr. Brown. There is certainly the connection between the bulk power system and the distribution system.

Mr. Markey. Right. Shouldn't we then integrate it to ensure --

Mr. Brown. But that doesn't mean that having a centralized authority is necessarily going to be more effective in terms of the reliability of the local system.

I think you need to distinguish between the physical assets, which for a long time have been under the dual control, and the cybersecurity requirements. And, as I say, in cybersecurity requirements I don't think the States would have huge problems with the Federal Government setting standards that apply throughout the system from top to bottom.

Mr. Markey. Let me go to you, Mr. McClelland. What do you think?

Mr. McClelland. Anytime that there is two-way communication between equipment there is a chance to compromise that equipment from a cybersecurity perspective. Deployment of two-way communication devices at the distribution level creates a huge technical challenge to secure that equipment, secure those protocols, and protect the assets up and down the line.

Mr. Markey. Ms. Hoffman?

Ms. Hoffman. When we are looking at performance measures, if emergency authority was provided as you look at the legislation that was stated as 2195 and 2165, if it is framed as developing performance measures, these performance measures could be implemented either at the State level or at the Federal level. So

one could look at the performance measure, and the State utility commissions could consider that as part of their responsibility. So the leadership could be provided at the Federal level under the form of a performance measure.

Mr. Markey. Yeah. On an ongoing basis, you know, we just have to take note of the fact that when we did have that blackout several years ago, a problem in Ohio affected Canada and New York City.

Mr. Upton. And Michigan, too.

Mr. Markey. I was trying to create the upper point, but you are right, I should have stopped in the continental United States.

By the way, you mentioned Canada in terms of the coordination. Did you include Mexico as well? Are you coordinating with Mexico?

Mr. DiStasio. Mexico to a lesser extent.

Mr. Markey. But Mexico is in?

Mr. DiStasio. Yes.

Mr. Markey. And, Mr. Cook, it is my understanding that over 2 years after the AURORA vulnerability was identified, NERC still has not established standards that would address that vulnerability in an optimal way. Why is that? And how can we possibly argue that the NERC process is adequate, given this delay?

Mr. Cook. The standards are moving in a direction to address some of the vulnerabilities that the AURORA incident disclosed,

and we are in a constant process of upgrading those standards. And that is in the process.

Mr. Markey. So what is your timeline on completion?

Mr. Cook. The Commission has directed us to give them a timeline for completing the changes to the standards. They recently issued an order, and we are to give them that timeline by the end of this year. We are in the process of developing that timeline right now.

Mr. Markey. Are the standards that you are developing specific to AURORA or optimized to deal with AURORA?

Mr. Cook. They don't focus solely on AURORA. They are looking at a range of the threats that the system is dealing with.

Mr. Markey. Okay. I thank you.

The Chair's time has expired. The gentleman from Michigan is recognized for 5 minutes.

Mr. Upton. Thank you, Mr. Chairman.

Mr. McClelland, Mr. Brown said in his testimony that the CIP standards already in place are adequate for both physical and cybersecurity. Do you think is that accurate?

Mr. McClelland. No, the Commission directed an order 706. When we approved the eight standards, we directed modifications to every standard. Some are very substantive and significant. I mean, I could provide specific examples as to why they are not adequate, but they are not adequate yet. There are still significant gaps.

There is also a significant lag as far as compliance with the standards. Only the most experienced and largest entities that fall under bulk power system jurisdiction have to be compliant with the standards today, and only 12 requirements of the standards do they have to be required with. It is a phased-in implementation.

Mr. Upton. Ms. Hoffman, would you agree with that?

Ms. Hoffman. Yes.

Mr. Upton. Mr. McClelland, can you describe for us, the members here, as well as the audience, what an EMP attack would be? What are the dynamics of that?

Mr. McClelland. There are two sources of electromagnetic pulse. One source is naturally occurring. It is a solar magnetic activity that disturbs the Earth's atmosphere, magnetic fields, and ionosphere. It rolls them back, if you will. During that rollback time, the Earth's magnetic fields are disturbed. It collapses back on itself; and that produces ground currents, geomagnetically induced currents. Those currents travel through the earth; and everything that they hit on the bulk power system they wreak havoc on, particularly large bulk power system transformers. They will destroy those transformers within a matter of seconds if they haven't been mitigated against such an occurrence.

There is also --

Mr. Upton. No, go ahead.

Mr. McClelland. There is also manmade EMP, electromagnetic pulse attacks. Those generate three separate times of energy disbursement. One is termed an E1. It happens within a billionth of a second. It is a very high, very strong radio frequency type energy burst. The wires and the transmission wires and facilities act as antenna. They pick that burst up, and it destroys all control equipment.

Very shortly thereafter, there is an E2 effect, which is similar to lightning. Utilities are very well mitigated against lightning. However, after an E1 burst, it is really uncertain as to how much more devastation it would cause.

And then, finally, there is the E3 effect, which is the first effect I described that happens naturally, every so often.

Mr. Upton. And how difficult is it to build a manmade device that would emit these EMPs?

Mr. McClelland. It is not difficult. For a nation state, for a sponsored terrorist organization, it is not difficult. And it is getting easier all the time.

Mr. Upton. And can you tell us about what the cost might be?

Mr. McClelland. I don't have any information about cost. For a small -- if it is a radio frequency weapon, a small RFI platform, those are less than a hundred thousand dollars apiece. Those can be portable, and they can be directed -- you have to be pretty close to your target, but if you are close --

Mr. Upton. Pretty close, within a quarter mile, a hundred

yards?

Mr. McClelland. Within hundreds or thousands of feet, depending upon the quality of the weapon itself. It is certainly possible to put a small portable weapon in a vehicle-mounted platform and direct that at facilities.

Mr. Upton. And our bulk power distribution system, it would be pretty vulnerable to that type of attack, is that right?

Mr. McClelland. The Commission doesn't have any information as far as what folks have done or haven't done regarding EMP mitigation. We suspect there hasn't been a lot of activity there.

Mr. Upton. And, again, that is a physical attack, not a cyber attack.

Mr. McClelland. That is correct.

Mr. Upton. And, Mr. Brown, as you indicated, you believe that H.R. 2165 is the best approach. H.R. 2165 looks at only cybersecurity. As I understand it, it does very little for physical security. So if what your statement is on page 5, that CIP standards already in place are adequate for both physical and cybersecurity, how does that comport to an E1 or, obviously, E2 or E3 as it relates to the distribution of that power across not only New York but all 50 States?

And that is sort of the crux, as we look at the two different bills before us, H.R. 2165, which you said is the better bill, does not have physical security. It does not include Alaska, Hawaii, Guam, New York, or as it gets to, as the chairman said,

the distribution.

I just don't know if you have had access to classified reports, as some of us were able to participate last week. Mr. McClelland was part of that discussion that we had. But I just want to know what evidence you have as you indicate that the present standards are adequate.

Mr. Brown. Well, obviously, I don't have access. And that is one of the concerns that we have, is we don't necessarily have access to some of the newer threats that are emerging. All we can judge on is what we know and see.

There are a variety of threats to the electric system besides EMP. You can take out an electric system in a variety of different ways, and that is why we have been trying to work with NERC on the broad array of security requirements that are necessary to protect the system. And that is why I pointed out the difference between a threat and a vulnerability.

If there is an active threat out there, I think everybody needs to know it; and I don't think any of the legislation at this point kind of has a mechanism in place that if there is a threat that there is a way of sharing that threat with all of the State jurisdictional agencies, law enforcement agencies that are going to need to address that threat. I am not sure a single standard somewhere established in legislation is going to be able to solve that problem or a new threat won't arise.

Mr. Upton. Our time has expired.

I just ask one quick question of Mr. McClelland; and that is, as they see threats that come in, it is too late if they are imminent. We have to be prepared. And I would presume that is why we need legislation very quick. Correct?

Mr. McClelland. Right. Right. That is correct.

Mr. Upton. I know my time has expired.

Mr. Markey. The gentleman's time has expired.

The Chair recognizes the gentleman from California, Mr. McNerney.

Mr. McNerney. Thank you, Mr. Chairman.

Mr. McClelland, I want to thank you for hosting me when I visited FERC and alerting me to the AURORA vulnerability at that time.

You discussed in your written testimony the challenges posed by smart grid technology. In your opinion, are the local utilities aware of this vulnerability? And, if not, what can we do to enhance that lack of preparation?

Mr. McClelland. We have an expression inside the Commission that the utilities are out in the wild. What that means is that they haven't really been brought in and briefed about the level, the sophisticated level of threat that could occur with cyber vulnerabilities, with two-way communications. I think that is evidenced by some of the activity that happens at other Federal agencies, Department of Defense, and sophistication of the levels of defense that they employ versus a utility that may be not as

sophisticated in that regard.

Mr. McNerney. Thank you.

Mr. DiStasio --

Mr. Markey. Mr. DiStasio, he is not talking about a utility in Silicon Valley. So you shouldn't take that personally, but --

Mr. McNerney. You mentioned that utility sector experts are not necessarily cybersecurity experts and lack high-level security clearances. Is there a particular path forward to remedying that problem that you envision?

Mr. DiStasio. Well, because of the emerging technologies, I will say this has really evolved over time as the electric grid has become operated in a more digital way, more SCADA controls and so forth. There has been a greater integration of the physical operators of the system and the technologists, and we actually both participate through the NERC process but within our own utilities. And we use what is called a layered defense in depth process where we look at people and technology and operations, controls that address both physical and cyber segregation of our systems, protection of our systems, control of information, training, and access to the individuals. So that is actually under way in most utilities across the Nation. I will say the diversity of our systems leads us not to be able to necessarily have a one-size-fits-all way to resolve that issue.

Mr. McNerney. Thank you.

You know, it seems to me that the real question here is how

much additional authority is needed to approach this problem.

Thank you, Mr. Brown, for bringing up the distinction between immediate and imminent threat versus vulnerabilities. When you look at 2165 versus 2195, 2165 is a little bit more specific and a little bit more limited range, whereas 95 is not as specific but has a broad range. I would ask anyone now on the panel, is there a utility preference for those approaches? For which one of those approaches would be preferable?

Mr. DiStasio. I would like to respond to that.

From the industry perspective, 2165, as I said in my testimony, would be preferential, because I think it is very important to distinguish between vulnerabilities which need to be dealt with on a continuous improvement basis over time on a proactive and a preventative measure versus immediate and imminent threats or emergency issues that we need confidential information to be able to respond to quickly. And so we think that 2165 best addresses that differentiation.

Mr. McNerney. Any other responders on the panel to that question?

Mr. Brown. Just that, in 2005, the authorization for NERC, I think a lot of progress has been made along the way in trying to address the vulnerability question, trying to set standards for the vulnerability question.

I think what makes the threat issue is where we believe the focus might be best served for this legislation, is that there be

more -- an ability, a process established by Congress that will say, if there is an imminent threat, exactly what the process will be in terms of disseminating that information to State regulators, utilities on a confidential basis so that we can all address this together. I think that is the most important part of the legislation. That kind of reinventing what has already been done in 2005 and trying move it again may be a step backward instead of a step forward.

Mr. McNerney. My final question, if I have a little bit of time, Mr. Cook, I was involved in setting standards in my prior life; and it is kind of an interesting process to get people to agree on these things. So how is that working out? I mean, are your participants finding ways to agree on these things and then the broader utility network buying into those agreements? Is that what is happening?

Mr. Cook. As a general matter, that is right.

Mr. Markey. The gentleman's time has expired. The witness will please try to answer the question.

Mr. Cook. Thank you.

The industry has stepped up and is providing experts and is working through the process. As I mentioned earlier, it is a continuous process of improving these standards, and we are making that progress.

Mr. Markey. Thank you.

The gentleman's time has expired.

The Chair recognizes the gentleman from Texas, the ranking member of the full committee, Mr. Barton.

Mr. Barton. Thank you, Mr. Chairman.

I am sitting here thinking what a perk it is to have you chairing a hearing with FERC and NERC, while the terrorists are smirking and lurking around. It is somewhat of a Herculean effort on your part. We appreciate it.

Mr. Markey. Excellent. I will try to respond before the end of your comments.

Mr. Barton. You are going to have to work to beat that. Of course, I had 10 or 15 minutes to think about it.

Mr. Markey. I think we should give the gentleman his full 5 minutes and note the incredible --

Mr. Barton. I am going to work on SMUD, too. We will see if we can get something done that is not vulgar on that.

Anyway, I would ask Mr. McClelland and Mr. Cook -- or Dr. Cook -- to comment on the relationship between the bulk power system and the distribution system and if you feel that the Federal Government should preempt the States in looking at this issue with regard to the distribution system.

Mr. McClelland. I can start.

The bulk power system is generally defined as 100,000 volts or above. The legislation EPAC 2005 required the Commission to approve standards -- review and approved standards for the bulk power system. However, it is defined by the regions. And so a

region that chooses to redefine the bulk power system as, say, 2000,000 volts and above can exempt 60 or 70 percent of the transmission facilities within that region by redefining the term "bulk power system". So I think it is important to make the distinction that it is not just distribution that would be excluded under bulk power system. It may also be what is traditionally considered transmission facilities that serve major metropolitan areas that could be excluded by that definition.

Now, back to the term "distribution facilities". It does -- the legislation does exclude facilities used for the distribution of local energy, which would be the facilities that would capture, say, the meters on the homes, smart meters, and any cyber facilities where appliances within the homes that communicate to the meters that may communicate then back to the transmission systems. And from an oversight perspective, from a reliability standards perspective, it is extremely difficult to regulate that communication without that ability, without that jurisdiction.

Mr. Barton. Mr. Cook?

Mr. Cook. For us, it is a matter of priorities, that the consequences are most profound at the bulk system level. And that is where our focus has been, and that is where we believe the focus needs to be.

Mr. Barton. Would the witness from the Department of Energy want to comment on that?

Ms. Hoffman. Any leadership that FERC provides in developing

performance measures to protect the reliability of the bulk power system could be applicable to the distribution system if the State PUC regulators decide to choose and follow them.

Mr. Barton. Mr. Chairman, I am going to yield back. I think, to be really serious, this is a very serious hearing, and I am glad you are doing it. I would hope, though, that we could legislate at the Federal level without impinging too much on the local or the State level for distribution systems. I would be reluctant to be too bold in preempting the States. But I think this is an important issue, and I am very glad that you and Chairman Markey are addressing it in the way that you are addressing it.

And with that I yield back.

Mr. Markey. Thank you, Mr. Barton, as well. I thank you. You have drawn our attention to this issue in another way that, for better or worse, there is a quirk that NERC and FERC do not have --

Mr. Barton. I almost used quirk.

Mr. Markey. -- do not have that jurisdiction; and, as a result, some jerk could hurt the system. And we have to close that regulatory black hole here.

Mr. Barton. Great minds think alike, Mr. Chairman.

Mr. Markey. I am not sure other people are viewing us that way. But I thank the gentleman.

The Chair recognizes the gentlelady from Wisconsin.

Ms. Baldwin. Thank you, Mr. Chairman.

One very specific question and hopefully followed by a broad, open question.

In our briefing memo from committee staff, we have our attention pointed to physical vulnerabilities of the grid. And I am just going to read you an excerpt.

For example, large transformers, essential to the reliable operation of the grid, are manufactured outside of the United States; and replacement may require up to 2 years. A limited number of spare large transformers are available within the United States; and industry has developed a program, the Spare Transformer Equipment Program, or STEP, another acronym, providing for sharing of such assets in the event of a terrorist attack. Any policy recommendations of how we can -- and I will ask you, Ms. Hoffman, recommendations for how we could be more prepared in the event of an emergency?

Ms. Hoffman. You bring up a very, very important point that critical to the reliability of the bulk power system is the recovery of that system. So an important aspect of that is the focus on manufacturing and manufacturing capabilities in the United States. So as we look at developing protection mechanisms, we must recognize that some parts of the grid will go down. So another key aspect is how fast can we restore? And that is directly to your point, which is very important.

Ms. Baldwin. What is our domestic manufacturing capacity and

what are we doing to bolster it?

Ms. Hoffman. For large transformers, very limited. In fact, I think there is only one company that will be looking at large transformers.

Ms. Baldwin. Thank you.

On a much broader question for all of you is the issue of communication and information exchange. And we have had testimony from the State perspective, from the NERC perspective of the frustration being that much of this is classified and tightly held and needs to be communicated to actors with the ability to prepare and plan; and yet we have sensitivities with getting certain information out. We have been grappling with this as a committee on previous legislation relating to chemical plant security, with water treatment plant security, now in this arena.

I know it is a very broad question, but I would like to hear your perspectives on how we get the information that we are learning at the Department of Energy and FERC to the hands of the people who actually need to plan and help us prepare, while protecting that information carefully. And we haven't even talked about ISOs, but they are another level of all of this.

And if you wouldn't mind, just starting with Mr. McClelland and going through the panel, that would be helpful.

Mr. McClelland. One of the problems we had with the AURORA advisory, the advisory went out by NERC in June, and the Commission was asked to do follow-ups to determine how effective

the mitigations were put into place. We couldn't protect the information, or felt that we may not be able to protect it from a FOIA request, and so we ended up asking for industry volunteers and reviewed their plans one at a time without taking any information back to the Commission. This information transfer, the inability to protect the information severely impeded folks' ability, the entities' ability to implement mitigation strategies.

Now, we saw a whole gambit. I don't want to say that was the only reason. There were some folks that were very well mitigated. There was good old-fashioned American ingenuity that had been deployed, but there were other entities that did nothing, and additional information didn't appear as if it would have helped. So we have asked that any additional authority that be conveyed provide the ability for the Commission to protect that information.

Ms. Baldwin. Briefly, Ms. Hoffman.

Ms. Hoffman. Briefly, point one, clearances. I think there has to be a wider, greater distribution of appropriate levels of clearances across the electric sector. Two, we need to protect the information from FOIA requests in accordance to -- very similar to maybe what DHS does with their Critical Information Act.

Ms. Baldwin. Mr. Brown? Any comment on the communications issue?

Mr. Brown. We deal with confidential information at the

State level all the time in terms of information regarding the bulk power system. I think we are well prepared and positioned, if we get the information, to protect it and use it.

The electric systems run on contingencies all the time. That is how the electric system is run. It is always planning for the worst thing that could happen; and that, if it happens, the system will stay up because there is adequate backup. Obviously, the more information available about threats, the better that contingency system can work.

Ms. Baldwin. Mr. Cook.

Mr. Cook. We have been successful in the last year in arranging for cleared briefings for some CEOs to have access to some more of that information. More of that needs to happen.

I agree with Ms. Hoffman that the clearances program needs to be accelerated, and there needs to be a way that this information can get out to folks without them having to make it public. The State Open Records Acts sometimes get in the way of that, because anything that some State agencies get has to be made public then.

Ms. Baldwin. Mr. DiStasio.

Mr. DiStasio. I would agree with Mr. Cook. I think that is an important step for Congress to consider. Because, right now, without adequate clearance, the information we might get would be limited and not applicable to a pending emergency or vulnerability that we are the ones responsible for addressing. So we certainly support additional clearance levels to make sure that threats can

be dealt with in a timely manner and confidentially.

Mr. Markey. The gentlelady's time has expired.

The Chair recognizes the gentleman from Illinois.

Mr. Shimkus. Thank you, Mr. Chairman.

If you all would just, if you have got a piece of paper, scribble down solar storm, radio frequency, EMP, and then cyber. And then my first question -- there is two questions -- I would ask you to prioritize the threat as you see it in those four categories, and then I would ask you to prioritize costs of recovery.

And kind of following up on my opening statement about where our focus should be, I think sometimes we don't really know what is the biggest threat, what is the biggest cost recovery.

And so if I could start with Mr. McClelland and just go down the line, if you all could do that for me. And if you don't want to, you don't have to, but I mean, if you could, that would be helpful.

Mr. McClelland. That is a difficult question.

Mr. Markey. Who wants to be a millionaire? If you can rank them one, two, three, four, and then we can fill it in.

Mr. McClelland. Tough to do. Cyber I had as one; solar storms I have as two. And, in fact, solar storms could be one because they are inevitable. We are going to get another storm. We are going to get another 1921 event, which has been called a one-in-100-year storm. That is going to happen. And, if it does,

it will be devastating consequences.

RF weapons and EMP would be the next two on the list.

Mr. Shimkus. Was radio frequency third or EMP third?

Mr. McClelland. I put RF weapons third only because they are so affordable and easier to tote, and EMP weapons fourth.

Mr. Shimkus. Thank you. And I will come back to the costs.

Ms. Hoffman. I did cyber as one, RF as two, solar storms as three, and EMP as four.

Mr. Shimkus. Great.

Mr. Brown. I want to emphasize cyber as one. These people are much more of experts and able to judge the vulnerabilities. But we are about to introduce -- perhaps the President has already announced -- billions of dollars of new moneys to allow --

Mr. Shimkus. Let me stop you there, because I do have that. It is a Washington Post article today. President Obama plans to unveil Tuesday $3.4 billion in grants to smart meters, updated transformers, and other devices. Is that where you are headed?

Mr. Brown. Yes, exactly. And the point is there is going to be a whole new system of two-way communications introduced to the electricity industry that really --

Mr. Shimkus. Does that make that more secure or less secure?

Mr. Brown. It can be both. It should be more secure. More real-time information about the system should be good. But it introduces new vulnerabilities to the system, which if not protected is bad.

Mr. Shimkus. All right. I have limited time. So you talked about cyber, so cyber -- what is your priority?

Mr. Brown. Cybersecurity would be, far and away, number one. I was going to say two, three, and four I am not really that capable of assessing.

Mr. Shimkus. Okay. Great.

Mr. Cook?

Mr. Cook. I would put cyber at a very high number one, solar after that. And as between RF and EMP, I am not sure.

Mr. Shimkus. Great.

Sir.

Mr. DiStasio. I would also put cyber number one. And, frankly, I would like to consult with the industry. Because I put two, three, and four again --

Mr. Shimkus. Okay. Let me go back to cost of recovery, if any of you could do that based upon these attacks.

Mr. McClelland. EMP and RF weapons I would put as number one. And I would rate them the same because it is the same mitigation for either of those two. Cyber I would put as number two. That is highly dependent, though, on what the utility has or has not done. And solar I would put as number three as far as the least-cost alternative.

And I do want to add that in the original grouping I don't have these -- although I ranked them for you, I don't have them very far apart.

Mr. Shimkus. Yeah, thank you. And I am going to stop there because I am on limited time.

I want to highlight that on April 21st, 2009, a study by the National Academy of Scientists found the U.S. could suffer one to two trillion in damages as a result of EMP; and it would take four to 10 years to fully recover. By contrast, Hurricane Katrina inflicted $150 billion to $300 billion in damage. So this is my fear or concern.

I have a wind generating power plant that went down because of an Internet connection, and it went down for 10 or 15 days. Bespeaks to the greening of America and the reliability of electricity.

The other issue that I wanted to address, although we have kind of covered it, this also speaks of my opinion, everybody knows I am a supply guy here on this committee, more generation versus less. If we limit the ability for us to increase generation in America, we increase the ability to put ourselves at risk when any one, two, or three of these are targeted. So I would be in support of a position that says let's build more power plants, not less.

And thank you, Mr. Chairman, and I will yield my remaining time. Thank you, Mr. Chairman.

Mr. Markey. The gentleman's time has expired.

The Chair recognizes the gentleman from Georgia, the sponsor of the bill, Mr. Barrow.

Mr. Barrow. I thank the Chair.

The table has pretty much been set for the issues that we are going to be taking under deliberation in negotiations going forward on this. But one thing that hasn't been talked very much about, and it is an issue that is very much on the minds of the folks who are going to be tasked with following or implementing any policies that we are going to be authorizing the implementation of, and that is with the electrical industry, the generators and the distributors.

So I want to talk just briefly, at least kind of set the stage for those discussions by asking if any of you all can identify any issues of disparate treatment or disparate impact that might result from the kinds of rules that we are all talking about trying to create and authorize here? Can you foresee, looking down the road, that there might be any disparate impacts in terms of some of the mandates that might be forthcoming? Impacts that might be disparate in terms of whether or not you are a big guy, a big for-profit utility company as opposed to a little guy, an EMC, whether any regional impacts that you can see as a result of the mandates that we are contemplating here.

We all want to do the right thing, and I know the generators and distributors all want do the right thing. But I am sure that as there are staggering costs we are trying to avoid, there are going some costs we are going to incur along the way.

So the first thing I want to ask is, can anybody here on the

panel give us some idea as to the kinds of costs and especially issues of equity and fairness, disparate impacts that might result from any of the mandates we are talking about today?

Mr. Brown, I think you are sort of on the hot seat representing the utility commissioners of the country. Why don't you go first?

Mr. Brown. Sure.

I am not sure about disparate impacts, but I think you need to put this into a context. If there is a federally mandated cost that we have got to recover from our rate payers, it means perhaps we won't be able to do something else that we have been trying to do.

Mr. Barrow. An opportunity cost, in other words.

Mr. Brown. Right now, at the State level, we are collecting money for renewable portfolio standards. Over 30 States have that. Energy efficiency programs, infrastructure needs, new transmission. So there is a lot of pressures already on electricity rates.

Mr. Barrow. What kind of costs do you foresee? What kind of magnitude?

Mr. Brown. Billions of dollars on a State level, tens of billions of dollars on a national level. At the same time, customers that are over 60 days in arrears on their bills -- in New York is over $600 million is in arrears. That is up 25 percent from a year ago. So just the rates that we have today,

people are unable to be able to pay it.

So I guess my concern is the more mandates that we get requiring expenditures is going to mean dollars that we are not going to be able to collect to do other things that we really want to do maintaining the reliability, safety, and efficiency of the system.

Mr. Barrow. Mr. McClelland, Ms. Hoffman, do you all have any thoughts to suggest along these lines? What do you foresee?

Mr. McClelland. As far as disparate treatment, the generators that don't fall under tariffs before the Commission, any generators that have, say, cost-based contracts or contractual arrangements would not necessarily qualify for security upgrades for cybersecurity or for, say, EMP expenditures. So that would have to be addressed.

There may be -- and I won't speak to the particulars, but there may be utilities or entities under cost freezes. They may be under rate freezes within different States. And that treatment or security upgrade would have to be considered by the State commissions, especially if it was a security upgrade necessary for distribution systems, say, smart metering upgrades.

And as far as whether or not we incur the costs, I think the threat is here. The vulnerability is here, and the threat is here. This is a different world. There are entities that are intent -- they believe that the bulk power system in the United States, the electric grid, is a legitimate military target; and

they have set their sights on that system. And so whether or not -- the costs are just going to have to be incurred. We are going to have to address the issue.

Mr. Barrow. Any way you slice it, the costs of prevention are a whole lot smaller than the costs of inaction is what you are saying.

How about you, Mr. DiStasio.

Mr. DiStasio. I would just want to add, from the industry perspective, the actual NERC regime that was enacted in 2005, we have already added significant compliance resources and industry experts to that at a cost of a fair amount of money. And one of the reasons that we are actually supportive of the approach that you are taking to this is it does tend to appropriately focus this on emergency threats, which to me that represents a much smaller cost.

I think I mentioned the fact that we have 400 miles of transmission but 10,000 of distribution, which is not uncommon for many utility systems; and if you look at the expansion of taking it down to lower probability assets in the distribution system, it adds significant costs without certainty that that is going to have the same disruptive effect as the bulk power system.

Mr. Barrow. Thank you.

My time has expired. I would like Ms. Hoffman to feel welcome to respond, but my time has expired. Thank you, Mr. Chairman.

Mr. Markey. The gentleman's time has expired, but real quick.

Ms. Hoffman. Real quick the only comment I would add is one size reliability does not fit all. Defense Department, manufacturing industries require higher level of reliability than, say, residential customers or what they are more willing to accept. On-site generation, micro grids, UPS systems are alternatives to look at as we consider reliability.

Mr. Markey. Great. Are there others who wanted to say a word? No.

The gentleman's time has expired.

Mr. McClelland, do you want to say a word here?

Mr. McClelland. I had an opportunity.

Mr. Markey. Okay. Good. Great.

The Chair recognizes the gentleman from Texas, Mr. Burgess.

Dr. Burgess. Thank you, Mr. Chairman.

And, Chairman Brown, I was particularly intrigued by your comments, how much are we willing to pay for marginal increases in security? And obviously that is the fine balance that we have here today. And I don't know if I have a -- conceptually, if I have a good idea of the number of dollars that it would take to harden our grid against an electromagnetic pulse, either whether it is generated by natural occurrences, by a solar flare, or a legitimate military target, as was outlined by Mr. McClelland.

Can you give us some sense of the task ahead? If we were to

have a grid that was completely impervious to anything versus what is actually practical, what are the cost differentials that we are talking about?

Mr. Brown. We have infrastructure needs at State regulatory levels of billions of dollars just to maintain the existing aging system. The idea that you could make it impervious I think is tens of billions of dollars of investment. It is an entirely new and different way of doing the system.

Earlier, we talked about the bulk power --

Dr. Burgess. Can I stop you there?

Do we, in fact -- does the technology exist to do that if dollars were not an issue? Do we have the technical know-how to do that?

Mr. Brown. It is a matter of duplication. You can duplicate a lot of the system over and over and over again so that technically -- I will leave it to some of the experts whether it is completely impervious, but that is a lot of money.

And this is all a cost-benefit analysis. I think that is what regulators do all the time, is cost-benefit analysis. I could gold-plate the electric system in New York and make sure that we don't have as many outages, but the costs might be two to three times -- the rate payers, they would find it unaffordable to pay the rates that are out there.

It is always a balance between reliability and cost, and you can't just look at cost because you would have an unreliable

system. But you can't just look at liability, because you will have a gold-plated, expensive system. Tough balance.

Dr. Burgess. On balance, the legislation that is the subject of this hearing, do you think we are threading that needle appropriately with trying to balance those two ends?

Mr. Brown. One of the concerns I had about some of the legislation was it is reaching down all the way into the distribution system, which was the chairman's first question.

And I will note that, for example, the three major blackouts we have had in New York City, ranging from 1965 on, were all bulk power system disruptions, problems that the bulk power level got to the local level. It wasn't problems with the local system.

So spending a lot of money on the local system and then perhaps sacrificing some things being done on the bulk power system may not be a cost-effective way of meeting the concern. That is why we would like to see the focus on the bulk power system, and we think the work that began in 2005 with NERC is the appropriate way to be moving towards that goal.

Dr. Burgess. And yet I mean there are technologies available today that weren't available 5 or 10 years ago. And those technologies do, as I think you pointed out in your testimony, add increased vulnerabilities in different ways.

With this legislation, are we taking an appropriate over-the-horizon look at what may be available to electricity consumers in the future in providing them the protections? Or are

we looking at a situation where we may have to be back here in 5 or 10 years, 15 years and revisiting this entire issue? Do we have the appropriate eye on what is coming down the pike for the future?

Ms. Hoffman. In order to prevent that, I think we need to do a continual risk evaluation of what the new threats are and the new concerns are, as well as what the new technology is so that we can keep feeding and cycling through that loop so we stay ahead of the game.

Mr. Brown. And that is why I also emphasize cybersecurity. That is the new element that is coming into the system. The smart grid two-way communications, we really need to get that secure. I think that is the most important focus at this point in time.

Dr. Burgess. I just back home. There was an effort to go to smart meters, and then they turned out to not be in compliance with what we said they ought to have. And so you have got a company down there now that is asking its rate payers to pick up the millions of dollars for meters that aren't going to be able to be used. We do have to be careful how we implement these things, because we can end up costing people a lot of money for very little return.

And at the same time, as Mr. Shimkus points out, the far end of the scale is we may be asking for hundreds of billions of dollars of investment to protect us against trillions of dollars in loss and decades of recovery.

So thank you, Mr. Chairman. I will yield back.

Mr. Markey. Great. The gentleman's time has expired.

The Chair recognizes the gentleman from Utah, Mr. Matheson.

Mr. Matheson. Thank you, Mr. Chairman.

I have heard some different opinions about whether or not utilities receive specific actionable intelligence from the Federal Government regarding imminent cyber threats. And so I was wondering -- I would ask all the witnesses or anyone to respond -- what your thoughts are about this and do you think utilities should receive more clearances or more information?

Mr. DiStasio. I could address that from the industry perspective. To date, we have not received any notifications or specific actionable intelligence relative to imminent threats. We did have the information that has been discussed regarding AURORA. There were 30 utilities, as was mentioned, that worked on a voluntary basis to try to understand and mitigate that.

I do believe we do need additional clearance. Because while there are many reports out there that there are significant threats and while there have been briefings that suggest that these things are real and imminent, the utility industry to date has not been notified with any specificity in order to best mitigate those or prevent them. We do work through the NERC standards on a prospective basis, but we do think that additional confidential clearance and additional ability to get additional Federal authority to provide specific and actionable information

would be very helpful.

Mr. Matheson. Okay. Thanks. Yeah.

Mr. McClelland. I guess I want to be very clear right up front, the NERC standards are wholly inadequate to address threats to national security through the power grid. The NERC standards, on average, take 4 years to develop. Modifications, many different iterations. They are done in an open and inclusive forum. So not only is the reason for the standard published but also all the proposed mitigation strategies, and bad guys have access to the Web sites and can look at those proposed mitigations.

So the NERC standard -- the existing standards that are in place, the Commission has identified substantial security gaps in those standards, directed modifications, and are awaiting the NERC process to finish the modifications.

As far as information to utilities, yes, I agree utilities do need more specific information to be conveyed. But it is not just the information. In the AURORA advisory which was issued in June, there were very specific mitigations that were requested. An advisory is voluntary. There is no ability for any Federal agency to direct utilities to take action to protect their systems in the event of a threat or a vulnerability. So the advisory was voluntary, and we saw compliance that wasn't great. We didn't see great compliance even with entities that understood the issue. However, everyone could have benefited by additional information.

Mr. Cook. Just to answer your question, the feedback we are getting is that more specific actionable intelligence information is what is needed. That is the feedback we got on AURORA. There were limits on what could be said. So it is a combination of clearances to the industry and figuring out ways of having -- arranging a classification of information such that it can get out. Both of those are important.

Mr. Matheson. Okay. I appreciate that.

Mr. McClelland, I was going to ask you if the new Federal authority that issues cyber emergency orders is too broad. That could also cause some other unintended consequences. Do you have thoughts about where we get the sweet spot on this?

Mr. McClelland. Yeah, that is very difficult. The authority has been called extraordinary. It is extraordinary authority. And the Commission is not an intelligence agency. Some may say we don't even have intelligence. But we don't collect intelligence. So we would depend on other agencies such as DOE, DHS, DOD, CIA to bring vulnerabilities and threats that would endanger national security, use our authority then to order mitigation. It is very specific mitigations that may be targeted at very specific utilities for a limited period of time. That is much more targeted and specific than, say, a standards action might be.

Mr. Matheson. Okay. And can I ask you, do you have thoughts about steps the Federal Government could take to -- you heard questions about costs from other members. Do you have thoughts

about how the Federal Government could work with utilities to help mitigate the cost impact relative to the risks that we are trying to address?

Mr. McClelland. Yes. We had the benefit of reviewing with the utilities. We asked for 30 volunteers and did get 30 volunteers on the AURORA mitigation. We had the benefit of spending a day with each of those utilities, and there were some very good ideas that came from the utilities back to the Commission. So it would be an iterative process.

The Commission would have to move quickly. If it was a vulnerability or threat that endangered national security, we would issue that. There would be a hearing process or a back-and-forth process where alternative practices could be proposed by the utilities to accomplish the same purpose but nevertheless not delay the mitigation being put into place to protect the economy, its citizens, and the military of the United States.

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

Mr. Markey. The gentleman's time has expired.

The Chair recognizes the gentleman from Oregon, Mr. Walden.

Mr. Walden. Thank you, Mr. Chairman.

So I want to see if I have this right. Basically, folks in the power industry don't get the information of the specificity of the threat that they are supposed to figure out how to deal with. Right? I mean, isn't that what you are saying?

Mr. DiStasio. What I said was, to date, there has not been any specific actionable information provided. Not to say there aren't vulnerabilities, but there has not been an individual threat that has been communicated beyond this AURORA test.

Mr. Walden. And yet we know there are, Mr. McClelland, to the extent you are able to talk about this, that there are fairly specific threats. Well, we all know every computer it seems like is being attacked by somebody at some point. And so how do we bridge this? It would seem to me with so much on the line that there must be a way that we can communicate the information you need to understand how serious this is and to cope with it. I understand you understand how serious it is. How do we bridge that?

Mr. DiStasio. I want to be very clear on one point. The utility industry has been dealing with vulnerabilities maybe that originated from reliability and now much more security and cyber-based for many, many years and will continue do that. So we are not awaiting information to do that. However, if there is a gap, it is around this issue that there is a lot of discussion around pending threats that seem to be more imminent that have not been communicated; and we just need to understand what those are so we can best mitigate them on the ground within our systems for the consumers.

Mr. Walden. And is the issue here that you want to know the very timely, specific threat, as in X organization is going to do

Y to your system, or is it -- is there anything you are not doing now to protect your system that that kind of information would help you protect?

It would seem to me it is pretty clear where the threat -- not where it comes from from a specific individual or organization necessarily, but there are only so many ways to get into your system and do damage. And I guess that is the question. You would think you would know what those ways are and be set up to mitigate, right?

Mr. DiStasio. And we do believe that we are in a position to best mitigate. I mentioned before that we use this layered approach --

Mr. Walden. Right.

Mr. DiStasio. -- to deal with these. But to the extent there was something that is yet not known to the industry that needs to be communicated, we would benefit by having specific and actionable information on that.

Mr. Walden. So let me go to our government witnesses here. Without getting into specific things we can't talk about here, are the actions they are talking about they are doing, the sort of physical actions to deal with management of their systems and prevent against those threats, do they have as much knowledge as they need to know, need to have to deal with it without knowing specific time, place, type of attack?

Mr. McClelland. The distinction between classified and

unclassified is who is the actor and what specific systems are being targeted.

The vectors back as far as the AURORA advisory, for instance, there was sufficient information and detail within that advisory for folks to be able to perform mitigation actions. And that advisory was not developed by the Commission. It was developed by DHS, DOE, and NERC and then issued to industry.

I think part of the question here is, is there a central agency that is responsible to get the information to the industry and then can hold industry accountable? Right now, all that we have is we have a coordination and a great partnership with DOE, DHS, and industry. But the advisories, the information that is conveyed is voluntary in nature.

Mr. Walden. And is it also your sense that those advisories, that information, those recommendations are not being acted upon to the extent they need to be acted upon? In other words, the systems aren't being upgraded or modified to deal with the threat, and they should be fully aware of what that threat is absent the classified piece of who it is and specific targets?

Mr. McClelland. Right. Congress asked the Commission to verify, for instance, the compliance with the AURORA advisory. And, on that basis, I would answer the question that, no, compliance is not sufficient. The Commission reached the conclusion that only if it can be compelled would we be able to assure that compliance has been executed for that.

Mr. Walden. Mr. Brown, let me give you the last 14 seconds.

Mr. Brown. The more information the better. I will use New York State as an example. The single largest contingency we plan for is a 1,200 megawatt nuclear power plant going down, because that is our single largest worst thing that could happen. And at all times they maintain what is called spinning reserves, so if that plant goes down, everything is cool. Then they figure out the next biggest contingency and start planning for that.

The more information the more you can do those contingencies and be prepared for what happens to your system. Without the information, without a specific threat, they are going to be operating as if the situation was normal. And that is where I think you become most vulnerable at that point, when you are not prepared for two or three things happening at once, which if you knew that there was a threat of that you could plan your system around it.

So that is why the control area is even more important than the utilities when it comes to this. The utilities maintain their little footprint. But especially in the Northwest and in the Northeast, there are larger control areas that are looking at the system as a whole; and the larger a system you are looking at, the more contingencies you can use to address any problems that develop.

Mr. Walden. Okay. My time has expired. Thank you very much for your testimony.

Mr. DiStasio. Mr. Chairman?

Mr. Markey. Mr. DiStasio, yes.

Mr. DiStasio. I would like to make one follow-up.

The industry does not agree that the information was specific and actionable, and what we would like to do is submit something for the record for the committee's benefit.

Mr. Markey. Okay. That would be very helpful, as this hearing has been.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Markey. We are going to focus very keenly in on all of the issues that have been identified here today. It is not lost on the committee that in a recent survey by the NERC of the generation owners in America that only one-third of them could identify a single critical asset to which the NERC cyber standards would apply. And so that, in and of itself, says something about this issue, that only one-third of all generators in America felt that they had any critical assets at all that should have protection.

So there is a big gap here. We have to find a way of closing it. And I think today you have really helped us to shape kind of the challenge for the committee: bulk power system versus the distribution system, cyber threats versus physical threats, emergency authority versus standards being set. So we have to walk through each of these issues, illuminated by the testimony that you have provided for us here today.

We thank all of you very much for your testimony. We want to stay very close to all of the stakeholders in this discussion so that we can ensure that we make the right decision in terms of the legislation, and we want to invite all the members of the committee as well to work with us so that we put together the best possible legislation.

The gentleman from Texas?

Dr. Burgess. Mr. Chairman, I wonder if I might just ask one

additional question while we are all gathered here.

Mr. Markey. The gentleman interrupted the chairman's concluding statement in order to make that unanimous consent request. So, without objection, the gentleman will be recognized to ask one question of the panel.

Dr. Burgess. And I apologize, because I thought it was a soliloquy. I didn't realize it was the concluding statement.

On the issue of the --

Mr. Markey. When Chairmen Tauzin and Barton used to utter them, it was almost as if it was coming down from Mount Sinai as the 10 Commandments; and so I understand the different perspectives actually orient members differently when they hear the person with the gavel speaking.

Dr. Burgess. It was just a general knowledge question on the issue of the solar interference.

Mr. McClelland, I guess this is for you. A couple of years ago, when I was working with the pilots union and flight attendant unions on trying to mitigate their exposure to in-flight radiation, I got the impression there was a predictive ability to these. Are we able to predict with any accuracy the sudden burst of solar activity?

Mr. McClelland. That is an excellent question, and it speaks to -- I have had the same question sort of posed a different way: If the Commission did have emergency authority to be able to order mitigations against, say, solar magnetic activity, how could it

exercise that when the warning would be so little?

There is a satellite deployed, it is the ACE satellite, that gives us about 15 to 30 minutes of warning for solar activity. And, in fact, some of the most massive solar storms in history have been with little or no sunspot activity. So sunspot activity is not a good predictor of the magnitude of solar storm that might occur. Fifteen or thirty minutes would be wholly inadequate unless the Commission had ordered mitigation plans be put into place first.

For instance, the EMP Commission said that a good way to mitigate against E3, this effect, would be to put a resistor in series with the transformer, maybe even a capacitor. Those could be put into place with 15 to 30 minutes. As long as the entities were practiced, they could be given that notice. And the thought would be that they will get more and more time, and they could switch those in to mitigate.

Dr. Burgess. Thank you, Mr. Chairman.

Mr. Markey. The gentleman's time has expired.

We thank all the witnesses again. The big solar announcement today, of course, is that the President is down at Florida Power & Light making this big announcement about solar technology in Florida and its interrelationship with the smart grid. So, obviously, that focuses us on solar, on smart grid, on making sure we build this out correctly. Because obviously in this new distributed energy world that solar presents we need to continue

to think through. But my congratulations to Florida Power & Light for that big breakthrough today with the President.

And, with that, this hearing is adjourned.

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