SECURING THE MODERN ELECTRIC GRID FROM PHYSICAL AND CYBER ATTACKS

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JULY 21, 2009

Serial No. 111–30

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

53–425 PDF WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
ERIC J.J. MASSA, New York
DINA TITUS, Nevada
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

YVETTE D. CLARKE, New York, *Chairwoman*

LORETTA SANCHEZ, California
LAURA RICHARDSON, California
BEN RAY LUJÁN, New Mexico
MARY JO KILROY, Ohio
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
PAUL C. BROUN, Georgia
STEVE AUSTRIA, Ohio
PETER T. KING, New York *(Ex Officio)*

JACOB OLCOTT, *Staff Director*
DR. CHRIS BECK, *Senior Advisor for Science and Technology*
DANIEL WILKINS, *Clerk*
COLEY O'BRIEN, *Minority Subcommittee Lead*

CONTENTS

Page

APPENDIX I

APPENDIX II

SECURING THE MODERN ELECTRIC GRID FROM PHYSICAL AND CYBER ATTACKS

Tuesday, July 21, 2009

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY,
Washington, DC.

The committee met, pursuant to call, at 2:13 p.m., in Room 311, Cannon House Office Building, Hon. Yvette D. Clarke [Chairwoman of the subcommittee] presiding.

Present: Representatives Clarke, Thompson, Richardson, Luján, Lungren, and Austria.

Also present: Representatives Harman, Lofgren, Langevin, Jackson Lee, Pascrell, and Bartlett.

Ms. CLARKE [presiding]. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on securing the modern electric grid from physical and cyber attacks. We have been joined here today by many of my distinguished colleagues, who don't sit on this subcommittee, but who are an integral part of the deliberations that we do, and I would like to acknowledge them and ask that they be given unanimous consent to sit and participate in our hearing today.

Hearing no objection, so ordered.

I want to recognize some of our colleagues from other committees who are participating in today's hearing, including Mr. Bartlett. We would not have a robust road map for addressing the EMP threat if it were not for his vision and leadership and I thank him for that.

I also have my colleagues who serve on the full committee, Zoe Lofgren, of California, Congresswoman Jackson Lee of Texas, and Mr. Bill Pascrell of New Jersey. I thank you for attending this very important hearing.

We expect to be joined by many other Members, and I would like to just acknowledge them in absentia for right now; Mr. Langevin, who is my predecessor as Chair of this committee. I would like to congratulate him on his new Chairmanship and thank him for his leadership on the electric grid security issue.

I would also be expecting a colleague on the Subcommittee for Intelligence to the Homeland Security Committee, Ms. Harman, and thank her for her attendance today.

Unfortunately, a number of my colleagues and our friends from the Energy and Commerce Committee are unable to attend and participate in today's session due to their work on the health care

legislation. We have reached out to Mr. Waxman, Mr. Markey, and Mr. Barrow to ask them to act with urgency on the subject matter we will discuss today.

Our national health care delivery system, just like all of our critical infrastructure systems, requires secure and reliable electric system. That is what this committee has been investigating for years, and what we will discuss today.

The electric grid is fundamental to our lives and our country's existence. Without electricity, medicines expire, banks shut down, food goes bad, sewage and water plants don't function. Chaos ensues and our security is compromised.

We simply cannot afford to lose broad sections of our grid for days, weeks, or months.

It is our very reliance on this infrastructure that makes it an obvious target for attack. We know that many of our adversaries, from terrorist groups to nation-states, have and continue to develop capabilities that would allow them to attack and destroy our grid, at a time of their choosing.

There are two significant threats that will be discussed at today's hearing. One is the threat of a cyber attack.

Many nation-states, like Russia, China, North Korea, and Iran, have offensive cyber attack capabilities, while terrorist groups like Hezbollah and al Qaeda continue to work to develop capabilities to attack and destroy critical infrastructure, like the electric grid, through cyber means.

If you believe intelligence sources, our grid is already compromised. An April 2009 article in the Wall Street Journal cited intelligence forces who claim that "the grid has already been penetrated by cyber intruders from Russia and China, who are positioned to activate malicious code that could destroy portions of the grid at their command."

The other significant threat to the grid is the threat of a physical event; that could come in the form of a natural or man-made electromagnetic pulse, known as EMP. The potentially devastating affects of an EMP to the grid are well documented.

During the Cold War, the U.S. Government simulated the effects of EMP on our infrastructure because of the threat of nuclear weapons, which emit an EMP after detonation. Though we may no longer fear a nuclear attack from Soviet Russia, rogue adversaries including North Korea, and Iran, possess and test high-altitude missiles that could potentially cause a catastrophic pulse across the grid.

These are but two of the significant emerging threats we face in the 21st Century. Our adversaries openly discuss using these capabilities against the United States.

According to its cyber warfare doctrine, China's military strategy is designed to achieve global electronic dominance by 2050, to include the capability to disrupt financial markets, military and civilian communications capabilities, and the electric grid prior to the initiation of a traditional military operation.

Cyber and physical attacks against the grid could both be catastrophic and incredibly destructive events. They are not inevitable.

Protections can, and must, be in place ahead of time to mitigate the impact of these attacks. My colleague on the Homeland Secu-

rity Committee, and I, have spent nearly 3 years identifying and reviewing the security protections that are in place to mitigate the affects of any intentional or unintentional attack on the electric system.

Our goal is to determine whether appropriate protections are in place that would mitigate catastrophic incidents on the grid. Our review has required extension discussions and assessment with the private sector, which owns, operates and secures the grid.

The private sector develops its own security standards, the private sector also oversees compliance with these standards. In short, the private sector has the responsibility for securing the grid from electromagnetic events and cyber attacks.

In the course of our review, we have questioned hundreds of experts, and reviewed thousands of pages of research and analysis. Many have submitted statements for the record today. They have all reached one conclusion. The electric industry has failed to appropriately protect against the threats we face, in the 21st century.

In the past, this committee has been deeply critical of the standards that the industry has written. They are, in the words of GAO and NIST and other independent analysts, inadequate for protecting critical national infrastructure.

The committee has suggested that the industry adopt missed standards for control systems, if it hopes to achieve greater security. My understanding is that the industry has not embraced this suggestion.

The committee has also been critical of the industry's effort to timely mitigate the Aurora vulnerability. What should have been an urgent action issue has taken some utilities years to fix. Many have not even hardened their assets at all.

This is especially troubling given the catastrophic damage that could be caused by an Aurora-style attack. Today, there is a new problem.

Many in the industry are apparently trying to avoid compliance with their own inadequate standards. I am deeply concerned about this irresponsible behavior.

A letter dated April 7, 2009, which is attached for the record, sent to the industry by the NERC chief security officer, Mike Assante, suggests that industry is choosing not to identify critical assets in order to avoid securing them.*

According to Mr. Assante, only 29 percent of generation owners and generation operators reported identifying at least one critical asset. Sixty-three percent of transmission owners identified at least one critical asset.

This effort seems to epitomize the head-in-the-sand mentality that seems to permeate broad sections of the electric industry. The committee will be following up with NERC to learn which utilities have not appropriately identified assets, and seek to make this information public.

It is amazing that many within the industry would rather gamble with our national and economic security, than implement precautionary security measures. What is even more amazing is that

*The information referred to is included in Appendix I.

utilities have chosen to take this posture, even though they can be reimbursed for these security expenditures in their rate cases.

I am at a loss as to why the industry isn't apparently securing its assets. But clearly, the time has come for change.

I am pleased to join Chairman Thompson and Ranking Member King and my other colleagues in co-sponsoring H.R. 2195. Given the industry's lackluster approach toward securing its own assets, I believe this measure will provide the Federal Energy Regulatory Commission with the appropriate authorities to ensure that our grid is secure and resilient against the threats we face in the 21st Century.

This subcommittee will continue to perform rigorous oversight until we are satisfied that progress is being made.

I now recognize my colleague, the gentleman from California, Ranking Member, Mr. Lungren, for his opening statement.

Mr. LUNGREN. Thank you very much, Madame Chairwoman, I commend you for holding this hearing on the security of our Nation's electric grid.

As you know, I share your concern about the continuing vulnerability of our electric grid, which many consider the most critical piece of our Nation's infrastructure.

As everyone knows, without electricity our banking, commerce, transportation, health and medical services would be unavailable or severely limited. Indeed, our economy and the public welfare have become severely dependent on electricity. Consequently, securing this grid is a critical national economic priority that Congress must, and I am sure we will, address with urgency.

In recent decades, the push towards making our society more reliant on electric power has also made us more vulnerable. Because of expanding digital and computerized connections, our electric grid is now, more than ever, vulnerable to cyber and physical attacks. These attacks could disable wide segments of the grid for weeks, months, possibly years.

The effective functioning of the electric grid is highly dependent on today's control systems, which are computer-based, and used to monitor and control sensitive processes and physical functions.

You know, once largely proprietary, closed systems, control systems are now increasingly connected to open networks such as corporate intranets and the internet. The expansion of control systems, including supervisory control and data acquisition, SCADA systems, and the ability to monitor them via the internet, has increased the vulnerability of our Nation's critical infrastructure to cyber attack.

As was mentioned, U.S. adversaries, whether they are nation-states or rogue nations, can strike crippling blows to our Nation's infrastructure from remote locations around the world.

I think these nation-states that have the offensive cyber attack capabilities understand that it is far cheaper, and oftentimes unattributable, to attack and destroy U.S. critical infrastructure through cyberspace rather than risk any type of conventional warfare.

The other significant threat to our grid, is as mentioned by the Chair, that of EMP. My colleague from Maryland, who has done as much work on this as anybody as I know in the House, and it is

a concept that, unfortunately, I am afraid most Members are not fully aware of.

It is because of rogue nations, and their ability now to command certain missile delivery systems, it seems to me that this is a far more urgent matter than it was just a number of years ago.

While we understood the importance of this vulnerability during the Cold War, I am not sure we have visited this subject with the intensity and the urgency that is necessary. So I do appreciate what we are doing in this hearing.

Because of these increased cyber and EMP threats to our electric grid and the Federal Energy Regulatory Commission's lack of authority to address them in an expeditious manner, I join Chairwoman Clarke and the Chair of the full committee and the Ranking Member of the full committee in co-sponsoring H.R. 2195.

I believe our legislation will provide FERC with emergency authority to create mandatory physical and cybersecurity standards to protect the electric power system.

I would just like to say, we are all in this together, whether we are in the private sector or the public sector. We have got a lot of catching up to do.

I would hope that we would try and strive for solutions. Not necessarily be overly critical of all the participants in this. It is just my reflection that we have, in some ways, come to this late, both as a Congress, as an Executive branch, as the private sector as well. We need to work together as quickly as we can to protect this system.

It is a lifeline to so much of our economic life, and actually, life period, in this country. The vulnerabilities have to be recognized up front. We can't be embarrassed about them. We have to work with one another to try and solve this very urgent problem.

That is why I am very pleased that we have this hearing today. I think we have a good line-up of witnesses that can give us various perspectives and help us move in the direction that I hope we can move in on a bipartisan basis with some urgency.

So, I thank the Chairwoman.

Ms. CLARKE. I thank you.

I now recognize prime sponsor of H.R. 2195, Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Chairwoman Clarke. Thank you for holding this critical hearing today.

Like you, I am determined to prevent any attack on the United States homeland. A multitude of failures contributed to our inability to prevent the attacks on New York City, and Washington, DC on September 11.

Mindful of our previous mistakes, let's review the set of facts before us in today's testimony.

We have significant vulnerabilities in the grids' electrical infrastructure. The infrastructure is only getting more vulnerable with Smart Grid technology. There is a massive computer espionage campaign being launched against the United States by our adversaries.

Intelligence suggests that countries seek, or have developed, weapons capable of destroying our grid. A congressional commis-

sion says that our grid, and the critical infrastructure that relies on the grid, is not adequately protected.

Our military installations are vulnerable because they rely on an insecure electric grid. The private sector is in charge of writing its own security standards, but experts have judged the standards to be ineffective in securing the infrastructure. Many utilities are avoiding compliance with these standards.

I ask my colleagues here today, and those who could not join us, what more do we need to hear from, before we act? We are more motivated, than we need to. The warning signs are flashing red.

Now is the time to act to secure the electric grid, not after a major incident has occurred. This committee has a bipartisan, bicameral legislative solution to secure the electric grid. Our bill is comprehensive in its scope, because the grid is only as strong as its weakest link.

We believe that all elements of the grid, from generation to transmission, to distribution, to metering infrastructure, should be included. Our bill covers physical attacks like electromagnetic pulse, as well as cyber attacks. The Critical Electric Infrastructure Protection Act will do four things to improve our defensive posture.

No. 1, it requires FERC to establish interim measures deemed necessary to protect against physical and cyber threats to critical electronic electric infrastructure. This will improve existing mandatory standards.

No. 2, it provides FERC with the authorities necessary to issue emergency orders to owners and operators of electric grid after receiving a finding from DHD about a credible or imminent cyber attack.

No. 3, it requires DHS to perform on-going cybersecurity, vulnerability and threat assessment, to critical electric infrastructure and provide mitigation recommendations to eliminate those vulnerabilities and threats.

No. 4, it also requires DHS to conduct an investigation to determine if the security of Federally-owned, critical, electric infrastructure has been compromised by outsiders. I am proud of this bill. I know my colleagues are proud also. We have support of both Republican and Democratic co-sponsors.

Madame Chairwoman, I look forward to the testimony of our two panel witnesses today, and I yield back.

Ms. CLARKE. Thank you. I now recognize Mr. Bartlett, who is widely acknowledged here on the Hill as one who has been a visionary and a leader in providing a robust roadmap for addressing the threat of EMP, and I would like to acknowledge him and have him make his comments at this time.

Mr. BARTLETT. Thank you very much for inviting me to sit with you today. I am very pleased that there is now increasing recognition of the vulnerability of our grid and our country, to EMP. I have been concerned about this a number of years. Dr. Graham is here, who has chaired the commission that my legislation set up in 2001, and this is probably one of the longest-serving commissions on the Hill. I hope that it will be serving for a while yet, because the job is not done.

If an EMP attack were vigorous enough, and you know, this is kind of tough, because it is said that if it is too good to be true,

it is probably not true, and in this case, if it is too bad to be true, it is probably not true. But in this case, I am sorry to say, it could be true.

If the EMP lay down were vigorous enough, you could find yourself in a world that, essentially the only person you could talk to is the person next to you, unless you were a ham operator with a vacuum tube set, which is a million times less susceptible. The only way you could go anywhere, is to walk, unless you were the proud owner of a Edsel or similar vintage automobile with coil and distributor.

Of course, if you do not have electricity, you do not have anything in our world. Our very vulnerability invites attack, and it doesn't have to be a nation-state. Anybody who can get a tramp steamer, buy a SCUD launcher for $100,000, with a crude nuclear weapon, could do an EMP lay down. Not country-wide, but certainly over New England. By the way, if you missed your target by 100 miles, it is as good as a bull's-eye.

So this would obviously be the most asymmetric attack that could be launched against us. My wife says I shouldn't talk about this, because I am giving these people ideas, you know. But it is in all of their literature. It is in all of their war games. Not one out of 50 Americans may know about EMP, but I will assure you that 100 percent of our potential enemies know all about EMP.

So thank you very much for your vision in holding this hearing, and thank you for inviting me to be with you.

Ms. CLARKE. Other Members of the subcommittee are reminded that under committee rules, opening statements may be submitted for the record.

I welcome our first panel of witnesses today. We are joined by a distinguished panel of private sector witnesses. Dr. William Graham is the chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse, also known as the EMP Commission.

Mr. Fabro is the president and chief security scientist of Lofty Perch. Mr. Michael Assante, is the chief security officer of the North America Electric Reliability Corporation, also known as NERC, and Mr. Steve Naumann, is the vice president of wholesale markets at Exelon Corporation. Mr. Naumann is providing testimony on behalf of the Electric Industry Association, Edison Electric Institute, and the Electric Power Suppliers Association.

Just to give you an idea of the importance of this topic, we received a number of statements for the record. I have made these statements available to the Members ahead of time, but ask unanimous consent that the following statements be included into the record. The National Association of Regulatory Utility Commissioners; Dr. Bill Rodasky, President of Metatech, and John Caperman, Metatech consultant. George Anderson and Gail Nordling of Emprimus. Mike Frankel, executive director of the EMP Commission, Joe Weiss, Applied Control Solutions, and Curtis Birnbach, president of Advanced Fusion Systems.

Hearing no objections, it is so ordered.

In the interest of time, I will ask that each of you provide a brief biography of your work without objection. The witnesses' full statement will be inserted in the record. I now ask you to introduce

yourselves, and summarize your testimony for 5 minutes, beginning with Dr. Graham.

STATEMENT OF WILLIAM R. GRAHAM, CHAIRMAN, COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE

Mr. GRAHAM. Thank you, Madame Chairwoman, distinguished Members of the committee, for the opportunity to testify today on the matter of the nuclear magnetic pulse threat to the United States, to our forces, our allies and our friends worldwide.

By way of background, I am an electrical engineer and a physicist, who first served as a junior officer in the Air Force in 1962, and encountered the EMP problem as a great surprise to all of us, as a result of the high altitude test series that the United States conducted over the Pacific, primarily Johnston Island, at that time.

I continued to work on the problem throughout my career, now some 45 years, including as, among other things, the director of the Office of Science and Technology Policy in the Executive Office of the President and the science advisor to President Reagan during his second term.

Several potential adversaries have or can acquire the capability to attack the United States with high-altitude nuclear weapon-generated electromagnetic pulse. In fact, a determined adversary can achieve an EMP attack capability without having a high level of technical sophistication. EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences.

EMP will cover a wide geographic region within line-of-sight of a nuclear weapon explosion. It has the capability to produce significant damage to critical infrastructures, and thus the very fabric of U.S. society, as well as the ability of the United States and western nations to project influence and military power. The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled with critical infrastructures.

An example of this, and the increase in potential vulnerability, can be seen in the Smart Grid, where considerable interest and effort is being made in adding electronics to our electric distribution grid for efficiency, effectiveness, and safety. But it can undermine that grid if it is not designed properly. This EMP impact is asymmetric in relation to our potential adversaries who are not so dependent on modern electronics.

The current vulnerability of our critical infrastructure can both invite and reward attack, if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish. In fact, with proper design of protection for both physical and cyber attacks, which should be integrated in our electrical distribution and other critical infrastructure systems, I believe we can actually work to a net economic benefit, because of the improved reliability and performance that we will achieve with these critical infrastructures.

However, there is an implicit invitation in the fact that the United States is vulnerable in this area, to adversaries. We know that geomagnetic storms will occur and they will damage electric power distribution systems. The question is not if, but when?

Concerning EMP, the logic of the position is upside-down, in often-made statements about it being improbable. By ignoring large-scale catastrophic EMP vulnerabilities, we invite such attacks on our infrastructure by adversaries who seek to attack us where we are weak, not where we are strong, and to take advantage of that vulnerability.

We have prepared two unclassified reports, one on critical national infrastructures, and an executive oversight report by the commission, and I submit those to you as well, Madame Chairwoman.

I would like to say then, while much of our discussion is contained in those, in conclusion I would say that I would like to go on the record as supporting H.R. 2195, the bill to amend the Federal Power Act, to provide additional authority to adequately protect the electrical infrastructure against cyber attack, and for other purposes.

At the same time, I would like to strongly recommend that very large-scale electromagnetic threats to the critical infrastructure, both EMP and naturally occurring, be addressed explicitly in the bill, in a manner comparable to and parallel with the cyber threats now contained in the bill. Thank you very much.

[The statement of Mr. Graham follows:]

PREPARED STATEMENT OF WILLIAM R. GRAHAM

JULY 21, 2009

Mr. Chairman, Members of the committee, thank you for the opportunity to testify today on the matter of the Nuclear Electromagnetic Pulse (EMP) threat to the United States, its forces, its allies, and its friends worldwide.

ABSTRACT

Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication.

EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of U.S. society, as well as to the ability of the United States and Western nations to project influence and military power.

The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The impact of EMP is asymmetric in relation to potential protagonists who are not as dependent on modern electronics.

The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.

BACKGROUND

I am an Electrical engineer and physicist who has served as a junior officer in the Air Force, as Director of the Office of Science and Technology Policy in the Executive Office of the President, and in the aerospace industry, together for over 45 years. I have also served on several Government advisory boards, including as Chairman of the President's General Advisory Committee, and a member of the Defense Science Board, the Department of State's International Security Advisory Board, The National Academies Board on Army Science and Technology, and from 2001 to 2009 as Chairman of the statutorily established Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. While now retired, I have worked on problems related to EMP during much of my career, be-

ginning with my service in the Air Force at the Air Force Weapons Laboratory in 1962.

The commission requested and received information from a number of Federal agencies and National Laboratories. We received information from the North American Electric Reliability Corporation, the President's National Security Telecommunications Advisory Committee, the National Communications System (since absorbed by the Department of Homeland Security), the Federal Reserve Board, and the Department of Homeland Security.

INTRODUCTION

A high-altitude electromagnetic pulse results from the detonation of a nuclear warhead at altitudes of about 40 to 400 kilometers above the Earth's surface. The immediate effects of EMP are disruption of, and damage to, electronic systems and electrical infrastructure. EMP is not reported in the scientific literature to have direct effects on people.

EMP and its effects were observed during the U.S. and Soviet atmospheric test programs in 1962. During the U.S. STARFISH nuclear test at an altitude of about 400 kilometers above Johnston Island,, some electrical systems in the Hawaiian Islands, 1,400 kilometers distant, were affected, causing the failure of street lighting systems, tripping of circuit breakers, triggering burglar alarms, and damage to a telecommunications relay facility.

In their testing that year, the Soviets executed a series of nuclear detonations in which they exploded 300 kiloton weapons at approximately 300, 150, and 60 kilometers above their test site in South Central Asia. They report that on each shot they observed damage to overhead and underground buried cables at distances of 600 kilometers. They also observed surge arrestor burnout, spark-gap breakdown, blown fuses, and power supply breakdowns.

The physical and social fabric of the United States is sustained by a system of systems; a complex dynamic network of interlocking and interdependent infrastructures ("critical national infrastructures") whose harmonious functioning enables the myriad services, transactions, and information flows that make possible the orderly conduct of civil society in this country while also supporting our economic strength and national security. The vulnerability of these infrastructures to threats—deliberate, accidental, and acts of nature—is the focus of significant concern in the current era, a concern heightened by the events of 9/11, major hurricanes, recent wide-area power grid failures, and large-scale cyber attacks to date directed at other countries.

In November 2008, the commission released an unclassified assessment of the effects of a high altitude electromagnetic pulse (EMP) attack on our critical national infrastructures and provides recommendations for their mitigation. The assessment entitled *Critical National Infrastructures* was informed by analytic and test activities executed under commission sponsorship, as discussed in the report. An earlier executive report: *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP)—Volume 1: Executive Report* (2004), provided an earlier unclassified overview of the subject. The commission also prepared and submitted to the Congress and the administration several classified reports addressing military, nuclear weapon, and intelligence aspects of the subject.

The electromagnetic pulse generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences. The increasingly pervasive use of electronics of all forms represents the greatest source of vulnerability to attack by EMP. Electronics are used to control, communicate, compute, store, manage, and implement nearly every aspect of United States (U.S.) civilian systems. When a nuclear explosion occurs at high altitude, the electromagnetic fields it produces will cover the geographic region within the line of sight of the detonation.[1] This intense electromagnetic phenomena, when coupled into sensitive electronics through any connected wires or other electrical conductors, has the capability to produce widespread and long lasting disruption and damage to the critical infrastructures that underpin the fabric of U.S. society. Because of the ubiquitous dependence of U.S. society on the electrical power system, its vulnerability to an EMP attack, together with power grids increasing dependence on electronics for efficiency, control, and safety, as reflected for example in increasing national interest in "Smart Grid" design and implementation, creates the possibility of long-term, catastrophic consequences.

[1] For example, a nuclear explosion at an altitude of 100 kilometers would expose 4 million square kilometers, about 1.5 million square miles, of Earth surface beneath the burst to a range of EMP field intensities.

THE IMPLICIT INVITATION

Some in Government have taken the position that EMP attack and geomagnetic storm disruption are low-probability events. Of course, we know that geomagnetic storms will occur, and large ones can seriously damage very long-lead components of the electrical system—it is only a question of when, not if. Concerning EMP, the logic of their position is upside-down. By ignoring large-scale, catastrophic EMP vulnerability, we invite such attack on our infrastructure by adversaries looking to attack us where we are weak, not where we are strong. Our adversaries know how to take advantage of this vulnerability, and when coupled with increasing nuclear weapon and ballistic missile proliferation, it is a serious concern. A single EMP attack may effectively instantaneously degrade or shut down a large part of the electric power grid in the geographic area of EMP exposure. There is also a possibility of functional collapse of grids beyond the exposed area, as electrical effects propagate from one region to another, as has happened in power grid failures over the last 40 years.

The time required for full recovery of electrical power service would depend on both the disruption and damage to the electrical power infrastructure and to other national infrastructures. Larger affected areas and stronger EMP field strengths would prolong the time to recover. Adding to the recovery time, some critical electrical power infrastructure components, such as large high-voltage transformers, are no longer manufactured in the United States, and even in routine circumstances their acquisition requires up to a year of lead time.

Damage to or loss of these components could leave significant parts of the electrical infrastructure out of service for periods measured in months to a year or more. There is a point in time at which the shortage or exhaustion of sustaining backup systems, including emergency power supplies, batteries, standby fuel supplies, communications, and manpower resources that can be mobilized, coordinated, and dispatched, together would lead to a continuing degradation of critical infrastructures for a prolonged period of time.

Electrical power is necessary to support other critical infrastructures, including supply and distribution of fuel, communications, transport, financial transactions, water, food, emergency services, Government services, and all other infrastructures supporting the national welfare, economy, and security. Should significant parts of the electrical power infrastructure be lost for any substantial period of time, the commission believes that the consequences are likely to be catastrophic, and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities. In fact, the commission is deeply concerned that such impacts are likely in the event of an EMP attack unless practical steps are taken to provide protection for critical elements of the electric system and for rapid restoration of electric power, particularly to essential services.

A PLAN OF ACTION

It is the consensus of the EMP Commission that the Nation need not be vulnerable to the catastrophic consequences of an EMP attack. As detailed in the commission reports provided to the Congress, the Nation's vulnerability to EMP that gives rise to potentially large-scale, long-term consequences can be reasonably and readily reduced below the level of a potentially catastrophic national problem by coordinated and focused effort between the private and public sectors of our country. The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures threatened. In fact, electromagnetic protection of the critical national infrastructures may over time provide a net saving of money through the more reliable and robust operation of the systems involved.

The appropriate response to the EMP threat is a balance of prevention, protection, planning, and preparations for recovery. Such actions are both feasible and well within the Nation's means and resources to accomplish. A number of these actions also reduce vulnerabilities to other serious threats to our infrastructures, thus giving multiple benefits.

It is not feasible to reduce the consequences of an EMP attack to an acceptable level of risk by any single measure. However, in the view of the EMP Commission, it is possible to achieve an acceptable level of risk and reduced invitation to an EMP attack with a strategy that integrates several significant measures:

- Pursuing intelligence, interdiction, and deterrence to discourage EMP attack against the United States and its interests;
- Protecting critical components of the infrastructure, with particular emphasis on those that, if damaged, would require long periods of time to repair or replace;

- Maintaining the capability to monitor and evaluate the condition of critical infrastructures;
- Recognizing an EMP attack and understanding how its effects differ from other forms of infrastructure disruption and damage;
- Planning to carry out a systematic recovery of critical infrastructures;
- Training, evaluating, "Red Teaming," and periodically reporting to the Congress;
- Defining the Federal Government's responsibility and authority to act;
- Recognizing the opportunities for shared benefits;
- Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects.

Finally, I would like to state for the record that I support H.R. 2195, a bill to amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes. At the same time, I strongly recommend that electromagnetic threats to the critical electric infrastructure, both from nuclear EMP attack and from naturally occurring, large-scale geomagnetic storms, be addressed in the bill in a manner explicitly comparable to and in parallel with cyber threats as now contained in the bill. It is important to do this because an integrated approach to protecting critical electrical infrastructure will be much less expensive and more effective and expedient than any fragmented approach to the problem, and unlike the Department of Defense, the Department of Homeland Security, from its establishment forward, has shown neither an understanding nor a willingness to consider the problem of electromagnetic threats to our country.

Mr. THOMPSON [presiding]. Thank you very much, Dr. Graham. Chairwoman Clarke had to go and cast votes in a mark-up. She will return shortly.

Mr. Fabro, 5 minutes.

STATEMENT OF MARK FABRO, PRESIDENT AND CHIEF SECURITY SCIENTIST, LOFTY PERCH

Mr. FABRO. Thank you to the committee for the opportunity to testify today. My name is Mark Fabro and I am the president and chief security scientist of Lofty Perch, a company focused on providing control systems, cybersecurity services and research. I am a member of the UTC Smart Network Security Committee; the chairman of the Canadian Industrial Cyber Security Council; and co-chair of ISA–99, Working Group 10.

I am here today to provide insight as to what measures can be taken to help protect the modern electric grid from cyber attack. There is no doubt as to whether or not our electric infrastructure will continue to converge with internet-based systems, and as it matures, it will inherit cyber vulnerabilities.

We know there is a problem. We know the cause of the problem. We know what works to correct it. We just need a plan to implement. Our challenge is to ensure that, as we go forward, we have done our due diligence, improving solutions as secure and reliable, and that we protect what might be the most vital of all critical infrastructures.

But it is important to note, the findings regarding cybersecurity risk are not ubiquitous across all the entities supporting the bulk power system. Moreover, they are not unique to single countries, entities or operators, and they most certainly are not indicative of an overall generally poor security posture.

We continue to witness excellent examples of effective cybersecurity activities from many entities and observe progress that does not align with the popular opinion that the bulk power system is ripe for total cyber compromise.

The complexity of the problem in trying to measure how secure or resilient the grid is from cyber attack, cannot be overstated. Often, and erroneously, the cybersecurity problem is framed under the assumption that there is simply a single, uniform grid, and that a mitigation strategy, be it technical or policy-based, should be applicable in all areas.

Nothing could be further from the truth. Clearly, the strategy for securing the modern grid requires significant utilization of information security technology, security research, information-sharing capabilities, and the integration of these in a manner that meets the challenges associated with current and future power delivery requirements.

To that end, it becomes important to understand that many of the cybersecurity vulnerabilities in the bulk power system that were once only theorized, have indeed been proven. Sometimes the risk is connected to the core technology, vulnerabilities in hardware, and software and various protocols, can manifest in a multitude of attack vectors, even ones that could involve the compromise of large aggregated systems that could impact millions of consumers simultaneously.

But as researchers and subject matter experts, our ability to communicate findings in a broad and effective manner is often impeded by the absence of an effective information sharing system. Thankfully, there is good work being done today that can be leveraged for a secure grid tomorrow.

We have seen the NERC standards in action, reducing some cybersecurity risk profiles by orders of magnitude.

We have seen the creation of non-invasive security assessment tools that create usable guidance for securing energy management systems. We have seen extensive energy sector road maps that have provided for the creation of technologies that can be used for security of electricity domain.

As proven time and time again, there are public-private partnerships already in place contributing to the mitigation of security threats to the bulk power system. Rather than develop new plans that are tied to more aggressive standards and enforcement, we need to ramp up the efforts in place now and support the continuation of what has been proven to work.

I feel that there are three areas that should be focused on to meet the emerging security challenges; research, improved standards, and procurement language.

First, research, the research effort regarding the cybersecurity of the bulk power system needs to be expanded and nurtured. A sanctioned activity that promotes the independent assessment of power system technologies without the risk of legal retaliation or negative attribution is necessary.

In essence, cybersecurity's researchers must be protected. This research must also include information sharing and cyber incident response functions so that we can better prepare for, detect, and respond to incidents unique to bulk power system architectures.

Second, refining standards, the continued development of cybersecurity standards for grid elements is required. This effort should leverage standards that are already in place and accepted by the national and international community of stakeholders.

These standards should be updated to be more flexible so that they can accommodate shared threat and vulnerability information, but not so flexible to allow for erroneous reporting regarding critical assets and cyber assets. The standards should also incorporate instruction regarding how to implement emergency orders related to specific and imminent cyber attacks.

Third, for procurement guidance, this public-private activity should leverage the existing body of work done for industrial control systems and enhance it with sections tailored to the electric sector. Simple refinement of existing procurement guidelines can have a tremendous influence in bulk power system cybersecurity and it can be done immediately.

To the committee, Madame Chairwoman, Ranking Member, I thank you for this opportunity to testify here today and I commend you on your attention to this very important matter. I will be more than happy to answer any questions you may have at this time.

[The statement of Mr. Fabro follows:]

PREPARED STATEMENT OF MARK FABRO

JULY 21, 2009

Madame Chairwoman and Ranking Member, thank you for the opportunity to testify today before the Homeland Security Subcommittee on "Securing the Modern Electric Grid from Physical and Cyber Attacks."

My name is Mark Fabro and I am the president and chief security scientist of Lofty Perch, a company focused on providing cybersecurity services to critical infrastructure organizations such as those in the energy, water, transportation, and oil and gas sectors. I am a member of the Utilities Telecom Council Smart Networks Security Committee, the chairman of the Canadian Industrial Cyber Security Council, and co-chair of ISA SP99 Working Group 10: Governance and Metrics for Industrial Automation and Control Systems Security. For the last several years I've been a subject matter expert supporting the industrial control systems cybersecurity research effort at the Department of Energy's Idaho National Laboratory, as well as the efforts spearheaded by the Department of Homeland Security and the Control Systems Security Program. I have authored several key Recommended Practices for securing industrial control systems, and have participated in the development of specific guidance as it pertains to securing information technology in critical infrastructure systems. My professional experience has provided me the privilege of performing extensive cybersecurity research as it applies to the electric sector, and I have been involved in a multitude of assessments specifically performed to determine the cybersecurity of critical elements of the bulk power system.

I want to be clear in stating that my testimony today is based on my opinions and mine alone. This testimony was generated using my experiences in working with sector-specific organizations as well as many utilities, researchers, and other international government entities facing the same challenges regarding cybersecurity and the electric utility industry. My comments are based on my experience in working with stakeholders, asset owners, vendors, and from detailed cybersecurity assessment work specific to the electricity sector. I also want to state that I have reviewed and assessed material from other industry and subject matter experts who specialize in the field of cybersecurity for electric grid systems, and have vetted my concerns with them to ensure the committee is empowered with actionable intelligence.

BACKGROUND AND PROBLEM STATEMENT

As we look inwards to the Nation's vital information systems, such as those responsible for maintaining our most essential infrastructures, we continue to see, as Madame Chairwoman said in her March 10, 2009 opening remarks, "too many vulnerabilities existing on too many critical networks which are exposed to too many skilled attackers who can inflict too many damages to our systems." The statement is chillingly accurate and has specific applicability to the North American power grid. There is no doubt as to whether or not our electric infrastructure will continue to converge with internet-based systems, and as it matures it will inherit cybersecu-

rity vulnerabilities. As an example we are well on our way to seeing Smart Grid happen; it has already been proven to be successful in many cities and funding has been allocated to make it a proven reality. Our challenge is to ensure that as we go forward we have done our due diligence in proving these solutions as secure and reliable, and that we protect what may be the most vital of all critical infrastructures.

In the last several years the rate at which critical infrastructure entities have embraced modern information technology to enhance their business operations has been staggering. This activity is of course a natural progression, as a considerable portion of the Nation's critical infrastructure systems have been found to be significantly aged, have been built with a single purpose in mind, and deployed assuming isolation by both physical and technological means. In an ever-changing environment that demands businesses operate better, faster, and more efficiently these characteristics clearly showcase a need for modernization. With the President directing the National Security Council to undertake a 60-day review of the U.S. approach to cybersecurity it is important to recognize that the issues related to the national critical infrastructure are being investigated, and measures to protect vital systems are going to be done not unilaterally but with the cooperation of allies. Recently proposed bills have specific intent on augmenting current responsibilities as they pertain to protecting the bulk power system from cyber attack, as well as refine security and intelligence practices to specifically address cyber threats and vulnerabilities to the power grid. Congressional hearings have done an excellent job at highlighting the cybersecurity issues associated with the industrial control systems running our infrastructure, and the release of Smart Grid stimulus funds being conditional on cybersecurity plans showcases that the issues regarding cybersecurity are penetrating relevant communities of concern.

But the findings and risks regarding cybersecurity are not ubiquitous across all entities supporting the bulk power system. Moreover, they are not unique to a single country, they are not unique to a single type of entity, and they most certainly are not indicative of an overall "generally poor" security posture. We continue to witness excellent examples of effective cybersecurity activities from many entities, both large and small, and continue to see progress that does not align with the popular opinion that the bulk power system is ripe for total cyber compromise.

Unfortunately, regardless of how driven we are to address and mitigate the larger cybersecurity problem, there is almost an unavoidable introduction of cybersecurity vulnerabilities into grid-related elements. This problem is of course exacerbated by the cultural impediments that often drive reticence and the uncooperativeness of infrastructure asset owners to address cybersecurity. Issues with interdependency and cross-sector reliance mean that a single weak link in the cybersecurity chain is a very influential one, and an attack on even the smallest participant can have national impact. As interoperability is the cornerstone of the bulk power system, we need to ensure our current solutions and path forward are paved with the useable safeguards we implement today. Indeed, robust situational awareness and a cohesive response plan are necessary components within any cyber risk reduction plan, but we must not forget that a majority of the North American critical infrastructure is not owned or operated by Government. As such, an understating of the real cybersecurity issues within the electric sector community, including those related to culture, multi-national interdependency and legacy operations is a fundamental requirement in protecting the power grid.

Extensive research has been done regarding the risk associated with migrating critical infrastructure systems over to modern IT architectures, with some specific material focused on industrial control systems. Numerous organizations, within both the public and private sector, have for years recognized this problem and have established several watershed efforts to meet the ever-changing challenges associated with this very important issue. However, resulting efforts have been disparate in nature, and only manage to accommodate the needs of certain communities of interest and not the Nation as a whole. As the protection of the North American bulk power system is not only a national issue it is a multi-national issue, we need to ensure our efforts become unified and provide consideration for the diversified stakeholders dealing with this problem.

KNOWING THE RISK

Of all the 18 critical sectors recognized by DHS, the security and reliability of the bulk power system could be considered the most critical. Studies have repeatedly shown that the ability for the other 17 to function properly depend on its availability. The realization that the grid is vulnerable to cyber attack is not new, as more than 12 years ago the National Security Telecommunications Advisory Com-

mittee's Information Assurance Task Force cited numerous electronic security incidents and threats to the grid. In their Electric Power Risk Assessment, the IATF referenced the possibility of electronic attack, cited technical hackers (including terrorists) as a threat, and cautioned on the pervasiveness of open source information that can facilitate the creation of target folders. At that time a majority of utility members agreed "that an electronic attack capable of causing regional or widespread disruption lasting in excess of 24 hours is technically feasible."[1] Today, we appear to be in the same position, and most would agree with the findings as if the report came out last week.

The complexity of the problem in trying to measure how "secure" or "resilient" the grid is from cyber attack cannot be overstated. Often, and erroneously, the cybersecurity problem is framed under the assumption that there is simply a single uniform "grid" and that a mitigation strategy, be it technical or policy-based, should be applicable to all areas. Nothing could be further from the truth. The processes and technology required to support the reliability and functionality of the bulk power system, across all entities and interconnects, is incredibly diverse. An immeasurable number of different vendor technologies, protocols, operating systems, communications media, and operating procedures simply cannot facilitate for a security "silver bullet" in either the policy or technology space. With the power infrastructure comprised of legacy systems that cannot provide for useable event data, and newer systems unable to be tuned to account for cybersecurity, it becomes very difficult to discern between inherent system irregularities and incidents generated by malicious cyber attack. Compounding the problem is the fact that modern cybersecurity technologies are not always adaptable to control system environments, as the need for perpetual system availability often precludes even the simplest countermeasure.

Clearly, the strategy for securing the modern grid requires significant utilization of energy technology, information security technology, research, and the integration of these in a manner that meets the challenges associated with current and future power delivery requirements. As the bulk power system does and will continue to depend on diverse information technology solutions, many of which possess inherent cybersecurity vulnerabilities, we must be diligent in understanding the cyber risk associated with critical cyber assets. The past several years have brought about a significant increase in attention to the issue of cybersecurity and industrial control systems as well as the development of enforceable cybersecurity standards for the electric sector entities. Indeed, the work both nationally and internationally has been substantial. It is no question that we as a society are committed to protecting the power grid. But it has become very clear that the security safeguards we have created are often not commensurate with the levels of protection required for a system with such high value. The economics associated with the energy business has in many ways threatened the potential of well-intended cybersecurity guidance, and perhaps may have contributed towards many of the recent incidents that precipitated this hearing and affiliated bills. We now know that we have a situation that, if left unattended, could have catastrophic results.

SPECIFIC SECURITY ISSUES

As a concerned community, we need to ensure that the issues regarding cybersecurity in the bulk power system are presented and studied in the appropriate light and not necessarily in the same context as cybersecurity for general IT systems. Accurately understanding the threats and vulnerabilities associated with the bulk power system will only serve to ensure that future State architectures will have the necessary countermeasures and mitigations properly embedded. To that end, it becomes important to understand that many of the cybersecurity issues in the bulk power system (including Smart Grid) that were once only theorized have indeed been proven. We have been able see the impact of hostile mobile code on nuclear facilities, witness hackers tunnel into distribution systems, create attacks that can take over a large metering infrastructure, and watch researchers create useable exploit code that is specific to a vendors industrial control system product. Although we see threats and malicious activity, we still lack reports of any cyber attacks that have directly impacted the bulk power system. Presenting these issues is not intended to instill fear or panic, nor is it intended to question the surety of our current and future grid plans as advantageous. Rather, they are presented to support the problem statement with facts that can be used to structure coordinated and effective mitigation activities. With proposals in place to possibly adjust the current

[1] National Security Telecommunications Advisory Committee Information Assurance Task Force "Electric Power Risk Assessment", March 1997, *www.solarstorms.org/ElectricAssessment.html*.

landscape of authority as it pertains to the cyber protection of the bulk power system, familiarization with some of the more core problems is required. It is intended that such a discussion can facilitate for a better understanding of key issues, thus empowering the committee to make informed choices going forward.

Many elements that make up the bulk power system are not secure from cyber events, whether they are of malicious intent or not. On a regular basis we see cyber incidents impact some aspect of our energy infrastructure, and as connectivity increases, along with hacker interest, we will continue to hear more. Sometimes the risk is connected to the core technology. The bulk power system can be disrupted by using attacks that neither NERC nor FERC can regulate, such as those that exploit vulnerabilities inherent in vendor technologies. Vendors that use a single security safeguard across their entire solution makes the attacker's work considerably easier, as the compromise of a single device can often mean a compromise of many devices in the command-and-control architecture. This is particularly applicable to Smart Metering, and to date various research teams have shown vulnerabilities that could be exploited across a metering infrastructure rendering the network inoperable (or under the control of an attacker). In some instances vulnerabilities exist within devices that have capability for remote disconnect, suggesting attacks could disable a metering infrastructure, impact utility load forecasting, and perhaps impact control. Remote disconnect capability can be deployed to the residential level as well, and compromised meters could lie dormant until a later date and be used to attack other devices or grid elements. One must consider what would happen in the event of an aggregated attack, where an attacker was able to compromise 5 million meters in a city-wide deployment, and suddenly render those 5 million endpoints off-line—what is the impact to the bulk power system when the load from 5 million residences suddenly vanishes? I do not know what that would look like in terms of grid coordination efforts but I know it would definitely be non-trivial and require some expensive investigation. Consumer trust in Smart Grid would surely be impacted.

New vulnerabilities in the embedded systems responsible for the availability and integrity of electricity operations continue to be discovered. An emerging security issues relates to how some critical field technology can be compromised by exploiting methods used for upgrading device firmware, such as those for substation and field operations. These attacks that can render the device inoperable, make the data collection/submission capabilities useless, or cause undesirable impact to control capabilities. Such an attack would significantly impact a utility's ability to provide market data, impact load forecasting, impact ability to accurately control load shedding operations, and possibly be used to force improper and unexpected load shedding.

By creating and deploying control system solutions that utilize commercial radio technologies with tunable antennas, the compromise of networked grid equipment with embedded vulnerable radios could lead to the creation of an unauthorized broadcast network, causing interference on almost any radio frequency. This could impact radio communications used by transmission operations, as well as integrated water and gas systems, transportation functions, and municipal emergency services. In addition to impacting electric grid control, the result could be millions of rogue radio transmitters broadcasting multi-frequency noise across the radio spectrum of a major urban metropolis, with the potential to jam vital infrastructure communications. This issue is in the same category as those vulnerabilities recently discovered that, if exploited, can lead to a persistent denial of service in some utility operations.

The suite of protocols that allow our bulk power system to work is an extensive one, but many of the more common ones have for many years been compromised and well understood by hackers and engineers alike. With common industrial control protocols now using modern IT protocols as the basis for communication, hacker tools and methods are easily used against critical infrastructure systems. Attacks that compromise availability, integrity, and confidentiality can easily be launched against infrastructure systems, and we cite examples such as the worm attack on the Davis-Besse nuclear plant and the hacker attack on the California ISO. Considering the fact that many major protocols were openly published (to meet interoperability needs), the practice of reverse engineering both proprietary and open protocols has also increased the overall risk to our grid operations. Many of the meshed networks designed to heal themselves and ensure system communications have been found to be vulnerable to attacks traditionally only known to the IT world. This vastly extends the scope of plausible attacks useable by adversaries, and could lead to the compromise of grid integrity, energy operations, load control, and critical energy infrastructure information.

Finally, there is risk associated with the deployment of secure solutions in an insecure manner, a concern shared by many operators within the bulk power system.

The problem is cultural, and is a residual effect from many decades of using control environments isolated from internet-based networks. Moving to new modern interconnectivity, supported by the economics associated with energy markets and customer satisfaction, assessments have shown that energy management and even maintenance networks can be quite insecure from a cyber perspective. Field engineers using unknowingly compromised service computers, wrought with insecure instant messaging and social networking applications have authoritative access to vital grid elements. These issues, along with requirements for corporate operations to have on-demand access to energy management systems, create new conduits for attackers. The weaknesses that exist in some power system deployments can also impact the entire information path from the SCADA systems to the consumer. In some cases, this has actually manifested in attackers compromising utility customer service web portals, and hacking back into the command function of the utility to cause loss-of-control situations in the energy management system.

We have seen numerous vulnerabilities in our own research environment, in the assessment environment, and even in emerging Smart Grid elements such as Advanced Metering Infrastructure, or AMI. In some cases, the results and findings are discouraging. Assessments and incident response repeatedly provide alarming information, such as proof of qualified threats looking to use cyber means to impact electric grid operations. As a researcher and subject matter expert, my ability to communicate findings in a broad and effective manner is often impeded by the absence of an information sharing system.

POSITIVE PERSPECTIVES

There is very good work being done today that needs to be leveraged for a secure grid tomorrow. We have seen the NERC standards in action that, when implemented, have reduced an entities risk profile by orders of magnitude. We have seen the creation of non-invasive assessment tools and techniques that create useable guidance for securing energy systems. We have seen extensive sector-specific cybersecurity roadmaps that have provided forums for the creation of technologies that can be used in the energy domain. As an example, we have the knowledge and technological capability to shape an early detection and warning system that could be tuned for the bulk power system elements, as we have seen small-scale solutions deployed with great success. We have proven case studies that can be used to build effective "deter" and "detect" capabilities ones that can perhaps add completeness to a unified "respond" function. And, as is proven time and time again, the public/private partnerships are in place to ensure cooperative capabilities in mitigating security threats to the bulk power system on North America.

Even though we had warnings in the mid-1990's, in the last 12 months we have gone from simply knowing about the security concerns of the bulk power system to a widespread understanding that vulnerabilities have and continue to be exploited by adversaries. The problem has manifested to the point that DHS, DOE, and members of the defense and intelligence community have taken an interest. We are trying to categorize the threat and use our traditional analysis methods to fit our data into the boxes we are comfortable with. However, we need to ensure the tactical strategy for defending our bulk power system does not require a development runway so long it precludes us from defending against the threat today. To ensure we are successful in creating security mandates and mobilizing any response capability we need to leverage what is working presently. We do not have the luxury of time; we need to leverage and support existing efforts and public/private programs that are already established and move forward as opposed to sideways.

Many experts suggest that the realization of a secure bulk power system is "blue sky" wishful thinking. But to say that "Secure Power Grid" is an oxymoron is a dangerous and erroneous statement. The electric power industry regularly protects the bulk power system using advanced coordination and seamless response activities. Present-day capabilities, research initiatives, and subject matter expertise continues to facilitate for effective and self-sustaining solutions to ensure security in electric sector deployments. With appropriate direction, support, and funding the community of interest is more than capable to address these issues and provide for secure solutions. Much work has been done across the stakeholder community, and we need not start from zero. The required direction to mitigate the security vulnerabilities that could have an adverse effect on the bulk power system is well within our reach. Rather than develop new plans that are tied to more aggressive standards and enforcement we need to ramp-up the efforts in place now, and support the continuation of what has been proven to work. New activities that will attempt to create a secure energy infrastructure through hyper-rigorous compliance mandates is not the right approach. In the past we have seen how the process for

instantiating new mandates can bring progress to a grinding halt, and any new changes could actually reduce the security posture of the electric system while entities struggle to align with new directives. The stakeholder community may be very unreceptive to new instruction and mandates, especially if it could make their historical progress obsolete.

SUGGESTIONS FOR A PATH FORWARD

While many programs exist that can support a better understanding of how to address these issues, certain activities must be undertaken to ensure success in protecting key assets. I feel that there are three primary areas that must be focused on to meet the current and emerging challenges associated with protecting the bulk power system from cyber attack.

First: SUPPPORTED RESEARCH

The research function regarding the cybersecurity of the bulk power system needs to be expanded and nurtured. As in the traditional IT domain, having well-funded and approved research is vital in making sure the user community is safe from malicious cyber attack. A supported and sanctioned activity that promotes the assessment of vendor technology without the risk of legal retaliation or negative attribution is necessary. In essence, the cybersecurity researchers focusing on critical infrastructure must be protected and, whenever possible, empowered by having their efforts embraced by vendors and asset owners alike. This would of course contribute to the existing work being done through public sector initiatives. Working to remove the hurdles that prohibit cybersecurity testing for electric system solutions will dissolve a shroud of secrecy that provides for the ever-failing "security through obscurity". Believing threat actors do not know how a system works is no grounds to assume it is secure. With a wide range of on-line auctions that can be used to purchase systems that are identical to what we would call critical assets, we need to enroll our best minds, including private researches, to stay ahead of the threat. This research will provide additional value to those vendors that have long understood the impact of cybersecurity on critical infrastructure, as well as assist those that are new to the domain and need support in understanding the impact insecure solutions can have. This would provide specific value to the Smart Meter arena. A coordinated research effort between vendors, researchers, and utility operators would help precipitate mitigations that would maximize our own security postures and allow for easy integration into electric system solutions. Failure to do so simply provides the adversary with an advantage, and hinders our ability to proactively protect our assets. This research must also include the updating of information sharing and cyber incident response functions so that we can prepare, detect, and respond to cyber incidents unique to our bulk power system architectures. This action can be put in place today by leveraging existing public/private programs, with assurances that the research activities to date can be used to help protect the solutions being manufactured for delivery in the very near term.

The committee is encouraged to support the existing frameworks that can promote cybersecurity research for electric grid elements, and have it defined in such a way that both researchers and vendors are driven by appropriate incentives to promote the discovery and mitigation of cyber vulnerabilities. Specific technological security testing, perhaps under Cooperative Research and Development Agreement initiatives, could augment the analysis and processing of cybersecurity incidents that impact the bulk power system. When permitted, the inclusion of results from Federal research, such as that done by DOE, will provide significant value to the library of useful findings. As the issues of cybersecurity and the power grid are not unique to the United States, efforts to maximize the sharing of threat information among allies can only help to precipitate better understanding. The committee is also encouraged to facilitate these cooperative efforts by appointing a non-regulatory lead organization within the Federal Government to coordinate current research efforts, manage relationships and, when feasible, ensure existing public/private efforts can implement actions defined by research findings.

Second: REFINED STANDARDS

The continued development of cybersecurity standards is required to be the baseline for driving definitive specifications to protect grid elements, and to date we have working standards that are in effect across the sector. With such a broad scope of critical component functions, standards that define interoperability safeguards must also be provided. Standards must continue to be developed and improved with full support and contribution from the stakeholder community both nationally and internationally. Most importantly, these standards should be flexible to accommodate for refinement based on threat information, but not so flexible that it facilitates

erroneous reporting regarding critical assets and cyber assets. The reliability and security of the bulk power system is the responsibility of the United States, Canada, and Mexico and as such these standards must be enforceable by an integrated an overarching entity that can support emergency orders swiftly and with authority. The standards should also have applicability to the vendor community, allowing vendors to be empowered with guidance as it relates to building secure energy management technology solutions from the start. This must be provided so that vendors can insert cybersecurity into their Systems Development Life Cycle, and ensure security is built in to the solutions proactively. As many experts agree that the fear of regulation or audit greatly exceeds the fear of security breach, we must be careful of creating standards that move organizations in a direction opposite to a secure path, as we have witnessed instances where adherence to strict regulations actually decreases the cybersecurity posture of an entity.

These cybersecurity standards developed must take into consideration current and future states regarding threat intelligence, cyber incident reporting, control systems cybersecurity, and legal frameworks for information sharing. As such, an effective capability on sharing cybersecurity vulnerability and threat data as it relates to the critical electric infrastructure is required. This capability should support a Federal entity responsible for providing accurate and timely data on specific and imminent cyber threat. With that, sanitized information products can then be used to improve standards and proactive defensive activities. Of vital importance is that these improved standards must facilitate for better information sharing within the stakeholder community.

These standards must support a divergence from a culture based simply on compliance and towards one founded on the measurement of adherence to research-based best practices. The improved standards, using the stakeholders as leadership and critics, would also help maintain the tremendous success seen in private sector voluntary actions.

Third: PROCUREMENT GUIDANCE

To support utilities and asset owners acquiring and deploying secure electric system solutions, specific procurement guidance language should be developed. Such language will be a valuable facilitator that will drive vendors and asset owners to work together. This cooperative activity will help shape bulk power system technology cybersecurity requirements that can help make informed choices leading to better procurement. This public/private activity should leverage the existing body of work done for industrial control systems and enhance it with sections tailored to the electric sector.

Leveraging the existing procurement language developed to assist in the evaluation, development, and purchase of secure industrial control systems, the guidance to assist in selecting secure gird architecture elements, such as AMI, substation, and transmission elements, can be created using efforts by vendors, security researchers, and results from Government-led initiatives. It has been verified that vendors find such a language very useful to ensure future business, as it will guide them to develop secure solutions consumers clearly want and need. As proven in the control systems domain, inherent security becomes a market differentiator for the community as a whole, and that can lead to a better and more secure infrastructure. In this case, moderate re-engineering of existing procurement guidelines can have a tremendous downstream influence in bulk power system cybersecurity, and it can be done immediately. Recent advances in Smart Grid and Smart Metering cybersecurity, such as that done by AMI–SEC Task Force, UtiliSec, and NIST, could be easily incorporated.

Madame Chairwoman, Ranking Member, and the entire committee I thank you for this opportunity to testify here today. I would be happy to answer any questions you may have at this time.

Mr. THOMPSON. Thank you very much. The Chair now recognizes Mr. Assante for 5 minutes.

STATEMENT OF MICHAEL J. ASSANTE, CHIEF SECURITY OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. ASSANTE. Thank you. Madame Chairwoman, Chairman of the full committee, Ranking Member, Mr. Lungren, Members of the subcommittee, my name is Michael Assante, I am the chief security officer of the North American Electric Reliability Corporation.

As a designated electric reliability organization in the United States, and much of Canada, our responsibility and we are dedicated to doing so, is to ensure reliability of the bulk power system. This is a very sobering responsibility, especially in light of the comments today.

The last time our organization testified before this subcommittee, we committed to improving our response to cybersecurity. I am here confidently to report that we have done so, but we realize there is much more work to be done.

Cyberspace is proving paramount, both as a national and an economic security issue. The compromise of our national through this invisible battleground has cost billions of dollars from our economy in terms of theft of both intellectual property and the destruction of information systems.

Even though NERC is not aware of any cyber attacks that have directly affected the reliability of power systems in North America, we have no illusions of immunity, as we are well aware of both Government systems and business systems that have been successfully attacked at home and power systems that have been disrupted abroad.

The United States and Canada must be ready to act in the event of a specific and imminent cyber threat. We believe there is an important gap in authority when it comes to these emergency situations in the United States, and additionally, emergency authority should be put into place and put into place soon.

NERC and the electric sector have been working to answer President Obama's broad call to action, stemming from a 60-day cyber study completed in May 2009 and we are preparing for Canada's forthcoming national strategy and action plan for critical infrastructure and a national cyber strategy.

Some of these efforts include on-going revisions to NERC cybersecurity standards with the goal of building a stronger foundation. Phase 1 of these revisions was submitted to FERC for approval in May. Work on additional Phase 2 revisions continues and we are about to complete a thorough evaluation of how we can incorporate portions of this framework into the NERC standards.

I personally believe another important element of the revisions will be to consider how best to construct broad requirements for training and awareness programs, in incident response and reporting, to apply to all entities of the bulk power system.

We have also instituted and improved our voluntary alert mechanism, whereby NERC is able to reach nearly 5,000 professionals in control rooms, power plants, and engineering centers across North America within hours of being informed of a vulnerability, or a threat. NERC has issued nine such alerts over 2009.

Efforts also include expanded work on further assessments and deeper analysis of risk. NERC's cyber risk preparedness assessment, conducted in close coordination with the industry, is designed to evaluate the preparedness in dealing with challenging cyber threats.

While the pilot group will be small, the goal of this assessment is to develop a toolkit for entities so that they may assess their ability across the industry.

NERC is also partnering with the Department of Energy in a very important effort to breathe new life into the previous work to address high-impact, low-frequency risks, such as space, weather, electromagnetic pulse, and pandemics. Many of these are focused on cybersecurity risks, but physical risks in the security of the power system are a very real concern.

Our understanding, system redundancies, coupled with existing authorities far exceed what is in place to address a very structured and well resourced cyber adversary.

The threat is like no other, and to demonstrate my point, I will compare it to the rash of German U-boat attacks in the coastal waters surrounding the United States that begin in May 1942 and lasted for almost a year.

The submarine threat was a mysterious one, much like the ever-present but more deeply mass cyber attacks of today. The threat is playing out beneath the cyber seas, but unlike submarine warfare it has not stopped at our shoreline, attackers are able to strike without being in harm's way.

Cyber weapons are often not flagged and their true origins are unknown and therefore unattributable, and most importantly, they have been largely successful in evading the instruments available to prevent and deter it.

This is the risk to the power grid, that is the interconnective system of wires, power plants, and digital controls is still evolving, is still not yet fully understood. The potential for an intelligent attacker to exploit a common vulnerability across the system and impact many assets at once and from a distance is one of the most concerning aspects of this challenge.

This is not unique to the electric sector, but addressing it will require better intelligence, and new thinking, on top of sound operating and planning analysis. Complicating this issue, much of the information about security-related threats remain classified in Government communities, with restricted opportunity to share information with affected asset owners.

From a regulatory perspective, NERC believes the scope of Section 215 of the Federal Power Act, under which NERC both develops and enforces mandatory standards, appropriately places the focus on ensuring the security and reliability of the bulk power system.

With that said, the increasing adoption of Smart Grid technology, such as advanced metering systems in the distribution grid, has come with the need to build in more security and flexibility to mitigate the emerging risk of exploring this new connectedness.

While a single device in the distribution system will not be considered material to the bulk power system reliability aggregate, these assets may become material. There capricious magnitude of the priority of the issue at hand, and supports enacting legislation to address this. Moving forward, NERC is committed to complementing any Federal authority to address cybersecurity challenges, regardless of the form it takes. Thank you.

[The statement of Mr. Assante follows:]

PREPARED STATEMENT OF MICHAEL J. ASSANTE

JULY 21, 2009

INTRODUCTION

My name is Michael Assante and I am the chief security officer for the North American Electric Reliability Corporation ("NERC"). As the designated Electric Reliability Organization ("ERO") in the United States and much of Canada, NERC is dedicated to ensuring the reliability of the bulk power system in North America. As part of our mission, NERC evaluates, assesses, and works with industry to address risks to the bulk power system through study, information sharing, and, where appropriate, mandatory standards. Cyber- and physical security are two such risks.

The last time our organization testified before the subcommittee, we committed to improving our response to cybersecurity. I am able to confidently report that we have done so. We certainly have more work to do, but NERC and the industry have made encouraging progress on this issue since May 2008. My testimony today will provide an update on our activities, and will also provide some important perspectives for your consideration as you continue your vital work on this subject.

Notably, NERC firmly believes that additional, Federal authority is needed to address specific and imminent cybersecurity threats to the bulk power system.

RISKS TO THE BULK POWER SYSTEM

Cyber- and physical security are two of many reliability risks faced by bulk power system planners and operators.

Unlike other concerns, such as extreme weather, security-related threats can be driven by malicious actors who intentionally manipulate or disrupt normal operations as part of a premeditated design to cause damage. Cyber-related threats pose a special set of concerns in that they can arise virtually anytime, anywhere and change and emerge without warning.

While the industry deals with some physical security events, like copper theft, on a regular basis, other technical threats or hazards, such as electromagnetic pulse and space weather, are a concern and will require careful consideration to develop appropriate and effective mitigations. Cyber threats to control systems are still evolving and are not yet fully understood. The potential for an intelligent attacker to exploit a common vulnerability that impacts many assets at once, and from a distance, is one of the most concerning aspects of this challenge. This is not unique to the electric sector, but addressing it will require asset owners to apply additional, new thinking on top of sound operating and planning analysis when considering appropriate protections against these threats.

Complicating this issue, much of the information about security-related threats remains classified in the defense and intelligence communities, with restricted opportunity to share information with affected private-sector asset owners. The electric grid is placed at significant risk as a result of limited information-sharing. NERC is not aware, however, of any cyber attacks that have directly affected the reliability of the power system in North America to date.

NERC is presently working to expand the body of analysis of physical and cybersecurity risks on an industry-wide basis. These efforts include analysis and consideration of specific risks and vulnerabilities as they are identified by a group of security experts from industry, security researchers, and technology vendors, dubbed "Network HYDRA". This networked group of professionals provides important insight, feedback, and a communications vehicle to raise awareness of important security concerns.

Non-traditional risks are also the subject of a working group NERC has recently established in partnership with the Department of Energy to analyze "high-impact, low-probability" risks—or, more accurately, those risks whose likelihood of occurrence is uncertain relative to other threats, but that could significantly impact the system were they to occur. Officially launched on July 2, this working group will examine the potential impacts of these events on the bulk power system, focusing on influenza pandemic, space weather, terrorist attacks, and electromagnetic pulse events. The group will host an invitation-only workshop in the coming months to discuss their assessment and develop conclusions and recommendations to industry based on their work. These recommendations will be used to drive needed technology research, development, and investment and also to evaluate NERC's current standards and initiatives, potentially driving the creation of new standards to address these issues.

In addition to these on-going efforts, NERC is conducting a Cyber Risk Preparedness Assessment. This industry-led, voluntary assessment will focus on detection,

response, and mitigation capabilities for cyber incidents. Coordinated by NERC, the assessment will look beyond NERC's current cybersecurity standards for practices, procedures, and technologies that contribute to cyber preparedness across the industry. Generalized, aggregated results from the assessment will be used to inform standards development activities, alert the industry to potential areas of concern, and identify areas where research and development investment is needed. For security reasons, specific results of the assessment will remain confidential, a key condition of participation in the program.

Through these and other, more specific assessments, NERC seeks to broaden the understanding of cyber risk concerns facing the interconnected bulk power system and guide industry-wide efforts to develop prudent approaches to address the most material risks—in both the short-term, through appropriate alerts, and longer-term, through appropriate standards.

SCOPE OF NERC AUTHORITY

The scope of NERC's authority as the ERO is limited to the "bulk power system," as defined below in Section 215(a)(1) of the Federal Power Act:

"(A) Facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

"(B) electric energy from generation facilities needed to maintain transmission system reliability.

"The term does not include facilities used in the local distribution of electric energy."

This authority places appropriate focus on the reliability of the bulk power system, as outages and disturbances on the bulk system have the potential for far greater impact than those on distribution systems. Elements of the power grid outside this authorization include telecommunications infrastructure and "local distribution," which typically includes the infrastructure within urban areas and that serves many military installations.

The increasing adoption of "Smart Grid" and advanced metering systems on distribution systems has brought renewed focus to the appropriate definition of a bulk power system component. As grid operators rely on demand-response, rooftop solar panels, and other distribution-level assets in capacity planning and operation, the reliability of the bulk power system may become increasingly dependent on the operation of assets connected at the distribution level. While a single device would not be considered material to bulk power system reliability, in aggregate, these assets may become critical to the bulk power system.

As a result, NERC is working with the National Institute of Standards and Technology ("NIST"), the Department of Energy ("DOE") and the Federal Energy Regulatory Commission ("FERC") as security and interoperability standards are developed for "Smart Grid" technologies. Additional efforts at NERC include high-level assessment by several working groups. NERC's technical committees are presently considering the formation of a "Smart Grid Task Force" to further evaluate these issues.

NERC MANDATORY RELIABILITY STANDARDS & COMPLIANCE

Developing mandatory standards that apply to the more than 1,800 diverse entities that own and operate the North American bulk power system is a complex undertaking. Standards must apply equally to companies with thousands of employees and to those with only 20. Additionally, the standards must not do harm. They must take into account unique component configurations and operational procedures that differ widely across the grid. Given our extensive experience in standards development, NERC firmly believes the level of expertise needed to create standards that achieve security objectives and ensure reliability can best be found within the industry itself.

NERC develops all its Reliability Standards through an ANSI-accredited process, which we believe provides the appropriate framework for ensuring that subject matter expertise is used to create and vet the standards. Though use of an ANSI-accredited process is not specifically required, the Federal Power Act does specify that the standards development process must "provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards . . . ." (Sec. 215(c)(2)(D)).

In certifying NERC as the ERO, FERC found that NERC's ANSI-accredited standards setting process meets these requirements. The standards development process is set forth in NERC's Rules of Procedure, which FERC has approved.

The ANSI-accredited standards development process has yielded important results as NERC has revised its Critical Infrastructure Protection ("CIP") Reliability Standards over the past year. NERC's Board of Trustees approved revisions to eight

of the nine currently-approved CIP Reliability Standards on May 6, 2009, after the standards passed industry balloting with an 88 percent approval rating. The high approval rating indicates the industry's strong support for these development efforts, which has been vital to their success.

These revised standards were filed with FERC for regulatory approval in the United States on May 22 and are already mandatory and enforceable in parts of Canada.

NERC's Critical Infrastructure Protection standards fill a specific role in the protection of the bulk power system. The standards are comprised of roughly 40 specific requirements designed to lay a solid foundation of sound security practices that, if properly implemented, will develop capabilities needed to defend critical infrastructure from cybersecurity threats. The standards are not, however, designed to address specific, imminent threats or vulnerabilities.

Work on additional, phase-two CIP standards revisions continues, with initial industry validation on track for the fourth quarter of 2009. Modifications underway as part of the phase-two revisions include considering the extent to which elements of the Recommended Security Controls for Federal Information Systems under development by NIST can be incorporated into the CIP Reliability Standards. Also under consideration are broader foundational requirements for training and preparedness, specifically with applicability to entities who do not own or operate Critical Assets.

Additional modifications underway in this phase-two development work were the subject of a letter I sent to industry stakeholders on April 7, 2009. The letter addressed the identification of Critical Assets and associated Critical Cyber Assets that support the reliable operation of the bulk power system, as required by NERC Reliability Standard CIP–002–1. The letter was based on initial data collections NERC has used to evaluate the implementation of the standard across the industry prior to the start of formal audits, which began for some entities on July 1, 2009. The appropriate prioritization of assets for protection is a critical component of a successful security strategy, though its implementation poses a significant challenge to industry given the complex nature of the system and the changing nature of cyber threats.

In my April 7 letter, I called on users, owners, and operators of the bulk power system to take a fresh look at current risk-based assessment models to ensure they appropriately account for new considerations specific to cybersecurity, such as the need to consider misuse of a cyber asset, not simply the loss of such an asset. The letter is part of the iterative process between NERC and industry stakeholders as we work together to improve reliability. In this case, NERC gathered information about the status of implementation of the critical infrastructure protection standards and fed that information and its own insights back to the industry as part of a cycle of continuous improvement.

This effort demonstrates that NERC is working to address a critical element of the cybersecurity challenge: The educational learning curve and resulting compliance-related challenges that must be addressed to improve the cybersecurity of the bulk power system. Ensuring that each of the more than 1,800 entities that own and operate components of the bulk power system understands cybersecurity and the efforts needed to adequately protect the security of the bulk power system has been a priority for NERC.

The standards development and improvement process is producing results; however, NERC recognizes this process is not well-suited to addressing more imminent threats. As a result, NERC has been working with its stakeholders over the past year to develop and vet an alternate process for standards development to address imminent needs. This process is nearing completion and is expected to be submitted to FERC for approval before the end of the year.

ADDRESSING IMMINENT THREATS

At NERC, we are working in a number of areas to help provide or assist in the provision of the kinds of information that will help the industry better secure critical assets from advanced, well-resourced threats and other known cyber activity on an on-going basis. Strong and proactive participation by industry volunteers thus far has been encouraging.

In these efforts, NERC collaborates with DOE and the U.S. Department of Homeland Security ("DHS") on critical infrastructure and security matters on an almost daily basis. Additionally, NERC serves as the Electricity Sector Information Sharing and Analysis Center ("ES–ISAC"), which is responsible for promptly analyzing and disseminating threat indications, analyses, and warnings to assist the electricity industry.

NERC has in place a formal mechanism for issuing alerts to the industry about important matters that come either from NERC's own efforts, identified vulnerabilities or attacks, or from Government agencies with specific information about possible threats. Alerts issued through this mechanism are not mandatory and cannot require an entity to perform tasks recommended or advised in the alert. NERC has significantly improved this system over the past year and continues improvements through the development of a secure alerting portal, due to be complete this fall.

NERC is now able to provide timely, critical reliability information to nearly 5,000 security and grid operations professionals within minutes, and has demonstrated success by conducting training and using the system to send alerts, record acknowledgements and receive responses within several days. NERC has issued nine such alerts in 2009, with its most recent "recommendation" receiving a 94 percent response rate. The industry has been very supportive as we have worked to improve this process.

NERC's recent work to alert the industry of the Conficker worm, including lessons learned on mitigation, involved the issuance of one recommendation, two advisories, and an awareness bulletin over the span of 6 months. These efforts significantly contributed to overall preparedness and awareness of the underlying vulnerability and cyber threat.

We acknowledge and believe, however, that there are circumstances where NERC's efforts will not be adequate to identify or address specific imminent threats. Threats like those suggested by the April 8 Wall Street Journal article discussing the existence of "cyber spies" in the electric grid, for example, have been challenging for the industry to fully evaluate and address. Without more specific information being appropriately made available to asset owners, they are unable to determine whether these 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 to and understood by asset owners and operators in order to mitigate or avert cyber vulnerabilities.

NERC and the electric industry have been working closely in confidence to evaluate threats such as those described in the article. Specific information about these efforts is bound by confidentiality agreements.

EMERGENCY FEDERAL AUTHORITY NEEDED

Preparedness and awareness efforts like the assessments, alerts, and standards discussed above are necessary, but not sufficient, to protect the system against specific and imminent threats. NERC firmly believes that additional emergency authority is needed at the Federal level to address these threats, and NERC supports legislation that would give an agency or department of the Federal Government necessary authority to take action in the face of specific and imminent cyber threats.

For the reasons discussed above (that reliability standards must do no harm, take unique component configurations into account, and apply equally to all bulk power system entities—including those in Canada—regardless of size or structure), NERC firmly believes the level of expertise needed to create standards that achieve security objectives and ensure reliability can best be found within the industry itself. NERC believes an industry-based standards development process utilizing cross-border subject matter expertise will yield the best results for long-term reliability standards.

CONCLUSION

NERC, the electric industry, and the governments of North America share a mutual goal of ensuring threats to the reliability of the bulk power system, especially cybersecurity threats, are clearly understood and effectively mitigated. NERC has taken a number of actions to protect the bulk power system against cybersecurity threats and NERC will continue its work with Governmental authorities and industry stakeholders to do so. We believe these efforts have improved and will continue to improve the reliability and security of the bulk power system. We maintain, however, that these efforts cannot be a substitute for additional emergency authority at the Federal level to address specific and imminent cybersecurity threats.

NERC appreciates the magnitude and priority of this issue, and supports enactment of legislation to address this gap in authority as quickly as possible. Moving forward, NERC is committed to complementing Federal authority to address cybersecurity challenges, regardless of the form it may take. We commend this subcommittee for its action to date and look forward to supporting your efforts however possible.

Mr. THOMPSON. Thank you very much. Mr. Naumann, for 5 minutes.

STATEMENT OF STEVEN T. NAUMANN, VICE PRESIDENT, WHOLESALE MARKETS, EXELON CORPORATION; REPRESENTING EDISON ELECTRIC INSTITUTE AND ELECTRIC POWER SUPPLY ASSOCIATION

Mr. NAUMANN. Thank you. Chairwoman Clarke and Members of the subcommittee. My name is Steve Naumann, and I am vice president of wholesale market development for Exelon Corporation. Our utility companies serve 5.4 million customers in Chicago and Philadelphia.

I also serve as Chairman of the NERC Member Representatives Committee. As was noted, I am appearing on behalf of the Edison Electric Institute and the Electric Power Supply Organization. We appreciate the opportunity to testify about cybersecurity in a critical infrastructure on behalf of these organizations.

I would like to discuss three issues relating to securing critical electric infrastructure. First, the success of public-private partnerships in recognizing and addressing cyber threats and vulnerabilities; second, the need to avoid unintended consequences when implementing cybersecurity remedies; and third, policy proposals being considered by Congress and the administration.

The owners, operators, and users of the bulk power system take cybersecurity very seriously. To this end, as cybersecurity threats continue to evolve and our adversaries become more sophisticated, the public sector welcomes even more cooperation with, and information from, Government partners.

Both the Federal Government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attack.

Ideally, to ensure the cybersecurity of the Nation's electric grid and utilize the vast expertise of both public and private sectors, we need to, clearly, define these complementary roles and responsibilities while facilitating cooperation and information sharing between Government agencies and utilities.

Giving you an example of how Exelon operates, we address risks through a defense-and-depth strategy while balancing the considerations for consequences. This includes preventive monitoring and detective measures to ensure the security of our systems.

We regularly perform penetration tests to inform us of whether our preventative strategies are working so we can enhance our protection as technologies and capabilities evolve. These tests allow us to practice and enhance our monitoring capabilities while yielding lessons learned that are unique to our system.

But as was mentioned before, no two utility systems have identical network, hardware, or logistical strengths. No, single entity, will know the systems strengths or weaknesses like we do.

Going on to Smart Grid, one of the issues that was raised was the increased, possible, vulnerability of adding these devices to the distribution system. We believe it is very important to work with the manufacturers and the vendors to ensure that security is built into the devices and is upgradeable from the devices.

We would encourage the development of the security certification program, a good housekeeping seal of approval if you will, through which Smart Grid components and systems could undergo independent testing and receive that certification that security tests have been passed.

This would help the utilities differentiate among vendors to select those providing appropriate cybersecurity. The careful consultation with the electric utility industry helps ensure that Government intervention in protecting the grid from a cyber attack doesn't have unintended or harmful consequences.

As mentioned, the electricity grid is a complex system, there are certain measures that might prevent a particular cyber attack, could themselves, have adverse impacts to safe and reliable utility operation and service to customers.

For this reason, any new legislation that would give additional cybersecurity authority to a Federal agency should be limited to true national emergency situations where there is a significant national security or public welfare concern and should provide to the extent possible consultation with industry experts.

Congress should focus then, on what additional authority is needed in order to promote clarity and focus in response to imminent cybersecurity threats.

The Section 215, mandatory reliability framework, reflects years of work in broad consensus reached by industry and other stakeholders and is a good starting point to go by. EPSO and EEI and their member companies remain fully committed to work with the Government and the industry partners to increase security.

I appreciate the opportunity to appear today and would be happy to answer any questions. Thank you very much.

[The statement of Mr. Naumann follows:]

PREPARED STATEMENT OF STEVEN T. NAUMANN

JULY 21, 2009

Mr. Chairman and Members of the subcommittee: My name is Steve Naumann, and I am vice president for Wholesale Market Development for Exelon Corporation. I also serve as chairman of the member representatives committee of the North American Electric Reliability Corporation (NERC). I appreciate your invitation to appear today and the opportunity to testify about protecting the electric grid from cybersecurity threats.

Exelon is a holding company headquartered in Chicago. Our retail utilities, ComEd in Chicago and PECO in Philadelphia, serve 5.4 million customers, or about 12 million people—more than any other electric utility company. Our generation subsidiary, Exelon Generation, owns or controls approximately 30,000 MW of generating facilities, including fossil, hydro, nuclear, and renewable facilities. Our nuclear fleet consists of 17 reactors; it is the largest in the Nation and the third largest in the world.

I am appearing today on behalf of the Edison Electric Institute (EEI) and the Electric Power Supply Association (EPSA). Exelon is a member of both. EEI is the trade association of U.S. shareholder-owned electric companies and has international affiliate and industry associate members world-wide. EEI's U.S. members serve 95% of the ultimate customers in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry. EPSA is the national trade association representing competitive power suppliers, including generators and marketers. EPSA members own 40 percent of the installed generating capacity in the United States, providing reliable and competitively priced electricity from environmentally responsible facilities.

My testimony focuses on the nature of cybersecurity threats to the bulk power electric system and the efforts of electric utilities to respond to those threats. At the subcommittee's request, I also will share suggestions and observations regarding the

relationship between Government and the private sector in our efforts to secure the electric grid from cyber attacks.

I want to assure the subcommittee that as owners, operators, and users of the bulk power system, electric utilities take cybersecurity very seriously. We are actively engaged in addressing cybersecurity threats as they arise and in employing specific strategies that make every reasonable effort to protect our cyber infrastructure and mitigate the risks of cyber threats. As the industry relies increasingly on electronic and computerized devices and connections, and the nature of cyber threats continually evolves and becomes more complex, cybersecurity will remain a constant challenge for the industry. But we believe we are up to the task, building on our industry's historical and deep-rooted commitment to maintaining system reliability.

INDUSTRY STANDARDS, EMERGENCY AUTHORITY, AND LEGISLATIVE PROPOSALS

The industry believes it is appropriate for Congress to consider legislation providing the Federal Energy Regulatory Commission (FERC) new emergency authority to address imminent cybersecurity threats. I want to emphasize, however, that current law already provides the means to address many cybersecurity issues in the electric industry. Section 215 of the Federal Power Act (FPA), which was enacted by Congress as part of the Energy Policy Act of 2005, provides for mandatory and enforceable electric reliability rules, specifically including rules to address cybersecurity with FERC oversight.

The basic construct of the relationship between FERC and NERC, which FERC certified as the Electric Reliability Organization (ERO) under FPA Section 215, in developing and enforcing reliability rules is sound. In summary, NERC, using a well-defined stakeholder process that leverages the vast technical expertise of the owners, users, and operators of the North American electric grid (including those in Canada with whom we are interconnected) develops reliability standards, which are then submitted to FERC for review and approval. Once approved by FERC, these standards are legally binding and enforceable in the United States. NERC also submits these standards to regulatory authorities in Canada.

I suggest the question on which the subcommittee should focus is, "What additional authority should be provided to FERC in order to promote clarity and focus in response to imminent cybersecurity threat situations?" Legislation in this area should complement, not supplant, the mandatory reliability regime already established under FPA Section 215, and any new FERC authority should be appropriately narrow and focused only on unique problems that cannot be addressed under Section 215. The FPA Section 215 mandatory reliability framework reflects years of work and broad consensus reached by industry and other stakeholders in order to ensure a robust, reliable grid. It should not be undermined so early in its implementation.

Any cybersecurity legislation should promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures. Consultation is critical to improving cybersecurity.

Obviously, the scope of the damages that could result from a cybersecurity threat depends on the details of any particular incident. A carefully planned cyber attack could potentially have serious consequences. In considering the scope of damages that any particular cybersecurity threat might inflict, utilities must also consider the potential consequences caused by any measures taken to prevent against cyber attack. Certain measures that might prevent a particular type of cyber attack could themselves have adverse impacts to safe and reliable utility operations and service to electricity customers. Examples might include slower responses during emergency operations, longer times for restoration of outages and disruption of business operations dependent on internet access. That is why each situation requires careful consultation with utilities to ensure that a measure aimed at protecting the grid from a malicious cyber attack does not instead cause other unintended and harmful consequences.

Furthermore, every utility operates different equipment in different environments, making it difficult to offer generalizations about the impacts to the bulk power system or costs and time required to mitigate any particular threat or vulnerability. This complexity underscores the importance of consultation with owners, users, and operators to ensure that any mitigation that may be required appropriately considers these factors to ensure an efficient and effective outcome.

For the foregoing reasons, any new legislation giving FERC additional statutory authority should be limited to true emergency situations involving imminent cybersecurity threats where there is a significant declared national security or public welfare concern. In such an emergency, it is imperative that the Government provide

appropriate entities clear direction about actions to be taken, and assurance that those actions will not have significant adverse consequences to utility operations or assets, while at the same time avoiding any possible confusion caused by potential conflicts or overlap with existing regulatory requirements.

Because of its extraordinary nature and potentially broad impacts on the electric system, any additional Federal emergency authority in this area should be used judiciously. Legislation granting such authority should be narrowly crafted and limited to address circumstances where the President or his senior intelligence advisors determine there is an imminent threat to national security or public welfare.

PUBLIC-PRIVATE PARTNERSHIPS: COLLABORATION AND COMMUNICATION

The following comments address the specific issues raised by the subcommittee's invitation to testify regarding how Government and the private sector share information before, during, and after cybersecurity attacks.

Both the Federal Government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attack. The optimal approach to utilizing the considerable knowledge of both Government intelligence specialists and electric utilities in ensuring the cybersecurity of the Nation's electric grid is to promote a regime that clearly defines these complementary roles and responsibilities and provides for on-going consultation and sharing of information between Government agencies and utilities.

Information about cybersecurity vulnerabilities and attempts to exploit those vulnerabilities is shared with electric industry owners, users, and operators through a number of channels every day. Federal agencies that communicate this information to the private sector, such as the United States Computer Emergency Readiness Team (US–CERT), as well as cybersecurity hardware and software vendors, classify vulnerabilities in terms of the generalized risk to systems. Factors such as the seriousness of consequences of a successful attack, the sophistication required to conduct the attack, and how widely used the potentially affected assets are within an industry are used to rank vulnerabilities as "high", "medium", or "low" risk.

Fundamentally, however, the private sector can sometimes be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats because of inherent limitations on its access to intelligence information. The Government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. On the other hand, electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and we understand how our complex systems are designed and operate. Owners, users, and operators of the bulk power system are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation. Greater cooperation, coordination, and intelligence sharing between Government and the private sector should be encouraged, consistent with the public-private partnership model endorsed by the President's 60-day cybersecurity review.

Exelon, for example, is addressing the risks we know about through a "defense-in-depth" strategy while appropriately balancing considerations of potential consequences. This defense-in-depth strategy includes preventive monitoring and detective measures to ensure the security of our systems. We perform penetration tests where a contractor attempts to find and exploit vulnerabilities. The results of these regular penetration tests inform us about whether our preventive strategies are working so that we can enhance our protection as technologies and capabilities evolve. These penetration tests, which allow us to practice and enhance our monitoring capabilities, also yield lessons learned that are unique to our system. Because no two utility companies have identical network, hardware or logistical configurations, no single entity will know our system's strengths or weaknesses quite like we do.

NERC, which functions as the Electric Sector Information Sharing and Analysis Center (ISAC), disseminates alerts to provide information to the electric industry. With the input of its members, NERC has revised its procedures significantly over the past 2 years to improve the ability to quickly and securely provide this critical information to industry. This should ensure that when new vulnerabilities are uncovered, that users, owners, and operators will receive the needed information in a timely manner to take corrective action. Thus, we believe that the ISAC is providing timely and relevant analysis and alerts to the industry. Many of us have been frustrated with NERC's historically slow information-sharing process. I am pleased to note they have improved and we are getting information in a much more timely manner, though like anything else, there is always room for more improvement.

SMART GRID

As grid technologies continue to evolve and become "Smarter," they inevitably will include greater use of digital controls. Congress recognized the potential cybersecurity vulnerabilities, as well as benefits, that could result from greater digitization of the grid when it directed DOE to study these issues in Section 1309 of the Energy Independence and Security Act of 2007. Manufacturers of critical grid equipment and systems must fulfill their security responsibilities by adopting good security practices in their organizations, building security into their products, and establishing effective programs so that, as new vulnerabilities are discovered, they can inform customers and provide technical assistance with mitigation. As new Smart Grid technologies are developed, it is imperative for the industry to work closely with vendors and manufacturers to ensure they understand that cybersecurity is essential so that protections are incorporated into devices as much as possible.

It is equally critical that cybersecurity solutions be incorporated into the architecture being developed for Smart Grid solutions, so that the great benefits new Smart Grid technologies will provide are implemented in a secure fashion. With Smart Grid solutions in the early stages of development, opportunities exist to ensure this vision is fulfilled. EEI supports the process currently underway at the National Institute of Standards and Technology (NIST) to develop a framework of standards that will become the foundation of a secure, interoperable Smart Grid. It is imperative that NIST proceed boldly and expeditiously to establish standards applicable to all.

EEI is encouraging the development of a security certification program, through which Smart Grid components and systems could undergo independent testing and receive a certification that security tests had been passed. Such a program would help utilities differentiate among different vendor solutions to select those providing appropriate cybersecurity.

Finally, I would like to provide the subcommittee information on advanced metering implementation by Exelon's operating utilities. ComEd will be installing Advanced Metering Infrastructure under an Illinois Commerce Commission approved pilot program. PECO is installing Smart Meters in accordance with Pennsylvania law that requires distribution companies to deploy Smart Meters for all customers over 15 years. Cybersecurity has been a cornerstone of Exelon's Smart Grid/Advanced Meter Strategy from its inception in early 2008. Exelon understands and recognizes the potential risks associated with the deployment of such technologies throughout its service territories and treats cybersecurity with the utmost importance. To ensure security of these installations, Exelon is following internally developed security requirements and documenting them in requests for proposals to vendors for the supply of Smart Grid/Advanced Meter solutions. This includes the requirement to enumerate vendor security capabilities that ensures confidentiality, integrity, and availability. Exelon maintains a vulnerability management program which requires a documented penetration test to demonstrate that controls are implemented as designed. Third-party vendor audits are also performed to ensure vendor design & manufacturing controls are adequate. From an industry community and vendor perspective, Exelon is an active participant in the NIST Smart Grid Roadmap and Security Strategy development initiative and actively participates in other industry groups. ComEd and PECO will seek recovery of 100% of their costs of metering infrastructure in rate cases—as they do for all other infrastructure—except to the extent ComEd and PECO receive stimulus funding for advance meters. ComEd and PECO both plan to apply to DOE for Smart Grid Investment Grant (SGIG) funds to support their overall Smart Grid deployment efforts. Greater security is one of the benefits of the Smart Grid that DOE has articulated. Pursuant to this, SGIG applications are required to detail the cybersecurity implications of any project seeking funding. Cybersecurity has been a key consideration in the development of ComEd and PECO's Smart Grid plans and will be further detailed in their respective grant applications.

CONCLUSION

While many cybersecurity issues are already being addressed under current law, we believe it is appropriate to provide FERC with explicit statutory authority to address cybersecurity in a situation deemed sufficiently serious to require a Presidential declaration of emergency. In such a situation, the legislation should clarify the respective roles, responsibilities, and procedures of the Federal Government and the industry, including those for handling confidential information, to facilitate an expeditious response.

Any new authority should be complementary to existing authorities under Section 215 of the Federal Power Act, which rely on industry expertise as the foundation

for developing reliability standards. Any new authority should also be narrowly tailored to deal with real emergencies; overly broad authority would undermine the collaborative framework that is needed to further enhance security.

Promoting clearly defined roles and responsibilities, as well as on-going consultation and sharing of information between Government and the private sector, is the best approach to improving cybersecurity. Each cybersecurity situation requires careful, collaborative assessment and consultation regarding the potential consequences of complex threats, as well as mitigation and preventive measures, with owners, users, and operators of the bulk power system.

Exelon and other electric utilities remain fully committed to working with the Government and industry partners to increase cybersecurity.

I appreciate the opportunity to appear today and would be happy to answer any questions.

Mr. THOMPSON. Thank you very much, and I thank all the witnesses for their testimony. I will remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for the first set of questions.

Each of you have talked about this attack in one capacity or another. Starting with Dr. Graham and going to his left, can the panel tell this committee in their professional opinion if the electric industry has appropriate protections, today, to protect against a cyber or an EMP attack?

Mr. GRAHAM. Mr. Chairman, the electric industry today does not have adequate protection in place, or as far as I can tell, any protection in place for the power distribution and the power generation systems of this country.

Given that the power grids are in a state of transformation, I believe this is a particularly appropriate time to build that protection in and it will help not only with EMP but with such problems as grid collapse, as we saw on August 13, 2003 and earlier times as well.

So it could be very effective. It is very timely and I believe, very needed.

Mr. THOMPSON. Mr. Fabro.

I have to admit, also, I love the name of your company too.

Mr. FABRO. Thank you, sir. Thank you, sir. The question that you are asking is one that is quite difficult, because you are trying to encapsulate a very, very large problem with one single question.

Is the bulk power system of the electric grid completely immune and protected from cyber attack? No, but there are significant pockets, significant pockets, and significant pockets of progress that have shown that the overall cybersecurity risk profile of the bulk power system in North America, not just within the United States, within North America, because it is a multi-national issue, has improved substantially. Substantially. It is very easy to go and look at the things that are notably bad; reports from the press or other issues that we hear in various news outlets.

But overall, from someone who experiences on a day-to-day basis, who lives and works in the trenches of this, I actually see standards and work and cooperative engagements and what is being done by public-private partnerships in action and they work.

I cannot comment on EMP. I will just leave that, of course, to Dr. Graham.

Mr. THOMPSON. Thank you. Mr. Assante.

Mr. ASSANTE. I have been very encouraged by the progress in industry to secure vital systems to protect the bulk power system. It

is a very complex problem in order to wrestle. I will tell you this: I have been working for years and looking at the underlying technology, the vulnerabilities that exist in the unique operating environments in which the technology exists.

We do believe that there are vulnerabilities in the system. We know that we are not immune from these attacks. We are committed to this call to action. My letter, made on April 7, was a, I think, very important in that it brought out the dialogue that was necessary to talk about how to prioritize assets for protection.

There are some important issues to consider when you look at how one can manipulate technology in such a way to cause an impact. The misuse of technology is a very important thing to consider. The ability to exploit technology horizontally is important.

Industry, I believe, is up for that challenge. I don't think there is an easy answer, and it won't happen very quickly, or enhancing the standards. We are putting in place all the mechanisms necessary to be able to communicate about threats and warnings, so that we can take quicker action. We are dedicated to public and private partnerships to learn more information.

Very briefly on EMP, I again, believe that the electromagnetic pulse, is a high-impact concern is something that we are concerned in the electric power system. We are partnering with the Department of Energy. We have consumed the EMP Commissions report. We supported it, not only staff, but also industry experts, in the deliberation. We intend to look at these risks alongside of other risks to evaluate them and prioritize them and to take a look at what mechanisms we have to further mitigate the system for these types of threats.

Mr. THOMPSON. Mr. Naumann.

Mr. NAUMANN. Thank you.

My belief is that in general, the North American grid is well-protected against cyber attacks; at least those threats that we know about.

The biggest problem, we believe, we face is the lack of information because of the security nature of that information and it is hard to devise mitigation against something you don't know.

That is something that is on-going. We are trying to work with the Federal agencies. But that, to us, is the No. 1 thing that we need to work on.

As far as EMP attack, as Mr. Assante has said, and as Dr. Graham said, that this is a low-probability, high-impact event. It is something that the industry will pay attention to, wants to work with the Federal Government to devise mitigation and responses. But what we need to know is what is the design threat that needs to be dealt with? What are the mitigations from that that we need to work out? What are the consequences of that mitigation? What is the priority of this particular threat compared to the other low-probability, high-impact threats that have been mentioned?

Thank you.

Mr. THOMPSON. My time has expired. I recognize the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. Again, I would like to congratulate the panel, not only on their verbal testimony, but their written testimony. It is very helpful. We could

spend hours here and we have got two really serious subjects. One, the EMP and one cybersecurity, and I think it is good that we have them here together, but also there is a problem because we can't go in depth as to where we want to go on this.

First of all, Mr. Naumann, you talked about the problem with the industry not knowing the threat because of the security nature of the information from the Federal Government. Are we beginning to attack that problem? How would you suggest that we try and resolve that problem?

Mr. NAUMANN. I believe we need to have a more formal collaborative, where a certain set of industry people are given sufficient clearance. This is something that NERC is working on, where the Federal Government can give us high-level security information. Those experts can then, working with the Federal Government, devise the mitigation and then essentially censor the information, but send out the mitigation to the industry, so that we could implement that.

Mr. LUNGREN. Mr. Assante.

Mr. ASSANTE. We have been working hard, I think, and it is a critical impasse. I think it gets back to the Aurora vulnerability. What is needed to devise the best mitigation strategies is accurate information in order to support the development of those strategies. We have been working very hard with the Department of Energy, the Department of Homeland Security, and even through the intelligence community, to be able to share information.

To be able to validate information as we see it in the printed and public press, of the Wall Street Journal, to be able to understand the success and tactics that adversaries have been able to use to compromise systems, whether they be Government or private sector and being able to appropriately adjust our defense postures. Importantly, going past information sharing, we are working on the elements to share the information.

So within our industry, we can get that information to people who need to take action. We are also working on developing the ability to respond to and to contain and to minimize the consequences of a successful attack. We are not going to put all our effort into simply prevention. That has failed us as a Nation. Prevention is important, but it is not the only part of it and we are dedicated to working with entities to be able to put more focus on it.

Mr. LUNGREN. Let me ask you this, when we usually do a risk analysis, we talk about threat vulnerability and consequence. You obviously know the consequence, your companies would know the consequence of a problem; a disastrous or consequential interruption.

Are you saying what you need more from the Federal Government is information with respect to the threat only? Or also that the Federal Government has an ability to tell you what the vulnerabilities are above and beyond what you know your vulnerabilities to be?

Mr. ASSANTE. They are, actually, it is on both accounts. As far as it relates to threats, when the Federal Government can observe and analyze successful attacks. It is important for us to understand how those attacks looked and how we would respond to those at-

tacks. But importantly, as you address vulnerabilities, control systems are very complex, the implementation of that technology is complex and the ability of any one asset owner utility to understand the inner workings of that technology to all the underlying weaknesses that might be there, it is very difficult for the asset owner to do that.

Mr. LUNGREN. So who would you look to for that? The Federal Government? Both?

Mr. ASSANTE. It is the Government. The Department of Energy and the Department of Homeland Security have two very successful programs that have been testing control system technology. The discovery of vulnerability is very helpful for us to be able to enhance the security of those systems.

Mr. LUNGREN. Does that need to be somewhat made more robust? Or is there a problem with getting security ratings for your people? I mean, where is the problem there?

Mr. ASSANTE. Well, some of the problem has to do with the partnership that is required in this global supply chain of working with these vendors that supply the technology. A lot of times, they are willing to look at the technology, but under contract agreements, so that the information wouldn't be made public. That information then goes to the vendor to address. It is, in many cases, shared with the utilities. But that progress has been limited by the scope of those programs. We do believe they provide a lot of value.

We have been heavily participating——

Mr. LUNGREN. Well, if you need any additional legislative umbrella for that, let us know.

Dr. Graham, can you tell me, are there any other countries hardening their critical infrastructure to defend against EMP?

Mr. GRAHAM. Yes. In fact, we have helped some of our allies in that direction. We know that at least the Soviet Union, now Russia, has also worked on that. We know that China is extremely interested in EMP, has a large number of people there, engineers, scientists, working on it. There is enough traffic among these communities that deal with high-tech and nuclear subjects, outside the United States, that are among our adversaries that it is widely spread.

Mr. LUNGREN. Just one real short question. That is, are any countries ahead of us in terms of our efforts to either recognize our problem or react to it by hardening our critical infrastructure?

Mr. GRAHAM. They are all ahead of us in one way, which is they are less dependent upon computer-controlled information, dominant systems, than we are, and therefore less vulnerable.

In terms of number of people working on the subject, I think China is far ahead of us. In terms of the implementation in civilian systems, most of the European countries are ahead of us.

Mr. THOMPSON. Thank you very much. The Chair now recognizes the gentlelady from California for 5 minutes. Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman, and thanks for this hearing. I think the fact that we are here today speaks of our bipartisan intention to pay attention to this. Our new Chairwoman, Ms. Clarke, is joined, of course, by the Chairman of the full committee. Mr. Lungren has had a full interest in this for some time.

I notice Mr. Langevin, who chaired the subcommittee with jurisdiction over cyber was earlier here. A long time ago, I was the Ranking Member on the Cyber Security Subcommittee, when it was chaired by Mr. Thornberry. So it is many years of frustration over this situation that has brought us here today and I am happy to be an original co-sponsor of this bill.

I think back to the last Congress, at a hearing that we had, and we all knew, because we had been briefed in a classified setting, about some things that needed to be done to make the Nation secure and it was not happening. When we turned to FERC, they were unable to make it happen. We asked them if they wanted the authority to require the steps to keep the Nation secure? They basically saw—so they couldn't do it, and they didn't want to do it, which I thought was a pretty weird answer, in all honesty.

Because the comments made today about the need for collaboration, we agree with. The comments made about the role of the ISECs, we agree with. The need, and if there are suggestions, and that is my question, to add some additional steps so that the private sector has consultation, that will just enhance the matter.

But when all is said and done, the infrastructure that is owned, primarily, by the private sector is relied on by the entire country. If a SCADA system has a vulnerability that we know about, and steps are not taken to secure it, and the whole grid goes down, the Government has the right to be interested in that matter and right to, really, to require that steps be taken to protect the Nation.

So I am interested in specific comments that any of the witnesses may have about how you believe that collaboration might be enhanced in this bill. I don't think it precludes anything actually. I don't think there is a need to enhance it because it doesn't preclude the things that you have discussed. But if you have specific suggestions on how to involve the private sector, I would be interested in hearing them.

Before I turn to you, I didn't want to neglect Mr. Bartlett, who of course has been known for some time on the log, focusing on cyber, that is the issue he has focused in on for some time; that also needs attention.

So anybody who has a suggestion on private sector collaboration, I am all ears.

Mr. Graham.

Mr. GRAHAM. I believe in the line of collaboration, one of the first things that needs to be done is the Department of Homeland Security needs to be informed and take an interest in the subject of EMP and I presume cyber attack.

To give you an example, trying to—we have been, as a commission, unsuccessful in engaging Department of Homeland Security in this area. Today, I went to the Homeland Security website, I put in EMP, it took me to FEMA and there it told me that EMP was a form of radioactive fallout and it said "only those who rely on electronically-driven life support systems are at risk."

Ms. LOFGREN. Could I—very good. So you at DHS, pay more attention, our new Secretary, I think, will be paying attention. Mr. Fabro.

Mr. FABRO. I think that the questions, the statement that you have made is exceptionally accurate. That we have all the pieces

in place, from what I see, from what my experience indicates, is that the element of robustness, as it relates to what is coming upwards from independent research, what is actually being discovered and found within the operational environment of the private sector itself isn't coming upwards.

There is no sharing mechanism for that information to come upwards to either, validate, substantiate, disprove, or have some other impact on what is being done by the Federal research community. Make no mistake, the work that is being done with DHS and DOE, absolutely valuable, absolutely valuable. The capabilities for FERC——

Ms. LOFGREN. So, the research world needs to be brought in.

Mr. FABRO. It needs to be brought in. Has been spoken about earlier, the complexities involved with the fact that there is so much vendor-specific issues related to securing this, the vendors are often exceptionally reticent to accept the independent research, because it may impact a variety of different things from——

Ms. LOFGREN. Right.

Mr. FABRO [continuing]. From a business perspective.

Ms. LOFGREN. I don't know if I have time, Mr. Chairman, to get a few quick comments from the other two witnesses, under a minute total?

Mr. THOMPSON. You have a minute.

Mr. FABRO. I do believe our interests are well aligned here, in terms of what to protect. One of the obligations that we have is that we enhance our security incident reporting.

As incidents occur within the private sector, it is very important they quickly be shared. The incidents be absolutely analyzed. And information, lessons learned, be shared back, so others could protect themselves.

It is something we feel very strongly about. I think we demonstrated that recently.

We also believe in terms of research, that better cyber awareness tools, of what actually is occurring across the internet and large networks, is very important. This is an area that the Government can contribute greatly.

Ms. LOFGREN. Couldn't ES–ISAC be used to that effect?

Mr. FABRO. We absolutely believe the ES–ISACs can affect, and they probably need some analytical support in the ability to——

Ms. LOFGREN. Mr. Naumann, you have 15 seconds.

Mr. NAUMANN. That much. Thank you. Very briefly, just to add on. We think the most important thing is clear and concise communication. So that if there is a threat out there, that threat gets down to the users, owners and operators, who understand our system and equipment, so that we can take appropriate mitigation.

If we don't know about the threat, it is very hard to mitigate against it.

Ms. LOFGREN. So, this bill will certainly let you know about that threat.

Mr. NAUMANN. Yes, but if there is an emergency, to the extent there is time, it is very important that rather than issuing a directive, there be as much consultation as is possible under the circumstances, else our concern about unintended consequences of those directives.

Ms. LOFGREN. Thank you, Mr. Chairman, I appreciate the extra minute.

Mr. THOMPSON. Thank you very much. The Chair recognizes the gentleman from Maryland, Mr. Bartlett, for 5 minutes.

Mr. BARTLETT. Thank you very much. I want to thank you again for inviting me to be here.

EMP attack may be a low probability, it is certainly a high-impact event. But when you have such a potential like your house burning, you buy an insurance policy. You do something that will make you whole in the event that that happens.

I would submit that in our country, we have done essentially, nothing, that would make us whole, if this were to happen.

Dr. Graham, it is my understanding that electromagnetic pulse is an unavoidable accompaniment of any and every nuclear detonation. That if it occurs at ground level, that the area of the fireball and the EMP area, are not all that much different, that we have had little attention to EMP when it is a ground level attack.

But if it is at altitude, and if it is extra atmospheric, it is line of sight. A detonation 300 miles high above Nebraska, Iowa, would cover our whole country? Is that essentially correct?

Mr. GRAHAM. Yes, with a footnote that even for a surface, or near-surface nuclear burst, if there are things like power lines or conductors going into the fireball, that fireball acts like a tremendous battery. And will drive electrical signals miles and miles beyond its perimeter, but along the line.

Mr. BARTLETT. It is my understanding that in your work on the commission that you interrogated two Russian generals, who told you that the Soviets had developed, and they have enhanced EMP weapons that would produce 200 kilovolts per meter. That is correct?

Mr. GRAHAM. Yes, that is correct.

Mr. BARTLETT. That would be 100 kilovolts per meter at the margins of our country?

Mr. GRAHAM. It depends—it is somewhat north, south dependent affect, but in some directions, yes.

Mr. BARTLETT. It is my understanding that the most we have ever built and tested to is sometimes 30 and sometimes 50 kilovolts per meter. Is that correct?

Mr. GRAHAM. Yes, that is correct. The upper figure was used earlier, and now the lower.

Mr. BARTLETT. If in fact we could be exposed to 100 or 200 kilovolts per meter, protecting to 50 kilovolts per meter is little better than doing nothing, is—or 30, it is now 30. Is that correct?

Mr. GRAHAM. Well, it is unknown as to how good the protection would be above that, because, it would be an untested regime. In general, the test, the protection could fail at the higher levels.

Mr. BARTLETT. What proportion, what part of our electronic world would you expect to be affected by 200 kilovolts per meter?

Mr. GRAHAM. Essentially, every thing that wasn't in a conductive package, everything from PCs on up through power grids.

Mr. BARTLETT. It would have to be in a Faraday cage and grounded if it were to survive. Is that correct?

Mr. GRAHAM. Yes, individual components that are wrapped up in protective packages might survive it. But anything that is functional, or connected to other systems, would not.

Mr. BARTLETT. In a former life, I was a scientist. I am always amazed at scientists and their ability to understate. I am now kind of a recovering scientist.

But Dr. Graham is a scientist, and he says that "EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences."

In other words, "that could end life as we know it." Is that correct?

Mr. GRAHAM. Certainly as we know it in the United States. I don't think North Korea would find it a shock if they had an EMP event, because, they have so little infrastructure to begin with.

But, our country has many times the population it had say in 1900. Yet, our facilities could be driven back to the pre-1900 level by an EMP attack. The country could just not support that population.

Mr. BARTLETT. This has been described as a high-level EMP, robust EMP lay down, as a giant time machine that would move us back a century in technology. That is roughly correct?

Mr. GRAHAM. Yes, maybe a little more than a century affect.

Mr. BARTLETT. So, this is such a horrendous consequence. Why are we not paying more attention to it?

One of the great experts in this area, Lowell Wood, says "it is just too hard. They don't want to deal with it." Is that the problem?

Mr. GRAHAM. That is probably a better question for a social scientist to answer. But, I have heard it characterized as a low-probability, high-impact affect. The commission would not assign a probability to it.

However, we do know that all of our adversaries across their whole reach have all the capability necessary to execute this kind of attack. They know our vulnerability to it.

So, it seems to me that we cannot assign it a low probability of occurring. It won't happen every day. But, it would take us by surprise if it happened today.

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

Mr. THOMPSON. Thank you very much. For a recovering scientist, you do all right.

Ms. Jackson Lee for 5 minutes.

Ms. JACKSON LEE. I want to thank the Chairwoman and the Ranking Member for holding this committee. Thank you, Chairman.

Dr. Graham, I assume, and I am making the statement that you feel comfortable with your statement, and as chairperson of the commission to assess the threat to the United States from EMP. The research of that commission gives you comfort to make the statements you are making today. Is that correct?

Mr. GRAHAM. Yes, that is correct. Three other members of the commission are here as well.

Ms. JACKSON LEE. Let me thank them for their work. Let me just read the opening of your comments: "EMP is one of a small number of threats that we can hold our society at risk from catastrophic consequences."

Then you make mention of the fact that several potential adversaries have, or can acquire, the capability to attack the United States with a high-altitude, nuclear weapon-generated electromagnetic pulse, EMP. A determined adversary can achieve an EMP attack capability without a high level of sophistication.

Would you make these comments right at the front of your statement without substance and being able to substantiate it?

Mr. GRAHAM. Well, I would make those statements. We have substantiated them.

Ms. JACKSON LEE. Yes, and you would not make them without them being substantiated. Is that correct?

Mr. GRAHAM. Absolutely not.

Ms. JACKSON LEE. Why did you make those statements, Dr. Graham?

Mr. GRAHAM. We have issued several classified reports as well, that go into these in much more detail, which are available to the Congress. We have explored the subject with the intelligence community, and with the Department of Energy, and its nuclear weapon design laboratories, at great length. We base our conclusions on that.

Ms. JACKSON LEE. Let me ask the three gentlemen, I think to your right, if I am correct. A simple hurricane that most people don't know anything about called, "Hurricane Ike," which obviously is a natural disaster, had a catastrophic impact, or an exponential impact. Because in fact, after the storm was over, the community that it impacted, was without electricity for some 6 weeks-plus.

It is probably the most costliest hurricane in that Gulf region, short of Hurricane Katrina, and possibly Rita. But more importantly, the suffering was enormous.

Can you explain to me the basis of the self-regulation of your industry, Mr. Naumann? Why you wouldn't want more intense regulation? Because a potential attack, or impact of EMP, as Dr. Graham has said, "would be enormously catastrophic." In fact, whole communities could be wiped out.

Mr. Naumann.

Mr. NAUMANN. Thank you, I don't believe it is an issue of regulation. I believe it is an issue of getting together, setting the priorities, determining what the threat is and then——

Ms. JACKSON LEE. You don't think that you could do it better with a Government partnership? Having more stringent regulations as it relates to EMP?

Mr. NAUMANN. I don't believe the regulation itself would make the difference. The partnership would.

Ms. JACKSON LEE. So, you agree with Dr. Graham that we have the potential of a catastrophic impact with the EMP?

Mr. NAUMANN. I don't have access to the classified information Dr. Graham does.

Ms. JACKSON LEE. But I just asked Dr. Graham, whether he could substantiate it. So, based on his being able to substantiate, would you agree that it could have a catastrophic impact?

Mr. NAUMANN. I absolutely agree.

Ms. JACKSON LEE. I thank you.

Mr. Assante.

I think you are NERC, N-E-R-C, and I think that is the group that self-regulates and allows electric companies to go out during a hurricane, and have no criteria for getting back on.

What is your description of self-regulation? Do you feel there needs to be more regulation and partnership between the Government and its industry to protect it against EMP, as Dr. Graham has mentioned?

Mr. ASSANTE. Certainly, EMP as a threat is disturbing in that, different from Ike, it destroys components of the power system that will be difficult to restore from——

Ms. JACKSON LEE. Ike, is only an example, I mean it holds electricity.

Mr. ASSANTE. I absolutely understand. I do believe that, and we had the meeting with the commission, and we have met with experts that has provided testimony——

Ms. JACKSON LEE. So would you support more Government regulation and partnership?

Mr. ASSANTE. I would suggest partnership is really important to understand the problem——

Ms. JACKSON LEE. Regulation you would look at?

Mr. ASSANTE. I do believe Section 215, is an appropriate vehicle to——

Ms. JACKSON LEE. Is or is not?

Mr. ASSANTE. I think it could be and it is an appropriate——

Ms. JACKSON LEE. Let me go to—thank you very much.

The few minutes that I have, Mr. Fabro.

You heard my comments and Dr. Graham's comments. We have a real problem.

Do you believe that we need to have a greater enhancement of Government partnership? I call it regulation to ensure against this disaster?

Mr. FABRO. Absolutely, if the findings from Dr. Graham and his commission are accurate, as a scientist myself, I firmly agree that these issues are very important.

I think that the partnership, with involvement from the Federal Government is critical, to fully understand the issues. I think that the findings from that must be incorporated into future State standards.

From a regulation perspective, I don't know if it has to be a regulatory function, but I certainly do agree involvement from the Federal Government is required for a full picture.

Ms. JACKSON LEE. I thank you. I think without regulation, we don't get enforcement and implementation.

I thank you, and I yield back to the Chairman.

Mr. THOMPSON. Thank you very much.

Now, your 5 minutes, the gentleman from New Jersey.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Chairman, this legislation did not come out of the blue. It didn't materialize itself.

I want to associate myself with the comments of Mr. Bartlett. We should all be very seriously concerned. I guess that is why we are here.

But I remember last May, when NERC's CEO, Rick Sergel, sat in that seat over there. He admitted to this committee that we, the

committee, had been lied to by the electric industry. Maybe you will remember that.

For those Members who were not here last year, NERC told us in October 2007, that three-quarters of the industry had mitigated a vulnerability known as Aurora. NERC claimed that they sent the survey out to industry, and they had received, obviously, responses back.

We finally got the truth out, and found out that the survey hadn't been sent. NERC had no hard numbers. NERC just made them up to get us off their back. We found that out last year.

So we learned then to be suspicious. After the hearing, and to his credit, Mr. Sergel, brought in Mr. Assante to restore the credibility of NERC. The committee—and I believe he has chosen a very, fine person for this position.

I would like to ask Mr. Naumann a question.

You are here representing the Edison Electric Institute and the Electric Power Supply Association, Mr. Naumann, is that correct?

Mr. NAUMANN. Yes, Congressman.

Mr. PASCRELL. A question about September 11, your 2008 meeting of the NERC Critical Infrastructure Protection Committee. At the committee meeting, the NERC Infrastructure Protection Committee received a briefing on the report of the commission to assess the threat to the United States from the EMP. This is the report. Have you seen that report, Mr. Naumann?

Mr. NAUMANN. I have skimmed—scanned the report on-line, yes.

Mr. PASCRELL. Then you know, basically, what is in here then, right?

Mr. NAUMANN. I do.

Mr. PASCRELL. This report was written by the congressional commission that Dr. Graham chairs. The commission has been reviewing our electric grid security against an intentional, or unintentional, event for years. The commission found, Mr. Chairman, and Mr. Ranking Member, "a single EMP attack may seriously degrade or shut down a large part of the electric power grid in the geographic area of the EMP exposure, effectively instantaneously."

The commission came up with a number of steps that the private sector can take to help significantly reduce the threat of EMP. They were good recommendations. I do not believe they were prohibitively costly.

Now, here are the minutes of the meeting. Have you seen this, Mr. Naumann?

Mr. NAUMANN. No, sir.

Mr. PASCRELL. You never saw the minutes of the meeting?

Mr. NAUMANN. I am not a member of that committee.

Mr. PASCRELL. I know you are not. But I asked you if you saw the meeting—the minutes. Did you see the minutes, Dr. Graham?

Mr. GRAHAM. No.

Mr. PASCRELL. Okay.

I currently have in my hands, the minutes from the meeting. I ask for unanimous consent to introduce these minutes into the record, Mr. Chairman.

Mr. THOMPSON. Without objection.*

*The information referred to has been retained in committee files.

Mr. PASCRELL. You would think that an issue as serious as an electromagnetic pulse, which has catastrophic consequences, is not terribly expensive to fix, would have spurred the electric industry into action. You would think that an at-risk industry would want to fix its vulnerabilities. You would think that after not fixing the Aurora vulnerability for years, the industry would want to show some proactive security efforts, send a message that at least they are moving in the right direction.

But this is not what happened, Mr. Chairman, on September 11 of last year. According to the minutes, "there are no actions expected by the Critical Infrastructure Protection Committee or NERC to this rep."

No actions. Nothing. The industry, which is, as Chairwoman Clarke stated, "responsible for operating security grid plans are doing nothing to secure its infrastructure or to mitigate this threat."

Now, Mr. Naumann, why aren't your colleagues doing more to secure your infrastructure against an intentional or unintentional EMP event or cyber attack? Mr. Naumann.

Mr. NAUMANN. Congressman, as I said, we want to work with NERC and the industry in identifying what needs to be done, what the design threat is. I just heard from Congressman Bartlett, for example, whether the threat is 200 volts per meter or 50 volts per meter——

Mr. PASCRELL. Mr. Naumann, Mr. Naumann, excuse me. Why aren't you doing anything right now to secure the infrastructure?

Mr. NAUMANN. In order to——

Mr. PASCRELL. You are telling me something, everybody knows in this room. We listen.

Mr. NAUMANN. I——

Mr. PASCRELL. Well, then please answer my question?

Mr. NAUMANN. In order to secure the infrastructure, we first have to determine what threat to protect against and then design mitigation. As I understand it, through NERC, Mr. Assante is taking this up as one of the action items. But it has to be done in a thoughtful manner.

Mr. PASCRELL. So the industry—these are the minutes. I mean, I didn't make it up.

Mr. NAUMANN. I was testifying——

Mr. PASCRELL. I yield back.

Mr. THOMPSON. Thank you very much. I appreciate your—we have Ms. Richardson and Mr. Luján and we have four votes to take after that. Ms. Richardson.

Ms. RICHARDSON. Mr. Chairman, I will be very brief so I can give my colleague an opportunity to speak before our break.

Is Mr. Seán McGurk present, from the Department? Okay. I would like to recommend during the break, Dr. Graham, since you have said "you have had an unsuccessful engagement of speaking with the Department," he is right here, I think, in the third row. For the record, Mr. Chairman, I would like to recommend that maybe we submit the testimony to the new Secretary and urge her and her appropriate Department to review the information and give them an opportunity to come forward.

Mr. THOMPSON. I would be happy to do it.

Ms. RICHARDSON. My last point, and I do want to be brief, as I said, for my colleague. Having reviewed the bill that we have on the table, I would just like to work with the Chairman, possibly in a Manager's Amendment, as I listen to the testimony today, one of the things that I think we could add is in Mr. Fabro's testimony, in the very back, he gives three points that we could focus on. One is "research," which has been much discussed, much discussed today.

Second, "redefining standards," which there is the ability to do some of that in the bill. But what we don't talk about is he talked about "procurement guidance." Specifically from his testimony, he says "in the case moderate reengineering of existing procurement guidelines can have tremendous downstream influence, in both power systems, cybersecurity and it can be done immediately."

So I will work with my staff and in conjunction with some of the folks that have been here today to see if there is any way that we can help to strengthen it even further.

With that, I yield back the balance of my time.

Mr. THOMPSON. Thank you very much.

The gentleman from New Mexico for 5 minutes.

Mr. LUJÁN. Thank you very much, Mr. Chairman and thanks to my colleague, Ms. Richardson, for being so kind with her time.

Mr. Assante, did I hear you correctly that when there was a reference to cybersecurity that prevents—did you say something along the lines "prevention is not necessarily the answer?"

Mr. ASSANTE. I don't think we should put our full faith in preventing attacks. It is very important that we also address investments in being able to categorize, observe them, and respond to them, and minimize their consequences in the system. So we would like to take a comprehensive approach to cyber attacks, not just installing more cybersecurity solutions that have failed in the past. Some of the advanced threats are capable of getting around those solutions. We want to make sure that we have got the full capabilities to be able to handle this important challenge.

Mr. LUJÁN. Do any of the bulk power systems have a responsibility to report to NERC, or the body, if there is a cyber attack?

Mr. ASSANTE. They do. Under the CIP standards today, they have to report security incidents affecting critical cyber assets to NERC. NERC will take that information, analyze it and pass it on for warnings for other organizations.

Mr. LUJÁN. To date, have there been any reports to NERC?

Mr. ASSANTE. Yes. We have received reports of security incidents to the bulk power system.

Mr. LUJÁN. So is the grid safe today?

Mr. ASSANTE. I would tell you that it is—I believe that the grid is not immune from attack. We have seen the attacks occur. What we can do is try to respond to those attacks, enhance our security and ability to respond to them. It is definitely a concern. It is why we are asking for, immense authorities from the Federal Government to very specific and imminent cyber threats.

Mr. LUJÁN. So, Mr. Naumann, with that being said, I stand corrected, but I thought I heard you say earlier that you feel that the grid is safe today?

Mr. NAUMANN. I believe I said "it is relatively secure from the threats that we know of."

But it——

Mr. LUJÁN. Okay.

Mr. NAUMANN [continuing]. May not be secure from the threats we don't know of, which is why we support the emergency legislation.

Mr. LUJÁN. Mr. Assante, with that being said, I think that we heard from Ms. Richardson and others the importance of making sure that we are able to provide the information necessary so that you can prepare for any cyber attacks that do exist. But there was a Wall Street Journal article in April of this year that highlighted threats that we do know, that occurred, that I don't know if they have been addressed or not, but in your testimony you state "that there has been progress made through NERC with the bulk power systems."

Mr. ASSANTE. Yes.

Mr. LUJÁN. Can you just highlight those quickly?

Mr. ASSANTE. Sure. I absolutely can. Most importantly, our ability to communicate effectively with the 1,800-plus entities that comprise the bulk power system is an important capability that we work very hard to achieve.

The second piece is that we have been working in great partnership with the Department of Homeland Security and the Department of Energy to be able to analyze advanced threats. So when we become aware of them, and I will give you a quick example, we have seen suspicious activity against power system networks. They have reported that to me at the ES–ISAC. I shared that information with our Government partners and then provided excellent analysis of what it looked like, what it was, and we went back and we were able to notify and warn other entities of the suspicious activity.

So those are the types of progress that I think is very important. I think it—we are working full force in the collaborative side. But if a cyber threat was imminent and specific, we believe the necessity to have emergency authorities to deal with that and deal with it in a mandatory way are appropriate.

Mr. LUJÁN. Yes. With that being said, Mr. Naumann, there was a reference made earlier that there is not a set of standards in place for utilities across the country today, that everyone has their own platforms that they operate on and it would be difficult to institute a fix that would reach everyone. With that being said, is there a need to go to standard platforms, as utilities are making investments into the future? Understanding that this is a threat that does exist today?

Mr. NAUMANN. I think there is a need to go to standard protocols. For example, on the Smart Grid, dealing with Smart Grid, FERC has just issued a final rule that said "any Smart Grid devices that are attached to the system should follow protocols that are being developed under the auspices of this." So it is the protocols as to how they communicate and how they interact with the system, that it is very important; that they be common; and that they be secure.

Mr. LUJÁN. The last question I have, Mr. Chairman, is that as we go forward and we understand the direction where Smart Grid will take us and how broadband applications are going to be critical to achieving the efficiencies that we need with distribution and transmission.

Understanding that NERC's sole responsibility is with bulk power systems and does not include distributed generation or settlement, industrial utilities or applications, even within some of our rural cooperatives: Who is overseeing that aspect and is there anybody—are there any, I guess, large umbrella support systems other than State regulatory bodies that are working directly with them? Are those actually reported?

Mr. LUJÁN. Mr. Chairman, we can get back to that one later, if need be.

Mr. THOMPSON. The gentleman can answer.

Mr. NAUMANN. To answer very quickly, it is important that under U.S. legislation, that as it relates to Smart Grid in particular, that NIST, and the Department of Energy, in working with FERC, and NERC is then engaged in this activity, do address system standards, so that they can build security into this technology before it gets deployed in great numbers. But most of the jurisdiction and regulation of the system has been done at the local level and the State level. However, in a lot of cases, that can be very appropriate, based on local issues.

But NERC is concerned about the bulk power system and in the future, as devices in aggregate might cause a material issue to reliability, we would actively engage in those efforts.

Mr. LUJÁN. Mr. Chairman, just want to suggest quickly there, we may want to work with NARUC, the National Association of Regulatory Utility Commissions, to truly get an inventory of how many utilities, investor-run utilities across the country, have been working with their State partners. Having come to Congress as a former regulator, from the utility commission, in New Mexico, I can tell you that there is a concern that I have there and to make sure that we are working with our colleagues across the country that this information is truly being compiled.

Mr. THOMPSON. Mr. Luján, as you can see, once this legislation is brought up for mark-up, you will see some additions to it.

Let me thank our first panel of witnesses for excellent testimony and answers to the questions. We have four votes, plus 111th Congress photograph that will probably take about 35 or 40 minutes. But we release the first panel. Thank you for your testimony. The committee will recess and reconvene at the end of the votes.

[Recess.]

Ms. CLARKE. [Presiding.] I welcome the second panel of witnesses. We are joined by Joe McClelland, the director of reliability at the Federal Energy Regulatory Commission, also known as FERC. Our second witness is Patricia Hoffman, acting assistant secretary at the Office of Electricity Delivery and Energy Reliability, Department of Energy.

Our third witness is Seán McGurk, director of the Control Systems Security Program at the Department of Homeland Security. Welcome. Finally, Cita Furlani, is the director of the Information

Technology Laboratory, National Institute of Standards and Technology at NIST.

I want to welcome you all here. Without objection, the witnesses' full statements will be entered into the record. Hearing no objection, so ordered.

I now ask each of the witnesses to introduce yourself and summarize your statement for 5 minutes, beginning with Mr. McClelland.

STATEMENT OF JOSEPH H. MCCLELLAND, DIRECTOR OF RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

Mr. MCCLELLAND. Chairwoman Clarke, thank you. Member Lungren, and distinguished guests. Thank you for the privilege to appear before you today to discuss the security of the electric grid.

My name is Joe McClelland, and I am the director of Office of Electric Reliability at the Federal Energy Regulatory Commission. I am here today as a commission staff witness and my remarks do not necessarily represent the views of the commission or any individual commissioner.

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

Under the new authority, FERC cannot author or modify reliability standards. It must select an electric reliability organization, or ERO, to perform this task. The ERO develops and proposes reliability standards or modifications for the commission's review, which it can either then remand or approve them.

If the commission approves the proposed reliability standards, 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.

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

In addition to the reliability authority, FERC is also charged with the oversight of cybersecurity of the bulk power system. As is the case with non-security issues, FERC's authority in Section 215 over cybersecurity is to exercise the reliability standards developed by the ERO and approved by FERC.

Pursuant to this duty, FERC approved eight cybersecurity standards known as the Critical Infrastructure Protection, or CIP standards, proposed by NERC, while concurrently directing modifications to them in January 2008. 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 modification responding to the commission's directives was received from the ERO in May 2009, and they are now under review.

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 increases the grid's cyber vulnerability. The CIP standards will apply to some, but not all Smart Grid applications.

Physical attacks against the power grid can cause equal or even 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. In 2004, and again in 2008, the EMP Commission issues its reports.

Among the findings in the reports were that a single EMP attack could seriously degrade or shut down a large part of the electric power grid. Depending upon the attack, significant parts of the electric infrastructure could be, "out of service for periods measured in months to a year or more."

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

The standards development system utilized under FTA215, involved mandatory reliability standards using an open and inclusive process based on consensus. Although it can be an effective mechanism when dealing with the routine requirements of the power grid, it is inadequate when addressing threats to the power grid that endanger national security.

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

Any new legislation should address several key concerns. First, 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 appropriate confidentiality of security-sensitive information.

Third, the limitations of the term "bulk power system" should be considered, as FERC cannot act to protect against attacks involving Alaska and Hawaii as well as some transmission, and all local distribution, facilities in population areas.

Finally, entities should be permitted to recover costs they incur to mitigate vulnerabilities and threats. Thank you for your attention today and I am available to address any questions that you may have.

[The statement of Mr. McClelland follows:]

PREPARED STATEMENT OF JOSEPH H. MCCLELLAND

JULY 21, 2009

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

My testimony summarizes the commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act, and some of the limitations in Federal authority to protect the grid against physical and cybersecurity threats. The commission currently does not have sufficient authority to require effective protection of the grid against cyber or physical attacks. If adequate protection is to be provided, legislation is needed and my testimony discusses the key elements that should be included in any new legislation in this area.

BACKGROUND

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

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

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

Currently, the commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any Federal installations located therein. The current interpretation of "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding commission action to mitigate cyber- or other national security threats to reliability that involve such facilities and major population areas.

Critical Infrastructure Protection Reliability Standards

An important part of the commission's current responsibility to oversee the development of reliability standards for the bulk power system involves cybersecurity. In August 2006, NERC submitted eight proposed cybersecurity standards, known as the Critical Infrastructure Protection (CIP) standards, to the commission for approval under section 215. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "Bulk Electric System." NERC proposed an implementation plan under which certain requirements would be "auditably compliant" beginning by mid-2009, and full compliance would be mandatory in 2010. Pursuant to NERC's implementation plan for the CIP standards, the term "auditably compliant" means "the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'" At the end of July 2009, responsible entities will provide responses to NERC's self-certification survey. Those responses will include information on their progress towards compliance with the CIP standards.

On January 18, 2008, the commission issued a Final Rule approving the CIP reliability standards while concurrently directing NERC to develop significant modifications addressing specific concerns. The commission set a deadline of July 1, 2009 for NERC to resolve certain issues in the CIP reliability standards, including deletion of the "reasonable business judgment" and "acceptance of risk" language in each of the standards. NERC concluded that this deadline would create a very compressed schedule for its stakeholder process. Therefore, it divided all of the changes directed by the commission into phases, based on their complexity. NERC opted to

resolve the simplest changes in the first phase, while putting off more complex changes for later versions.

NERC filed the first phase of the modifications to the CIP Reliability Standards (Version 2) on May 22, 2009 and the filing is currently under review by commission staff. The filing includes removal from the standards of the terms "reasonable business judgment" and "acceptance of risk," which the commission found problematic, the addition of a requirement for a "single senior manager" responsible for CIP compliance, and certain other administrative and clarifying changes. The remaining phases of the CIP reliability standard revisions to respond to the commission's directives are still under development by NERC. Currently, there are no set time frames for the remaining phases.

Identification of Critical Assets

As currently written, the CIP reliability standards allow utilities significant discretion to determine which of their facilities are "critical assets and the associated critical cyber assets," and therefore are subject to the protection requirements of the standards. In the Final Rule, the commission directed NERC to revise the standards to require independent oversight of a utility's decisions by industry entities with a "wide-area view," such as reliability coordinators or the Regional Entities, subject to the review of the commission. This revision to the standards, like all revisions, is subject to approval by the affected stakeholders in the standards development process and has not yet been developed or presented to the commission. We expect this revision to be part of the remaining phases of CIP reliability standard revisions, as discussed above.

When the commission approved the CIP reliability standards in January 2008, it also required entities under those standards to self-certify their compliance progress every 6 months. In December 2008, NERC conducted a self-certification study, asking each entity to report limited information on its critical assets and the associated critical cyber assets identified in compliance with reliability standard CIP–002–1. As the commission stated in the Final Rule, the identification of critical assets is the cornerstone of the CIP standards. If that identification is not done well, the CIP standards will be ineffective at protecting the bulk power system. The results of NERC's self-certification request showed that 31% of responsible entities responding to the survey, and only 29% of generation owners and operators, identified at least one critical asset, while about 63% of transmission owners identified at least one critical asset. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009. In addition, NERC is working on a guidance document that will help industry to identify their critical assets. That document is still under development, and should be completed in approximately 6 months. Another self-certification by industry is due to NERC at the end of July, and includes additional questions designed to obtain a better understanding of the results from industry's critical asset identification process. Those results will help gauge how widely the CIP reliability standards have been applied.

The results of the NERC survey demonstrate that it is not clear, even today, what percentage of critical assets and their associated critical cyber assets has been identified and therefore made subject to the protection requirements of the CIP standards. It is clear, however, that this issue is serious and represents a significant gap in cybersecurity protection.

THE NERC PROCESS

As an initial matter, it is important to recognize how mandatory reliability standards are established. Under section 215, reliability standards must be developed by the ERO through an open, inclusive, and public process. The commission can direct NERC to develop a reliability standard to address a particular reliability matter, including cybersecurity threats or vulnerabilities. However, the NERC process typically requires years to develop standards for the commission's review. In fact, the existing CIP standards took approximately 3 years to develop.

NERC's procedures for developing standards allow extensive opportunity for industry comment, are open, and are generally based on the procedures of the American National Standards Institute. The NERC process is intended to develop consensus on both the need for, and the substance of, the proposed standard. Although inclusive, the process is relatively slow, open, and unpredictable in its responsiveness to the commission's directives.

Key steps in the NERC process include: Nomination of a proposed standard using a Standard Authorization Request (SAR); public posting of the SAR for comment; review of the comments by industry volunteers; drafting or redrafting of the standard by a team of industry volunteers; public posting of the draft standard; field testing of the draft standard, if appropriate; formal balloting of the draft standard, with

approval requiring a quorum of votes by 75 percent of the ballot pool and affirmative votes by two-thirds of the weighted industry sector votes; re-balloting, if negative votes are supported by specific comments; approval by NERC's board of trustees; and an appeals mechanism to resolve any complaints about the standards process. This process requires public disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments. NERC-approved standards are then submitted to the commission for its review.

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

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

In addition, a reliability standard submitted to the commission by NERC may not be sufficient to address the identified vulnerability or threat. Since FERC may not modify a proposed reliability standard under section 215 and must either approve or remand it, FERC would have the choice of approving an inadequate standard and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. Under either approach, the bulk power system would remain vulnerable for a prolonged period.

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

NERC's "Aurora" Advisory

Currently, the alternative to a mandatory reliability standard is for NERC to issue an advisory encouraging utilities and others to take voluntary action to guard against cyber or other vulnerabilities. That approach allows for quicker action, but compliance with an advisory is not mandatory, and may produce inconsistent and potentially ineffective responses. Also, an alert can be general in nature and lack specificity. For example, the issuance of an advisory in 2007 by NERC, regarding an identified cybersecurity vulnerability referred to as "Aurora," caused uncertainty about the specific strategies needed to mitigate the identified vulnerabilities and the assets to which they apply. Reliance on voluntary measures to assure national security is fundamentally inconsistent with the conclusion Congress reached during enactment of EPAct 2005, that voluntary standards cannot assure reliability of the bulk power system.

SMART GRID

The need for vigilance may increase as new technologies are added to the bulk power system. For example, Smart Grid technology promises significant benefits in

the use of electricity. These include the ability to better manage not only energy sources but also energy consumption. However, a smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points.

Smart Grid applications will automate many decisions on the supply and use of electricity to increase efficiencies and ultimately to allow cost savings. Without adequate physical and cyber protections, however, this level of automation may allow adversaries to gain unauthorized access to the rest of the company's data and control systems and cause significant harm. Security features must be an integral consideration when developing Smart Grid technology. The challenge will be to focus not only on general approaches but, importantly, on the details of specific technologies and the risks they may present.

Regarding data, there are multiple ways in which Smart Grid technologies may introduce new cyber vulnerabilities into the system. For example an attacker could gain access to a remote or intermediate Smart Grid device and change data values monitored or received from down-stream devices, and pass the incorrect data upstream to cause operators or automatic programs to take incorrect actions. As was mentioned previously, the potential exists for off-grid equipment to adversely affect the bulk power system through corrupted communications.

In regard to control systems, an attacker that gains access to the communication channels could order metering devices to disconnect customers, order previously shed load to come back on-line prematurely, or order dispersed generation sources to turn off during periods when load is approaching generation capacity, causing instability and outages on the bulk power system. One of the potential capabilities of the Smart Grid is the ability to remotely disconnect service using advanced metering infrastructure (AMI). If insufficient security measures are implemented in a company's AMI application, an adversary may be able to access the AMI system and could conceivably disconnect every customer with an AMI device. If such an attack is widespread enough, the resultant disconnection of load on the distribution system could result in impacts to the bulk power system. If an adversary follows this disconnection event with a subsequent and targeted cyber attack against remote meters, the restoration of service could be greatly delayed.

The CIP standards will apply to some, but not all, Smart Grid applications. The standards require users, owners, and operators of the bulk power system to protect cyber assets, including hardware, software, and data, which would affect the reliability or operability of the bulk power system. These assets are identified using a risk-based assessment methodology that identifies electric assets that are critical to the reliable operation of the bulk power system. If a Smart Grid device were to control a critical part of the bulk power system, it would be considered a critical cyber asset subject to the protection requirements of the CIP standards.

Many of the Smart Grid applications will be deployed at the distribution and end-user level so they may incorrectly be viewed as not affecting the bulk power system. For example, some applications may be targeted at improving market efficiency in ways that may not have a reliability impact on the bulk power system, such that the protection requirements of the CIP standards, as they are currently written, may not apply. However, as discussed above, these applications either individually or in the aggregate could affect the bulk power system.

The commission and its staff currently are coordinating with a number of Governmental and private sector organizations on cybersecurity issues surrounding Smart Grid technology, including the DOE Smart Grid Task Force, the NIST Domain Expert Working Groups, the Gridwise Architecture Council, and the FERC–NARUC Smart Grid Collaborative. The commission has issued a policy statement that would strongly encourage interoperability of Smart Grid technologies, recognizing that cybersecurity is essential to the operation of the Smart Grid. The Policy Statement stated that the commission will require a demonstration of sufficient cybersecurity protections in the proposed Smart Grid standards to be considered in rulemaking proceedings under the Energy Independence and Security Act of 2007 (EISA), including, where appropriate, a proposed Smart Grid standard applicable to local distribution-related components of Smart Grid. The commission also encouraged NERC to work with NIST in the development of the standards.

While the commission is doing what it can under its jurisdiction, EISA does not make any standards mandatory and does not give the commission authority to make or enforce any such standards. Under current law, the commission's authority, if any, to make Smart Grid standards mandatory must derive from the FPA.

PHYSICAL SECURITY AND OTHER THREATS TO RELIABILITY

The commission's current reliability authority does not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks and the Federal Government should have no less ability to act to protect against such potential damage. One example of a physical threat is an electromagnetic pulse (EMP) event. In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure. In 2004, the commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.

An EMP may also be a naturally-occurring event caused by solar flares and storms disrupting the Earth's magnetic field. In 1859, a major solar storm occurred, causing auroral displays and significant shifts of the Earth's magnetic fields. As a result, telegraphs were rendered useless and several telegraph stations burned down. The impacts of that storm were muted because very little electronic technology existed at the time. Were the storm to happen today, according to an article in Scientific American, it could "severely damage satellites, disable radio communications, and cause continent-wide electrical black-outs that would require weeks or longer to recover from."[2] Although storms of this magnitude occur rarely, storms and flares of lesser intensity occur more frequently. Storms of about half the intensity of the 1859 storm occur every 50 years or so according to the authors of the Scientific American article, and the last such storm occurred in November 1960, leading to world-wide geomagnetic disturbances and radio outages.

Further, the power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced power spikes. The collapse of numerous transformers across the country could result in reduced grid functionality or even prolonged power outages.

FERC staff has no data on how well the bulk power system is protected against an EMP event, and the existing reliability standards do not address EMP vulnerabilities. Further, the commission currently does not have any specific authority to order owners and operators of the transmission grid, generation facilities and other electric facilities to protect their facilities from EMP-related events, other than the general authority to order NERC to develop a reliability standard addressing EMP. Protecting the electric generation, transmission, and distribution systems from severe damage due to an EMP would involve vulnerability assessments at every level of electric infrastructure. In addition, as the reports point out, the reliable operation of the electric grid requires other infrastructure systems, such as communications, natural gas pipelines and transportation, which would also be affected by such an attack or event.

THE NEED FOR LEGISLATION

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

The commission's current legal authority is inadequate for such action. This is true of both cyber and non-cyber physical threats to the bulk power system that pose national security concerns. This lack of authority results in the electric grid being vulnerable to attacks, both physical and cyber.

---

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

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

Any new legislation should address several key concerns. First, to prevent a significant risk of disruption to the grid, legislation should allow the commission to take action before a cyber or physical national security incident has occurred. In order to protect the grid, it is vital that the commission be authorized to act before an attack to address vulnerabilities and threats. Second, any legislation should allow the commission to maintain appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Third, it is important that Congress be aware that if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would exclude protection against attacks involving Alaska and Hawaii, including any Federal installations located therein. The current interpretation of the term bulk power system also excludes some transmission and all local distribution facilities, including virtually all of the facilities in certain large cities such as New York, thus precluding possible commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas. Finally, it is important that entities be permitted to recover costs they incur to mitigate vulnerabilities and threats. The commission currently has authority to allow recovery by entities that meet the FPA definition of "public utility." If Congress believes it appropriate, it could include in legislation a directive that the commission establish a cost recovery mechanism for the costs associated with compliance with any FERC order issued pursuant to the emergency authority.

Finally, any legislation on national security threats to reliability should address not only cybersecurity threats but also intentional physical malicious acts (targeting, for example, critical substations and generating stations) and threats from an electromagnetic pulse. FERC should be granted authority to address both cyber and physical threats and vulnerabilities, primarily because FERC is the one Federal agency with any statutory responsibility to oversee reliability of the grid. This additional authority would not displace other means of protecting the grid, such as action by Federal, State, and local law enforcement and the National Guard. If particular circumstances cause both FERC and other Governmental authorities to require action by utilities, FERC would coordinate with other authorities as appropriate. Additionally, any FERC authority to address threats to the grid would be based on a determination by the President or a national security agency that national security is endangered.

CONCLUSION

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

Ms. CLARKE. Thank you very much, Mr. McClelland. Ms. Hoffman.

STATEMENT OF PATRICIA A. HOFFMAN, ACTING ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, DEPARTMENT OF ENERGY

Ms. HOFFMAN. Thank you, Chairwoman Clarke, Members of the subcommittee, for this opportunity to testify before you on electric sector vulnerabilities and cybersecurity issues.

For more than a decade, the Department of Energy has been engaged with the private sector to secure the electric grid. The Homeland Security Presidential Directive 7 designated the Department of Energy as the Energy Sector-specific agency and provided authorization to collaborate with all Federal agencies, State and local governments, and the private sector to conduct vulnerability assessments of the energy sector, and to encourage risk management strategies.

Securing the critical infrastructure is a shared responsibility and requires public-private partnerships. Asset owners bear the main responsibility for ensuring that key resources are secure and for

making the appropriate investments, for reporting emergency information to the Government, and for implementing protective practices and procedures.

With an economy that is in the process of recovering, it is even more critical that all energy sector stakeholders understand the available options, their associated costs, and the roadmap or path to a more secure energy infrastructure.

As we deploy Smart Grid technology, load management technology, plug in hybrid electric vehicles, distributed generation, micro grid, we may find that some measures may not be necessary, while new ones may emerge. The energy sectors threat analysis encompasses natural events, hurricanes, criminal acts, insider threats, and both 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. No single methodology or tool has been used to assess risk in the energy sector assets, such as what the Nuclear Regulatory Commission does with design basis threats.

Lessons learned from DBD analysis, in the nuclear industry could be applied to the electric industry, especially for large generating stations, large substations and major control centers.

To address the advancing capabilities of the global cyber threat as well as implementation of Smart Grid, the Department of Energy has requested an increase in our 2010 research budget for cybersecurity and energy delivery systems, from $12 million in 2009, to $50 million in 2010.

Activities proposed under this budget include, expanding our national SCADA test bed activities and cybersecurity assessments of control systems, utilizing existing control systems simulators as hosts for cyber training, develop trusted anchors to build trustworthy networks from untrusted components, and development of a cybersecurity Smart Grid test bed.

Currently, a laboratory industry and research effort to enhance the cybersecurity of the energy infrastructure has produced results in four areas. We have identified vulnerabilities, cyber vulnerabilities in energy control systems, and have worked with vendors to develop hardened systems that mitigate the risk.

Develop more secure communication methods between energy control systems in field devices. We have developed tools and methods to help utilities assess their security posture, and we have provided extensive cybersecurity training for energy owners and operators to help them prevent, detect, and mitigate cyber penetration.

The Department is working collaboratively with the private sector on several activities to ensure that cybersecurity is baked into the Smart Grid. Over the past year, the Department has been working collaboratively with the utilities communication architecture user group to develop security requirements for advanced metering infrastructure, a key application to the Smart Grid.

The Department is now working to leverage this effort in cooperation with the UCS user group to develop cybersecurity requirements for the full suite of Smart Grid technologies. Additionally, the Department is working on procurement standards as a part of this effort.

The Office of Electricity Delivery and Energy Reliability received $4.5 billion in the American Recovery and Reinvestment Act, of which about $3.4 billion is for grants for Smart Grid development and $650 million is for Smart Grid demonstration.

Cybersecurity should be addressed in every phase of the projects awarded under this funding, and includes design through on-going maintenance and support. The technical approach to cybersecurity should include in the proposals, a summary of cybersecurity risks and how they will be mitigated at each stage of the life cycle, a summary of the cybersecurity criteria utilized by vendor and device selection, a summary of the relevant cybersecurity standards or best practices that will be followed, a summary of how the projects support emerging cybersecurity standards.

In conclusion, the United States needs a comprehensive framework to ensure a coordinated response. The Government, in partnership with key stakeholders, should design an effective mechanism that integrates information from the Government and the private sector, and serves as a basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.

This concludes my statement, Chairwoman Clarke. Thank you for the opportunity to speak. I look forward to answering any questions you or your colleagues may have.

[The statement of Ms. Hoffman follows:]

PREPARED STATEMENT OF PATRICIA A. HOFFMAN

JULY 21, 2009

Thank you Chairwoman Clark and Members of the subcommittee for this opportunity to testify before you on electric sector vulnerabilities and cybersecurity issues.

All of us here today share a common concern that vulnerabilities exist within the electric system and that the Department of Energy, in partnership with the rest of the Federal Government and industry, should address the full spectrum of events, from high-impact, low-probability (HILP) to high-impact, high-probability. This is particularly true for Smart Grid systems, which by their very nature involve the use of information and communication technologies in areas and applications on the electric system where they have not been used before.

For more than a decade, the Department has been substantively engaged with the private sector to secure the electric grid. In December 2003, the Homeland Security Presidential Directive 7 (HSPD–7) designated the Department as the sector-specific agency (SSA) for the energy sector and provided authorization to collaborate with all Federal agencies, State and local governments, and the private sector, to conduct vulnerability assessments of the sector, and to encourage risk management strategies for critical energy infrastructure.

Securing critical infrastructure is a shared responsibility. Asset owners bear the main responsibility for ensuring that key resources are secure, for making the appropriate investments, for reporting threat information to the Government, and for implementing protective practices and procedures. As the SSA, the Department works closely with the private sector and State/Federal regulators to provide secure sharing of threat information and collaborates with industry to identify and fund gaps in infrastructure research, development, and testing efforts.

With an economy in the process of recovering, it is even more critical that all energy sector stakeholders understand the available options, their associated costs, and the roadmap or path to a more secure energy infrastructure. As we deploy Smart Grid technologies, load management technologies, plug-in hybrid electric vehicles and distributed generation/microgrids, we may find some measures may not become necessary, while new ones may emerge.

CRITICAL INFRASTRUCTURE PROTECTION AND RISK MANAGEMENT FRAMEWORK

Since the energy sector is characterized by very diverse assets and systems, prioritization of sector assets and systems is highly dependent upon changing threats and consequences. The significance of many individual components in the

network is highly variable, depending on location, time of day, day of the week, and season of the year.

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 and systems in the energy sector, a multitude of methodologies have been used to assess risks, vulnerabilities, and consequences. No single methodology or tool has been used to assess risks to energy sector assets, such as the Nuclear Regulatory Commission's design-basis threat (DBT) which is used to design safeguards and systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. Lessons learned from DBT analysis in the nuclear industry could be applied to the electric industry especially for large generating stations, large substations, and major control centers.

The exploitation of unintentional vulnerabilities has become one of the greatest concerns for potential disruption and high-consequence events. Control systems networks provide great efficiency and are widely used. However, they also present a security risk, if not adequately protected. Many of these networks were initially designed to maximize functionality, with little attention paid to security. With connections to the internet, internal local area and wide area networks, wireless network devices, and modems, some networks are potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could cause disruptions to the Nation's critical infrastructure.

The Department is planning to work with the Federal Energy Regulatory Commission and the North American Reliability Corporation (NERC) to examine the effects of HILP events on the bulk power system. The effort will focus on HILP events such as influenza pandemic, space weather, terrorist attacks, and electromagnetic pulses. The purpose of this effort will be to develop a framework to look at causes and consequences and provide a tool to summarize preparedness, response, recovery, and mitigation measures.

DOE does not have a program that would allow for private or publicly-owned utilities to receive Federal grants for hardening their equipment against an intentional or unintentional electromagnetic pulse.

CYBERSECURITY—INFORMATION SHARING AND EARLY DETECTION AND WARNING

The *Roadmap to Secure Control Systems in the Energy Sector (2006)* identified the need to improve information sharing between the Government and the private sector as a high priority. In their 2008 Annual Report, the Energy Sector Control Systems Working Group (ESCWG), which has worked in partnership with the Department to implement the Roadmap, stated that most information protection and sharing issues between the U.S. Government and industry still have not been resolved.

The Department of Homeland Security (DHS) receives the most complete intelligence related to critical infrastructure protection because of its cross-sector responsibilities. DHS's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) develops early intelligence warnings, which it shares with the Department. DHS alerts the US-Computer Emergency Readiness Team (US–CERT) and the North American Electric Reliability Corporation (NERC).

DOE does not have a separate alert system. DOE does, however, have mandatory reporting requirements for electric emergency incidents and disturbances (including cyber incidents) in the United States. Form OE–417, "Electric Emergency Incident and Disturbance Report," is used to alert DOE to electrical emergency incidents and disruptions within a 1-hour or 6-hour period depending on the type of emergency. This information allows the Department to quickly respond to energy emergencies that may impact the Nation's infrastructure. The information, collected from the electric power industry, helps DOE meet its overall national security and Federal Emergency Management Agency's National Response Framework responsibilities. DOE uses the data from this form to obtain situational awareness of energy emergencies of U.S. electric supply systems. DOE's Energy Information Administration (EIA) publishes the electric power emergency incidents and disturbances in its monthly EIA reports. The data may also be used to develop legislative recommendations, reports to Congress and as a basis for DOE investigations. When appropriate, information is shared with FERC.

Early intelligence warnings provide the industry and Government some insight into a potential attack but may not allow for timely defense against many of them. Besides early intelligence warnings, the Department recommends that the industry develop its own capabilities for monitoring rogue, malicious behavior on their systems. The industry should monitor communications on their systems just as they monitor system performance. Diligence in upgrading security software and protocols are essential to minimizing the impact of these events.

One of the challenges in creating an effective information sharing system is how to share classified intelligence information with State agencies and utility operators not cleared to receive this information. The DHS has been working to grant clearances to appropriate members of the community. An additional difficulty is the means by which the information can be communicated. For example, a security chief at a Regional Transmission Organization (RTO) may have a clearance, but not have any means of communication or storage to receive the classified information except through face-to-face communications.

CYBER STANDARDS

Improving the security of the electric sector will require coordination and cooperation between regulatory agencies and industry. Because the security of the electric grid does not rely solely on voluntary private-sector measures, much work is being done to develop necessary cybersecurity standards. The Federal Energy Regulatory Commission through the NERC Critical Infrastructure Protection (CIP) has mandated standards CIP–002 through CIP–009 to provide a security framework for the identification and protection of critical cyber assets that support reliable operation. In addition, the International Electrotechnical Commission (IEC) Working Group 15 of Technical Committee 57 is developing IEC 62351, focusing on power systems control, data communications, and security. The Power Engineering Society Substations workgroup is developing P1689, a trial use standard for retrofitting cybersecurity of serial Supervisory Control and Data Acquisition (SCADA) links in intelligent electronic devices for remote access. International Society of Automation security standard ISA99 addresses cybersecurity for control systems. The National Institute of Standards and Technology (NIST) is also developing specific recommendations and guidance for securing Smart Grid and other industrial control systems. It is clear that standards development is a priority, and this activity should be monitored closely for progress, implementation, and gaps.

DOE CYBER R&D PROGRAM

Our efforts to enhance the cybersecurity of the energy infrastructure have produced results in four areas. We have:

1. Identified cyber vulnerabilities in energy control systems and worked with vendors to develop hardened systems that mitigate the risks;
2. Developed more secure communications methods between energy control systems and field devices;
3. Developed tools and methods to help utilities assess their security posture; and
4. Provided extensive cybersecurity training for energy owners and operators to help them prevent, detect, and mitigate cyber penetration.

In 2003, the Department launched its National SCADA Test Bed (NSTB), a state-of-the-art national resource designed to aid Government and industry in securing their control systems against cyber attack through vulnerability assessments, mitigation research, security training, and focused R&D efforts. The Department has expanded the NSTB to include resources and capabilities from five national laboratories.

To date, researchers have assessed 90% of the current market offering of SCADA/Energy Management Systems (SCADA/EMS) in the electric sector, and 80% of the current market offering in the oil and gas sector. Twenty NSTB and on-site field assessments of common control systems from vendors including ABB, Areva, GE, OSI, Siemens, Telvent, and others, have led vendors to develop 11 hardened control system designs. Vendors have released countless software patches to better secure legacy systems, which are now being used by 82 system applications in the sector. Findings from NSTB vulnerability assessments have also been generalized by Idaho National Laboratory into its *Common Vulnerabilities Report,* which includes mitigation strategies asset owners across the sector can use to better secure their systems.

In 2005, the Department, in cooperation with the DHS and Natural Resources Canada, worked directly with experts in the oil, gas, and electricity industries to develop a detailed, prioritized plan for cybersecurity improvements over the next 10 years, including best practices, new technology, and risk assessment. The results of this work were published in the 2006 *Roadmap to Secure Control Systems in the Energy Sector,* which lays out a vision that in 10 years, controls systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function. Industry members defined goals, milestones, and priorities to guide the industry toward this vision.

Let me highlight two such projects that the Department is cost-sharing with the private sector to support the Roadmap:

- The Bandolier project, led by Digital Bond, is developing automated checklists of security configuration baselines, which, when deployed, can enable the audit of actual configuration settings against these baselines. Downloadable checklists have been developed and are now available for Siemens, Telvent, ABB, and SNC systems, and Digital Bond has worked to make its product available immediately and at a low cost to utilities by offering it as subscriber content on its website.
- The Hallmark project, led by Schweitzer Engineering Laboratories, is working to commercialize the Secure SCADA Communications Protocol originally developed by Pacific Northwest National Laboratory. The technology allows utilities to secure data communications between remote devices and control centers—a critical cyber access path. The technology will be available in a hardware device by mid-year.

The Department is also supporting research in academia through a multi-university R&D project entitled "Trustworthy Critical Infrastructure for the Power Grid (TCIP)." This project is led by the University of Illinois and includes Dartmouth College, Cornell University, Washington State University, and companies representing the spectrum of the electric power industry including utilities, vendors, regulatory bodies, control center operators, reliability coordinators, and market operators. TCIP is funded mainly by the National Science Foundation with supporting funds from the Department and the Department of Homeland Security, Science and Technology Directorate.

In addition to R&D and NSTB assessments, the Department supports extensive cybersecurity training to help asset owners learn security methods they can implement immediately to better secure their utilities. So far, the Department has trained more than 1,800 individuals in the energy sector and is also ramping up its new advanced Red Team/Blue Team training through Idaho National Laboratory. This week-long course invites asset owners to participate in a simulated attack scenario on an actual control systems environment, giving them hands-on attack and mitigation training.

In collaboration with the North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection Committee (CIPC), the Department leveraged its expertise and experience in cybersecurity assessments to develop foundational, intermediate, and advanced mitigations for the NERC "Top 10" vulnerabilities associated with control systems commonly used in the electric sector. The list was developed by NERC members including small, medium, and large entities across North America. The list is comprised of the most prevalent, most exploited, or highest-consequence vulnerabilities that a typical utility might find in their facilities. Utilities are encouraged to use this list to augment their risk management processes. Utilities also used the list as means to select vendors and purchase systems that had security "built-in."

In addition to its R&D and partnership initiatives, the Department is working collaboratively with the private sector on several activities to ensure that cybersecurity is "baked in" to the Smart Grid. Over the past year, the Department has been working collaboratively with the Utilities Communications Architecture (UCA) Users Group (including utilities, vendors, et al) to develop cybersecurity requirements for advanced metering infrastructure (AMI)—a key application for the Smart Grid. The group produced a document titled "AMI System Security Specifications" which will help utilities procure secure AMI systems. The Department is now working to leverage this effort in cooperation with the UCA User Group to develop cybersecurity requirements for the full suite of Smart Grid technologies.

The Department is also working with the ESCSWG to update the 2006 Roadmap. The update will incorporate new information and lessons learned, update end-states and milestones, and establish priorities that have come to the forefront since 2006, such as Smart Grid and wireless technologies. So far, the ESCSWG has identified gaps in the 2006 Roadmap, reviewed the Roadmap vision and goal structure, assessed changes in the control systems landscape, and collected ideas for implementation. In September 2009, the ESCSWG will bring together a broad section of asset owners and operators, researchers, technology developers, security specialists, and equipment vendors to establish new goals and prioritize control systems security needs in the energy sector. The ESCSWG plans to release the new roadmap in January 2010.

AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA)—TITLE XIII, SMART GRID

A Smart Grid uses information and communications technologies to improve the reliability, availability, and efficiency of the electric system. With Smart Grid, these technologies are being applied to electric grid applications, including devices at the

consumer level through the transmission level, to make our electric system more responsive and more flexible.

Enhanced grid functionality enables multiple devices to interact with one another via a communications network. These interactions make it easier and more cost-effective, in principle, for a variety of clean energy alternatives to be integrated with electric system planning and operations, as well as for improvements in the speed and efficacy of grid operations to boost electric reliability and the overall security and resiliency of the grid. The communications network, and the potential for it to enhance grid operational efficiency and bring new clean energy into the system, are key distinguishing features of the Smart Grid compared to the existing system.

The Office of Electricity Delivery and Energy Reliability received $4.5 billion in the ARRA, of which about $3.4 billion is for grants for Smart Grid development and $615 million is for Smart Grid demonstrations. In order to gain the greatest return on investment, this grant money will be disbursed in six areas: Equipment manufacturing, customer systems, advanced metering infrastructure, electric distribution systems, electric transmission systems, and integrated and/or crosscutting systems. The Federal funds for this program have been divided into two categories:

- Smaller projects in which the Federal share would be in the range of $300,000 to $20,000,000;
- Larger projects in which the Federal cost share would be in the range of $20,000,000 to $200,000,000.

Approximately 40% of Smart Grid Investment Grant (SGIG) funding will be allocated for smaller projects, while approximately 60% will be allocated for larger projects. DOE reserves the right to revise these allocations depending on the quantity and quality of the applications received.

DOE is working to reduce cybersecurity risks by including the following language in the grant announcement:

"Cybersecurity should be addressed in every phase of the engineering lifecycle of the project, including design and procurement, installation and commissioning, and the ability to provide on-going maintenance and support. Cybersecurity solutions should be comprehensive and capable of being extended or upgraded in response to changes to the threat or technological environment. The technical approach to cybersecurity should include:

- "A summary of the cybersecurity risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact).
- "A summary of the cybersecurity criteria utilized for vendor and device selection.
- "A summary of the relevant cybersecurity standards and/or best practices that will be followed.
- "A summary of how the project will support emerging Smart Grid cybersecurity standards."

DOE intends to work with those selected for award, but may not make an award to an otherwise meritorious application if that applicant cannot provide reasonable assurance that their cybersecurity efforts will provide protection against broad-based systemic failures in the electric grid in the event of a cybersecurity breach.

The following technical merit review criteria will be used in the evaluation of applications and in the determination of the SGIG project awards. The relative importance of the four criteria is provided in percentages in parentheses:

1. Adequacy of the Technical Approach for Enabling Smart Grid Functions (40%);
2. Adequacy of the Plan for Project Tasks, Schedule, Management, Qualifications, and Risks (25%);
3. Adequacy of the Technical Approach for Addressing Interoperability and Cyber Security (20%); and
4. Adequacy of the Plan for Data Collection and Analysis of Project Costs and Benefits (15%).

DOE's programs do not include grants to private or publicly-owned utilities for hardening their equipment against an intentional or unintentional electromagnetic pulse.

CONCLUSION

The United States needs a comprehensive framework to ensure a coordinated response by the Federal, State, local, and Tribal governments, the private sector, and international allies to significant incidents related to the Nation's electric power grid, particularly cyber. Implementation of this framework will require developing reporting thresholds, adaptable response and recovery plans, and the coordination, information sharing, and incident reporting mechanisms needed for those plans to

succeed. The Government, working with key stakeholders, should design an effective mechanism to achieve a true common operating picture that integrates information from the Government and the private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.

The focus should be on addressing the full range of threats and vulnerabilities to critical infrastructure versus the bulk power system and requires public-private and international partnerships.

Priority should be placed on deploying sensors for complete and greater depth in monitoring and diagnostics of physical and cyber events.

The Federal Government and industry must develop a security baseline and benchmark milestones for securing critical infrastructure.

As the capabilities of the threat continue to outpace our ability to develop and implement countermeasures, it is critical that control systems for critical applications be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical functions.

This concludes my statement, Chairwoman Clarke. Thank you for the opportunity to speak. I look forward to answering any questions you and your colleagues may have.

Ms. CLARKE. Thank you very much, Ms. Hoffman.

Mr. McGurk.

STATEMENT OF SEÁN P. MCGURK, DIRECTOR, CONTROL SYSTEMS SECURITY PROGRAM, NATIONAL CYBERSECURITY DIVISION, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. MCGURK. Thank you, Chairwoman Clarke, thank you, Member Lungren, distinguished Members of the subcommittee. I am Seán McGurk, the director of the Department of Homeland Security's Control Systems Security Program, and the director of the Industrial Control Systems Cyber Emergency Response Team, or the ICF CERT.

I am pleased to appear before you here today, to discuss the importance of securing control systems that operate our critical infrastructure including the Smart Grid. Control system electric power to operate the physical processes which produce the goods and services that we rely upon on a daily basis. Therefore assessing risk and effectively securing industrial control systems, is vital to maintaining our Nation's strategic interests, public safety, and economic prosperity.

In 2003, the Department of Homeland Security was designated as the lead agency for cybersecurity. Since then, several Homeland Security Presidential directives have established national policy and further outlined the Department's responsibility to collaborate with public and private sector entities to evaluate emerging technologies.

In May 2004, DHS created the control system security program. To further this mission and lead a cohesive effort focused on reducing the risk to control systems that operate the critical infrastructure. The CSSP recognizes that leading in these activities, such as understanding threats, vulnerabilities, and subsequent mitigation strategies, is essential to securing these systems.

To support our leadership role, CSSP funding for fiscal year 2009, is $22 million. This was an increase from a previous year's budget of $12 million that enabled us to expand and enhance our vulnerability discovery facility. This facility provides advanced ca-

pabilities that will aid in identifying the interdependencies of the critical infrastructures.

Additionally, the Federal workforce was increased from one position to an authorization of nine Federal employees. For fiscal year 2010, the President's budget request included an increase of $5.56 million for CSSP. Even with these enhancements, the requirements to evaluate new technologies and the ability to assess risk across the 18 critical infrastructures presents a challenge.

In order to understand the risk, it is important to understand the threats, including those actors and motivations, not only to control systems, but to digital computing in general. Common crackers or hackers comprise the most prevalent group of cyber attackers. They attempt to break in, in order to hack into computer systems to exploit flaws.

Often, motivation is data exfiltration for financial gain. Of greater concern are the hackers who install back doors such as trojans or root kits that enable them to remotely access the systems or the devices. The knowledgeable insider is probably the most dangerous threat to systems operation and security because this is someone who is trusted and has access to the networks and other important company information.

Cyber terrorists or, hacktivists, are those who seek to disrupt internet activity in the name of personal, political, or social cause or shared ideology. These individuals collaborate via cyberspace and work as an organized group against their target.

These challenges to security offer several opportunities for malicious actors to attempt to penetrate our systems, using the vulnerabilities and the advanced technologies that control our critical infrastructure. The CSSP evaluates risk, conducts operational risk management, and develops mitigation plans to manage risk to an acceptable level.

These activities include control system sector analysis, scenario development and the development of various tools and training products. In 2006, CSSP conducted the analysis based on the premise of using the electric grid to attack a facility. We demonstrated how a perpetrator could use the electric grid system to produce significant physical damage to the equipment and the systems.

The Aurora analysis highlights the importance of assessing risk, interdependencies, and the need to secure industrial control systems in order to maintain our Nation's strategic interests. While these efforts result in cybersecurity strategies that help to increase the overall security of the grid, they do not protect the grid from attack.

DHS works closely with responsible Federal agencies such as the Department of Energy and the Federal Energy Regulatory Commission, as well as the private sector, with the North American Electrical Liability Corporation, to provide mitigation measures that reduce the risk of cyber attack. The Secretary of Homeland Security takes these issues of securing our critical infrastructure very seriously.

Since 2004, this Department has conducted 148 assessments of electric sector facilities through the office of infrastructure protection. To further our mission, we lead a cohesive effort between Gov-

ernment and industry and the program created the Industrial Control Systems CERT to analyze and respond to private sector reports of control systems incidents.

We also engage with our Federal partners, such as the Department of Defense, the Department of Energy, and the intelligence community to address equities and mitigate the risks as we move forward. We also work closely with industry partners, such as NERC, to provide detailed analysis of cyber events in order to identify the risks and provide real-time, actionable information for asset owners.

Chairwoman Clarke, Ranking Member Lungren, and distinguished Members, I have outlined the role of the Department's Control Systems Security Program, and the role it will play in addressing the risk to technologies, including the Smart Grid. With your assistance, we will help the Department to continue to protect America.

Thank you again for this opportunity to testify, and I will be happy to answer your questions.

[The statement of Mr. McGurk follows:]

PREPARED STATEMENT OF SEÁN P. MCGURK

JULY 21, 2009

Chairwoman Clarke, Ranking Member Lungren, and distinguished Members, I am Seán McGurk, the Director of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP) at the National Protection and Programs Directorate. I am pleased to appear before you today to discuss the importance of securing the control systems that operate our critical infrastructure.

A control system is a general term that encompasses several types of systems, including Supervisory Control and Data Acquisition (SCADA), process control, and other automated systems that are found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes that produce the goods and services that we rely upon such as electricity, drinking water, and manufacturing. Control systems security in our electric power grid is particularly important because of the significant interdependencies inherent with the use of energy in all other sectors. Additionally, we rely on the electric grid to operate the Federal, State, and local, Tribal governments; therefore, assessing risk and effectively securing industrial control systems are vital actions to maintaining our Nation's strategic interests, public safety, and economic prosperity.

In 2003, the National Strategy to Secure Cyberspace designated DHS as the lead agency for cybersecurity. Since then, Homeland Security Presidential Directives (HSPD) 7 and 23 have established national policies and further outlined the Department's responsibility to collaborate with public and private sector entities to evaluate emerging technologies. Additionally, various Government Accountability Office (GAO) reports (e.g., GAO report: *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*) have further shaped Federal activities to improve the security of critical infrastructure and key resources (CIKR) by identifying the risks that could impact the networks that operate our critical infrastructure. In May 2004, DHS created the Control Systems Security Program (CSSP) to further this mission and lead a cohesive effort focused on reducing the cyber risks to the control systems that operate the CIKR.

To establish a framework to secure the CIKR, DHS issued the National Infrastructure Protection Plan (NIPP). This plan identifies the CSSP as responsible for leading activities to reduce the likelihood of success and severity of impact of cyber attacks against our Nation's control systems. The CSSP recognizes that understanding the threats, vulnerabilities, and subsequent mitigation strategies is essential in securing industrial control systems.

The CSSP funding for fiscal year 2009 is $22 million, an increase from the previous year's budget of $12 million that enabled us to expand and enhance the Advanced Vulnerability Discovery facility. This facility provides advanced modeling and simulation capabilities that will aid in identifying the interdependencies of the infrastructures. Additionally, the Federal workforce increased from one position to

an authorization for nine Federal employees. For fiscal year 2010, the President's budget request included an increase of $5.56 million for the CSSP. With these enhancements, DHS will be able to evaluate new technologies and begin assessing risk across additional CIKR sectors. CSSP continues to build a culture of reliability and security by partnering with Government agencies, industry, and the international community to reduce the cyber risks to U.S.-based control systems and evaluate emerging technologies such as the Advanced Metering Infrastructure and the Smart Grid for the energy sector.

In order to understand the risks, it is important to understand the threats, including actors and motivations, not only to control systems, but to digital computing in general.

- Common hackers comprise the most prevalent group of cyber attackers. They attempt to break-in or hack into computer systems or exploit flaws in software to circumvent systems security. Often the motivation is data exfiltration for financial gain. Other hackers install backdoors such as Trojans or other software such as rootkits that enable them to remotely access the system or device at a later date to perform a variety of nefarious actions.
- The insider is a dangerous threat to control systems because the individual has internal knowledge to processes and components. Insiders can defeat security measures put in place even when entities follow best practices and procedures.
- Cyber-terrorists or hacktivists are those who seek to disrupt internet activity in the name of a shared ideology or personal, political, or social cause. These actors collaborate via cyberspace and work as an organized group against their targets to further their political or social agenda. Web defacements, denial of service attacks, and redirects are the most common acts carried out against a target or targets.

These security challenges offer opportunities for malicious actors to attempt to penetrate our critical infrastructure using the vulnerabilities in advanced technologies such as the Smart Grid.

The CSSP evaluates risk and serves as the focal point for coordinating numerous resources to assist all critical infrastructure entities, including the members of the electric power grid. The CSSP conducts operational cyber risk management activities and leads strategic initiatives to develop the mitigation plans to manage cyber risk to an acceptable level. These activities include: Control systems sector analysis of vulnerabilities and interdependencies; scenario development; vendor product assessments; incident response activities; and the development of assessment tools, information products, and training.

In 2006, CSSP conducted an analysis based on the premise of using the electric grid to attack a nuclear facility (originally this was the "PANDORA" analysis that later became "AURORA"). This analysis was performed at the Control Systems Analysis Center (CSAC) operated by the Department of Energy's Idaho National Laboratory. The CSAC's analysis demonstrated how a perpetrator could use the electric utility system to produce significant nuclear plant apparatus and systems. It is important to note that this vulnerability was not related to a specific or imminent threat, and that the vulnerable control system and the equipment which could be damaged by an attack are often owned by two different entities. The analysis highlights the importance of assessing risk, interdependencies, and the need to secure industrial control systems in order to maintain our Nation's strategic interests, public safety, and economic prosperity.

While these efforts result in cybersecurity strategies that help to increase the overall security of the electric grid, they do not protect the grid from attacks. DHS works closely with the Department of Energy in providing mitigation measures that reduce the risk of cyber attacks, such as those exploiting the AURORA vulnerability. DHS works directly with the sector specific agencies such as the Departments of Defense and Energy, The Federal Energy Regulatory Commission (FERC) and the Nuclear Regulatory Commission (NRC), as well as with our private sector partners such as the North American Electric Reliability Corporation (NERC) to help them secure their infrastructure assets through voluntary programs.

The Secretary of Homeland Security takes the issue of securing our Nation's critical infrastructure very seriously and continues to emphasize an all-hazards approach to a safe and secure homeland. The CSSP focuses on a broad range of strategic cybersecurity initiatives related to securing the systems that operate the Nation's critical infrastructure, regardless of the cause.

Since 2004 the Department has conducted 148 assessments of electric sector facilities through the Office of Infrastructure Protection. These include cybersecurity assessments conducted by CSSP, which utilize several tools that we developed, such as the Control Systems Cyber Security Self Assessment Tool (CS2SAT) and the Cyber Security Vulnerability Analysis (CSVA). DHS and the other sector-specific

agencies perform these vulnerability assessments as directed in HSPD 7, which states that in accordance with guidance provided by the Secretary of Homeland Security, sector-specific agencies shall:

(a) collaborate with all relevant Federal Departments and Agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;

(b) conduct or facilitate vulnerability assessments of the sector; and

(c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

In addition to performing vulnerability analyses and assessments, the CSSP also created a series of recommended practices and informational products to assist owner-operators in improving the security of their control systems. These information resources are publicly available on-line at *http://www.us-cert.gov/control_systems/* and also are promoted through the monthly meetings held by the Cross-Sector Cyber Security Working Group, the Industrial Control Systems Joint Working Group's (ICSJWG) quarterly meetings, and other sector forums.

While products and tools allow asset owners and operators to understand the cyber risk to their control systems, it is essential that all stakeholders have knowledge of the fundamental principles of control systems security. To that end, we developed an advanced training center at the Idaho National Laboratory which includes functional models of critical infrastructure equipment. This center provides award-winning, hands-on training that ranges from introductory web-based courses to advanced, hands-on "Red Team/Blue Team" exercises and instructor-led classes. This effort has trained more than 14,000 professionals through both classroom and web-based instruction.

To further our mission and lead a cohesive effort between Government and industry, the Program created two overarching initiatives: the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) and the ICSJWG.

The ICS–CERT, in coordination with the Department's United States Computer Emergency Readiness Team (US–CERT), responds to and analyzes control systems-related incidents, conducts analyses of vulnerabilities and malicious software (malware), and disseminates cybersecurity guidance to all sectors through informational products and alerts. The ICS–CERT provides a more efficient coordination of control system-related security incidents and information sharing with Federal, State, and local agencies and organizations, the intelligence community, and private sector constituents including vendors, owner-operators, and international and private sector computer emergency response teams (CERTs).

Recently, the ICS–CERT responded to an incident at a public water utility, conducting on-site analysis of an event and providing recommendations to increase the security posture of the facility. Additionally, we conducted detailed digital media analysis of the system hard drive in order to determine the root cause of the incident. I am available to provide details of the incident in a classified brief at a later date. The CSSP and ICS–CERT regularly identify vulnerabilities and work with the vendors, owners, and operators of control systems to develop mitigation strategies tailored to their use and application in each of the critical sectors. We recognize there can be a gap between identification of a vulnerability and development of a vendor patch or full solution. To address this, the CSSP developed a Vulnerability Management Process operated by the ICS–CERT, in conjunction with trusted partners, to identify interim mitigation and consequence management approaches. We also engage with our Federal partners, such as the Departments of Defense and Energy as well as the intelligence community, to address equities and mitigate risks as we move from vulnerability identification, to risk assessment, to mitigation development and promulgation. These efforts help us evaluate new and emerging technologies such as Smart Grid, and the cyber risks that they introduce to control systems.

The ICSJWG follows a structured approach in accordance with the NIPP partnership framework and the Critical Infrastructure Partnership Advisory Council to continue the successful efforts of the Process Control System Forum to accelerate the design, development, and deployment of more secure industrial control systems. The ICSJWG is comprised of industry representatives from both private sector and Government coordinating councils and provides a vehicle for communicating and partnering across all CIKR sectors among Federal, State, and local agencies, and private asset owner-operators of industrial control systems. The ICSJWG and ICS–CERT collaborate with one another to leverage partnerships for information sharing and awareness of current threats and vulnerabilities. CSSP is also collaborating with the DHS Science & Technology Directorate (S&T) to ensure that their planned research and development in this area is well-informed and complements CSSP's related work with industry and owners/operators.

Implementation of the Smart Grid will include the deployment of many new technologies, such as advanced sensors to improve situational awareness, advanced metering, automatic meter reading, and integration of distributed generation resources. These new technologies will require the addition of multiple communication mechanisms and infrastructures that must be coordinated with the developing technologies and existing systems. Smart Grid deployment is likely to increase the complexity of the existing power grid system. Increased complexity and expanded communication paths could lead to an increase in vulnerability to cyber attack unless there is a coordinated effort to enforce security standards for design, implementation, and operation. As the lead agency for cybersecurity and preparedness, DHS is evaluating the risks and developing guidance to increase the security of control systems with the implementation of new technologies.

Chairwoman Clarke, Ranking Member Lungren, and distinguished Members, I have outlined the role the Department's Control Systems Security Program will play in addressing the risks that Smart Grid technologies will introduce to control systems. With your assistance, we will help the Department continue to protect America. Thank you again for this opportunity to testify. I will be happy to answer your questions.

Ms. CLARKE. Thank you, Mr. McGurk.

Our next testimony comes from Ms. Cita Furlani.

STATEMENT OF CITA M. FURLANI, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Ms. FURLANI. Member Lungren, and Members of the subcommittee. I am Cita Furlani, the director of the Information Technology Laboratory, at the Department of Commerce's National Institute of Standards and Technology.

Thank you for the opportunity to appear before you today, to discuss NIST's role in ensuring the cybersecurity and reliability of the information and communication aspect of the Smart Grid.

As the Nation's measurement and standards institute, NIST has earned a reputation as an impartial, technically knowledgeable third-party, with a long history of working collaboratively with industry and with other Government agencies. These strengths allow NIST to make a unique contribution to the establishment of the Smart Grid.

Recognizing the benefit of focusing this technical expertise in industry-oriented mission, on what is one of the Nation's most pressing issues, Congress, and the Energy Independence and Security Act of 2007, called on NIST to take a leadership role in ensuring an interoperable, secure, and open energy infrastructure, that will enable all electric resources, including demand-side resources, to contribute to an efficient, reliable electricity network.

NISTs three-phase approach is to build on the relationship with DOE, FERC, DHS, and other Federal agencies to engage stakeholders to achieve consensus on Smart Grid standards.

By early fall, the process will deliver the Smart Grid architecture framework, priorities for interoperability, and cybersecurity standards, and an initial set of standards to support implementation. In addition, plans to meet remaining standards needs.

Second, to launch a formal public-private partnership to facilitate development of additional standards to address remaining gaps and integrate new technologies.

Third, develop a plan for testing and certification to ensure that Smart Grid equipment and systems conform to standards for security and interoperability.

NIST views its role as accelerating the process by which the standards development can occur. The actual standards development work is a process that takes place largely in the private sector, with standards development organizations utilities, and other stakeholders.

NIST is reaching out to the private sector, and is using our expertise to identify where the barriers exist, where relevant standards currently exit, where standards exist but are not interoperable, and where gaps exist that require standards to be developed.

I would like to caution, however, that the process of creating comprehensive and effective standards can be time-consuming and difficult. To be effective, standards must be developed with broad representation and buy-in from all key stakeholders.

It can take time to do this right. But, NIST is establishing an agile framework that will meet the urgent national need for specific Smart Grid standards. For the reliability of the electric power industry to be fully realized, cybersecurity concerns must be addressed, in addition to assuring interoperability.

Congress recognizes, and is specifically calling out the issue of cybersecurity in the ESA legislation. This is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector, as it becomes more and more interconnected.

The need to address potential vulnerabilities has been acknowledged across the Federal Government. This need has also been cited in the 60-day cyberspace policy review.

With the adoption and implementation of the Smart Grid, the IT and telecommunications sectors will be more directly involved. These sectors have existing cybersecurity standards to address vulnerabilities, conformity assessment programs to evaluate cybersecurity products, and assessment programs to identify known vulnerabilities in systems.

Another issue for the Smart Grid, and the implementation of cybersecurity standards, is the concern that legacy equipment might be difficult to modify to meet new standards. Smart Grid cybersecurity strategy must address the addition and continual upgrade of cybersecurity controls.

The cybersecurity strategy will require the development of an overall cybersecurity architecture to address potential points of failure, conformity assessment procedures, and certification criteria for personnel and processes.

To achieve secure interoperability, products and systems will require conformity assessment that can be developed by NIST. Conformity assessment verifies that products adhere to the specifications define in the standards.

Once a standard has been published, conformity assessment can accelerate product development by giving vendors well-defined criteria to meet. Such testing should ensure that cybersecurity standards are affected and do not adversely impact interoperability.

NIST is proud to have been given such an important role in Smart Grid cybersecurity through the ESA legislation. We believe with the continued cooperation and collective expertise of the industry in this effort, we will be able to establish the cybersecurity standards to ensure the Smart Grid vision becomes a reality.

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

[The statement of Ms. Furlani follows:]

PREPARED STATEMENT OF CITA M. FURLANI

JULY 21, 2009

INTRODUCTION

Madame Chairwoman Clarke, Ranking Member Lungren, and Members of the subcommittee, I am Cita Furlani, the Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss NIST's role in ensuring the cybersecurity and reliability of the information and communication aspects of the Smart Grid as well as its physical security.

As the Nation's measurement and standards institute, NIST has earned a reputation as an impartial, technically knowledgeable third party with a long history of working collaboratively with industry and other Government agencies. These strengths allow NIST to make a unique contribution to the establishment of the Smart Grid.

Recognizing the benefit of focusing NIST's technical expertise and industry-oriented mission on what is one of the Nation's most pressing issues, Congress, in the Energy Independence and Security Act of 2007 (EISA) called on NIST to take a leadership role in ensuring an interoperable, secure, and open energy infrastructure that will enable all electric resources, including demand-side resources, to contribute to an efficient, reliable electricity network. Specifically, EISA gave NIST "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems . . . ". Cybersecurity and associated standards are being addressed as part of this Smart Grid Interoperability Framework that is under development.

NIST's three-phase approach is to:

- Build on the relationship with the Department of Energy (DOE), Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and other Federal stakeholders to further engage utilities, equipment suppliers, consumers, standards developers and other stakeholders to achieve consensus on Smart Grid standards. By early fall, the process will deliver:
  - the Smart Grid architecture framework;
  - priorities for interoperability and cybersecurity standards, and an initial set of standards to support implementation; and
  - plans to meet remaining standards needs.
- Launch a formal public-private partnership to facilitate development of additional standards to address remaining gaps and integrate new technologies.
- Develop a plan for testing and certification to ensure that Smart Grid equipment and systems conform to standards for security and interoperability.

After issuing the initial set of priorities, standards, and action plans in early fall, NIST will initiate the partnership and complete a testing-and-certification plan by the end of the year.

NIST views its role as accelerating the process by which the standards development can occur. NIST plans to implement the above-mentioned public-private partnership to serve as a mechanism to organize stakeholders and drive priority-setting of the standards. The actual standards development work is a process that takes place largely in the private sector, with standards development organizations, utilities, and other stakeholders. The duration of those processes will depend on the complexity of the specific problem. In some cases, it will occur very quickly—months—and in other cases, if it's technically very challenging, it may take considerably longer. But in the case of Smart Grid, NIST is moving as expeditiously as possible to get the framework set and move the standards development process along.

NIST is reaching out to the private sector and is using our expertise to identify where the barriers exist, where relevant standards currently exist, where standards exist but are not interoperable, and where gaps exist that require standards to be developed. With appropriations from the American Recovery and Reinvestment Act (Pub. L. 111–05), NIST is significantly expanding the public-private coordination so we can move more rapidly to make needed progress in Smart Grid interoperability standards. We are working closely at the interagency level to develop the detailed actions to support this expanded effort. This will allow us to define the interoper-

ability framework (system architecture); establish standards development priorities; support standards assessments; identify standards and conformity testing gaps; and accelerate standards development and harmonization efforts to provide the secure and reliable interchange of information that is necessary to accomplish the Smart Grid mission.

NIST will use the EPRI report in drafting the NIST Smart Grid Interoperability Standards Framework. The NIST document will describe a high-level architecture, identify an initial set of key standards, and provide a roadmap for developing new or revised standards needed to realize the Smart Grid. The first release of the NIST-prepared framework is planned to be available in September. In a *Federal Register* notice published on June 9, NIST released for public comment an *Initial List of Smart Grid Interoperability Standards.* This preliminary set of standards and specifications is identified for inclusion in the Smart Grid Interoperability Standards Framework, Release 1.0, and additional standards and specifications are anticipated to be included based on analyses of workshop input and public comments.

An initial step in this process is the release of a draft report, *Report to NIST on the Smart Grid Interoperability Standards Roadmap,* that identifies issues and priorities for developing interoperability standards for the Smart Grid. In a *Federal Register* notice published on June 30, 2009, NIST formally announced the availability for public comment of this nearly 300-page report, prepared under contract by the Electric Power Research Institute (EPRI).

I would like to caution, however, that the process of creating comprehensive and effective standards can be time-consuming and difficult. To be effective, standards must be developed with broad representation and buy-in from all key stakeholders. It can take time to do this right, but NIST is establishing an agile framework that will meet the urgent national need for specific Smart Grid standards. The proposed approach will provide that type of expert input through a voluntary consensus standards development process, while maintaining the aggressive schedule needed to develop the Smart Grid.

UNDERSTANDING THE RISK

For the reliability of the electric power industry to be fully realized, cybersecurity and physical security concerns must be addressed in addition to assuring interoperability. Congress recognized this in specifically calling out the issue of cybersecurity in the EISA legislation. This is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Existing vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.

Additional risks to the grid include:

- Increasing the complexity of the grid that could introduce vulnerabilities and disruptions and increase exposure to potential malicious attackers and unintentional errors;
- Linked networks can introduce common vulnerabilities;
- Increasing vulnerabilities to communication and software disruptions that could result in denial of service or compromise the integrity of software and systems;
- Increased number of entry points and paths for potential adversaries to exploit;
- Potential for compromise of data confidentiality, including the breach of customer privacy; and
- Increasing vulnerabilities to potential physical attacks or disruptions, such as those due to Electromagnetic Pulse (EMP), Electromagnetic Interference (EMI), and Geomagnetically-Induced Currents (GICs).

The need to address potential vulnerabilities has been acknowledged across the Federal Government including by NIST, DHS, DOE, and FERC. This need has also been cited in the 60-Day Cyberspace Policy Review, which states that " . . . as the United States deploys new Smart Grid technology, the Federal Government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks." With the adoption and implementation of the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cybersecurity standards to address vulnerabilities, conformity assessment programs to evaluate cybersecurity products, and assessment programs to identify known vulnerabilities in systems. These vulnerabilities need to be assessed in the context of the Smart Grid.

Another issue for the Smart Grid and the implementation of cybersecurity standards is the concern that legacy equipment may be difficult to modify to meet the

new standards developed. The issue of legacy equipment is not unique to the Smart Grid. There are many industrial control systems and IT systems that do not employ the most current suite of cybersecurity controls. In addition, the life cycle for information technology, particularly for software is very short—as short as 6 months for many applications—and the knowledge and skill level of adversaries to attack these systems continues to increase. To address this issue, the Smart Grid cybersecurity strategy must address the addition and continual upgrade of cybersecurity controls and countermeasures to meet increasing threats. These new controls and countermeasures may be allocated to stand-alone components within the overall Smart Grid architecture.

The overall cybersecurity strategy for the Smart Grid must examine both domain-specific and common requirements when developing a mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The following is a preliminary list of cybersecurity requirements applicable to the Smart Grid as a whole:

- Identification and authentication to components of the grid to system entities;
- Physical and logical access control to protect critical information;
- Integrity to ensure that modification of data or commands is detected;
- Confidentiality to protect sensitive information, including Personally Identifiable Information (PII) and proprietary information;
- Availability to ensure that intentional attacks, unintentional events, and natural disasters do not disrupt the entire Smart Grid or result in cascading effects;
- Techniques and technologies for isolating and repairing compromised components of the Smart Grid;
- Auditing to monitor changes in the Smart Grid;
- Supply chain security to ensure that products and services are not compromised at any point in the life cycle, a defense-in-breadth strategy; and
- Availability to ensure that intentional attacks, whether physical or cyber, unintentional events, and natural disasters do not disrupt the entire Smart Grid or result in cascading effects.

The cybersecurity strategy will require the development of an overall cybersecurity architecture to address potential single points of failure, conformity assessment procedures for Smart Grid devices and systems, and certification criteria for personnel and processes.

THE CYBERSECURITY STANDARDS LANDSCAPE

In addition to understanding and assessing the risks related to the Smart Grid's information and communications networks, it is important to gauge the applicability of existing and new cybersecurity standards to the Smart Grid. Several standards activities are on-going including:

- The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards CIP–002 through CIP–009, which provide a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Power System;
- The International Society for Automation (ISA) 99/International Electrotechnical Commission (IEC) 62443 suite of standards that address Security for Industrial Control Systems;
- The Advanced Metering Infrastructure Security task force (AMI–SEC), formed to define common requirements and produce standardized specifications for securing AMI system elements. These requirements are for electric utilities, vendors, and stakeholders; and
- NIST Special Publication (SP) 800–53, Recommended Security Controls for Federal Information Systems. This SP provides guidance for Federal agencies on cybersecurity controls with one section of the SP specifically addressing industrial control systems.

Although these standards are being developed by different standards bodies, there is significant interaction among the working groups. For example, there are current efforts to harmonize the NERC CIP, ISA99/IEC 62443, and NIST SP 800–53.

Standards are being assessed for applicability and interoperability across the domains of the Smart Grid, rather than developing a single set of cybersecurity requirements applicable to all elements of the Smart Grid. That is, the cybersecurity requirements of different domains, such as home-to-grid and transmission and distribution, may not be the same. For example, there are significant cybersecurity requirements to ensure the confidentiality of Personally Identifiable Information (PII) in the home-to-grid domain that may not be required at the transmission and distribution domain.

To achieve secure interoperability, products and systems will require conformity assessment that can be developed by NIST. Conformity assessment verifies that products adhere to the specifications defined in the standards. Once a standard has been published, conformity assessment can accelerate product development by giving vendors well-defined criteria to meet. Such testing should ensure that cybersecurity standards are effective and do not adversely impact interoperability.

COMMUNITY PARTNERSHIP

NIST is working with the International Society of Automation (ISA), the International Electrotechnical Commission (IEC), and the North American Electric Reliability Corporation (NERC) on current cybersecurity standards. NIST also works with other standards bodies, such as ISO, IEEE, and Internet Engineering Task Force (IETF) on cybersecurity standards. We will continue to coordinate with all these standards bodies in the development/revision of cybersecurity standards applicable to the Smart Grid.

To help ensure that we are addressing the cybersecurity requirements of the Smart Grid as part of the NIST Smart Grid Interoperability Framework, NIST has established a Cyber Security Coordination Task Group (CSCTG), including members from the Domain Expert Working Groups (DEWG) as well as cybersecurity and control systems experts from academia and the IT and telecommunications communities. The DEWGs are groups of technical experts established by NIST and the GridWise Architecture Council (GWAC) for information sharing on Smart Grid standards and interoperability issues in identified Smart Grid domains: Transmission and distribution, home-to-grid, business-to-grid, and industry-to-grid.

The CSCTG will coordinate among the DEWGs so that cybersecurity is addressed consistently and comprehensively in the DEWG discussions and work products. The focus of the CSCTG is to leverage the expertise of the members to identify the overall threats, vulnerabilities and risks to the proposed Smart Grid. In addition to cybersecurity, some physical security issues, including threat assessments related to electromagnetic pulse (EMP), electromagnetic interference (EMI) and geomagnetically induced currents (GIC), related to threat assessments, are also being considered within the CSCTG. This information will be used to identify the appropriate cybersecurity controls that will be allocated to various domains of the Smart Grid. The CSCTG is also considering a layered approach to cybersecurity to ensure that if one level is compromised, the next layer remains secure—a defense-in-depth strategy. These cybersecurity controls will be assessed by CSCTG members for effectiveness, scalability, and impacts on cost and the reliability of the Smart Grid, and will be integrated into the Smart Grid architecture from initiation. Interest is significant, and over 150 individuals have joined the CSCTG to date.

NIST will also coordinate closely with DOE, DHS, and FERC in the development of all Smart Grid cybersecurity products, and is also working closely with DOE, FCC and others to examine potential Smart Grid electromagnetic interference issues.

CONCLUSION

NIST is proud to have been given such an important role in Smart Grid cybersecurity through the EISA legislation. We believe that with the continued cooperation and collective expertise of the industry in this effort, we will be able to establish the cybersecurity standards, within the interoperability and standards framework, to ensure that the Smart Grid vision becomes a reality.

Thank you for the opportunity to testify today on NIST's work on Smart Grid cybersecurity. I would be happy to answer any questions you may have.

Ms. CLARKE. I would like to thank you, as well.

Ranking Member Lungren, and Members of the subcommittee, let me take a moment to request unanimous consent to insert additional written reports in testimony from the Canadian Electricity Association, the Industrial Defender Incorporated, Mr. Brian M. Ahern, and the Southern California Edison into the record.

Hearing no objections, so ordered.

I thank the witnesses for their testimony, and I will remind each Member that he or she will have 5 minutes to question the panel.

I will now recognize myself, for 5 minutes for questions.

Do any of you on the panel believe that the current FERC/NERC standard-setting process, where industry writes standards and self-

selects what assets it wants to secure, makes sense in the context of our national security?

We can start.

Mr. MCCLELLAND. No, the commission, the prior chairman and this chairman, and certainly this staff member, has been on record to say that the standards development process is adequate for routine matters attached to this power grid, the reliability of the power grid.

But for matters it would attack the bulk power systems, the power grid if you will, it is inadequate to protect against national security threats and vulnerabilities.

Ms. CLARKE. Anyone else's perspective on this?

Ms. Hoffman.

Ms. HOFFMAN. The standard-setting process is a process that does involve public and private partnerships in looking at baseline requirements for the system. The standard process can not be the only mechanism that is viewed as an opportunity to provide input into emergency and emergency requirements.

Ms. CLARKE. Mr. McGurk.

Mr. MCGURK. Madame Chairwoman, I concur with my colleagues. The challenge of coming up with operational or interoperability standards is usually followed through one process. But to respond to a threat, or respond to a vulnerability, requires emergency action, that may or may not be available given the current construct.

So, some challenges present themselves. Getting that information into the hands of the operators, and the authority needs to be there for the Government to direct that activity.

Ms. CLARKE. Yes.

Ms. Furlani.

Ms. FURLANI. I agree also, that when you start talking about interconnected systems, wherever the different types of systems touch is a vulnerable spot. There is not a—you really need an overarching understanding of the network and the architecture. You can't do it in isolated pieces.

Ms. CLARKE. Thank you, all. Let me direct my next question to Mr. McClelland and Mr. McGurk.

Can you please explain what additional authority you feel are necessary for FERC? And whether you think the language in H.R. 2195 is in line with what you are asking for?

Mr. MCCLELLAND. The commission requested, actually the chairman arrived at the position and again, staff concurred, that the commission needed additional authority in order to be able to direct action, measures to the industry to be able to communicate in a confidential manner.

Because the communications now, the information would have to have some assurance that the information would be protected there, regards cybersecurity or physical threats of our power system.

The commission would have a mechanism to engage industries, propose and direct to engage, industry and get a directive established to mitigate either a physical or a cyber threat.

The process under 215, by law, is open. So, if a standard were to be developed, it would have to be developed in an open forum.

So, not only the vulnerability or the threat would have to be disclosed, within the proposed mitigation.

It is not necessarily timely, because it is a very inclusive process that gets everyone to participate. It is not necessarily responsive, because the commission can't author a standard. It can't direct a specific measure.

It can make a directive to a specific mitigation. But it has no control over what might come back from industry.

So in that context, it is totally insufficient to assure that a vulnerability or a threat, either physical or cyber, has been addressed.

Mr. MCGURK. Yes, ma'am, from the standpoint of Department, we look at all the pending legislation and we look at opportunities to identify the best method to move forward. Of key concern, from our standpoint is, I go back to some of my previous experience as an arms control inspector under the START Treaty and INF Treaty.

We were directed to trust, but verify. There lies the key. I can issue a directive, but unless I have the ability to follow up and determine whether those actions were taken, I have no firm understanding whether or not the threat has been, or the risk has been mitigated.

So subsequently, language that addresses that opportunity, for whatever appropriate agency, will take those necessary steps, feel is vital to continuing the mission.

Ms. CLARKE. I am going to yield back the balance of my time and now recognize the Ranking Member of the subcommittee, the gentleman from California, Mr. Lungren, for his questions.

Mr. LUNGREN. Thank you very much, I would address this to all of you.

We talk about the Smart Grid. In some ways, it reminds me of some of the issues we had when we went to on-line banking. It is only going to be utilized by people. People are only going to have confidence in it if they feel that it is secure.

Are we doing what we need to do to make sure, as we develop the Smart Grid proposals at various levels, to build security into it?

Ms. HOFFMAN. Within the funding opportunity announcement, the Department of Energy did put very strict requirements for proposers to document and look at their cybersecurity aspect. They will have to include that in the proposals. So, we feel very comfortable with the language put in there that any proposers are going to have to address some of the elements that I have mentioned in my testimony as part of their Smart Grid projects.

Mr. LUNGREN. Let me put it another way. For other kind of enterprises, we have insurers who assess risk, and make insurance rates based on that risk. Obviously to mitigate those rates, you do certain things.

There are sometimes tax incentives. There are a whole host of things.

Is regulation the only and most effective way we can make sure that security is built into the Smart Grid? Or do we need to look at some of these other mechanisms as well?

Ms. HOFFMAN. If I may start, security is a service. It is a process that has to be included within the utility or within the Smart Grid infrastructure.

So, it is a service that must be maintained, just like we have service on our computers. So, it is a way to—it should be developed within the electric industry, so that there are companies, such as the ones you have heard of in the first panel, to provide the service to the industry as well as to the customers.

Mr. LUNGREN. Is there something we need to do to make sure that the rate structure allows for this?

Ms. HOFFMAN. Within the Smart Grid technologies, we are in within specific aspects of utility infrastructure. The rate structures can be used to support that.

For national security events, which is a public good, there are probably maybe other mechanisms that could be investigated.

Mr. LUNGREN. Well, let me ask you this, Mr. McClelland.

This goes to the question of EMP. We have heard low-probability, high-consequence. I would say the highest consequence.

Mr. MCCLELLAND. Yes.

Mr. LUNGREN. Almost. How do we ensure? Or, how do we provide incentives that the private sector and the—let's just concentrate on the private sector. The private sector will take seriously these sorts of things.

What I mean by that is this: If you are going to go to your whatever authority it is you have to go to for your rates, rate approval, and they say, "well, to justify your rates, you have to show us that there is a reasonableness to what you are doing, and what you want to charge for."

They go in and they say, "Well, low-probability, high-consequence." Does a rate-making organization authority in a State, or even a regional area, understand that? Do we need the focus of the Federal Government to actually have us take it seriously?

The reason I say that is, I just don't think we are taking this seriously enough. When you hear the testimony of the consequences, I mean, it makes "Katrina" look like a day in the park.

Mr. MCCLELLAND. Yes.

Mr. LUNGREN. Yet, after Katrina, we said, "Oh my god, we will never let that happen again. We have got to be more focused on it. We will put billions of dollars in to make sure that kind of thing doesn't occur."

Yet I don't sense that in terms of EMP. You seem to take EMP seriously.

Mr. MCCLELLAND. Yes.

Mr. LUNGREN. You seem to accept the argument that it could have devastating consequence.

Mr. MCCLELLAND. Yes.

Mr. LUNGREN. But yet it does not appear to me that we, either in the Congress or the Executive branch, have taken it seriously enough to make it the kind of priority that I would have. So I guess I would ask you, what do we need to do so that the range of costs that we have seen, the EMP Commission said that the range of costs to protect critical infrastructure components would range—could be from $150 million to $9 billion. That is a lot of change.

Do you believe Congress should provide cost recovery to utilities to cover these expenses through reimbursement by the rate payers? Is that reasonable? Is it something that Congress needs to do in terms of subsidies? Tax incentives? I mean, what do we need to do to make this happen?

Mr. MCCLELLAND. I would like to begin by—I will jump back for a second to your prior question about Smart Grid. Last week, the commission issued a policy statement under EISA. The commission's responsibility after NIST develops the standards, to codify the standard, to put the standards into place, to set the standards and in order that interoperability is established.

One of the key elements in the policy statement last week was that the commission would provide rate recovery and would even consider stranded costs for an entity that began to install Smart Grid equipment, but then the equipment was obsolete. It turned out to be obsolete, if the entity built in cybersecurity, that was one of the four elements.

So there is a cost recovery mechanism. The same application can and should be applied to EMP. It is unrealistic to think that entities, that utilities, will move forward on EMP mitigation measures in the context of high-risk low-probability.

If I just might say something about that, on the last panel there were two different witnesses, and I won't say who they are, but it was very telling. One witness classified it as high-risk, low-probability. A second witness, however, said high-risk low-frequency. There is a very big difference.

Mr. LUNGREN. Yes.

Mr. MCCLELLAND. Probability is not an assessment and I think you heard that very clearly, that without intelligence, without information, it is not an assessment that an entity or a person is qualified to make. That should be left to the folks that deal with intelligence.

So high-risk, low-frequency is a better way to classify it, coupled with a rate recovery mechanism. On the very end, I mean partnership is great, and we all hope that partnership works. But in the absence of a regulatory mechanism, to Mr. McGurk's point about trust and verify, in the absence of some regulatory mechanism to force an entity to take action, some entities just simply will not take action. Regulation is there for the entities that won't take action.

So I really believe, a personal perspective on this, and I was in the electric utility industry for 20 years before I came to Government for the past 5, that we knew about EMP, we knew about EMP mitigation measures. I saw a declassified report that showed a very specific attack vector and we were asked to evaluate that. I was asked as a controls and relays engineer. We did our job.

But the chance that industry would move forward, if it considers it to be a low probability of event, with everything else that is happening, is really not realistic.

Mr. LUNGREN. Thank you.

Ms. CLARKE. I now recognize Ms. Richardson, of California, a Member of the subcommittee, for her questions at this time.

Ms. RICHARDSON. Thank you, Madame Chairwoman.

Mr. McGurk, as you saw, I introduced you to one of the witnesses, who seemed to have made some attempts to reach out to the Department, but had not been successful. How long have you been in your position?

Mr. MCGURK. [Inaudible.]

Ms. RICHARDSON. Could you turn your microphone on?

Mr. MCGURK. Pardon me, Congresswoman.

I joined the Department in January 2008. In September 2008, I participated in a brief, hosted by the Department of Defense, for the cross-sector cybersecurity working group on the EMP process.

We also engaged with the doctors' group to evaluate the impacts on the critical infrastructure and produced a report in November, recognizing the importance of not only the impacts on the electric grid, but the other critical infrastructures across our country.

So we have been engaging across the board. The doctor has met with individuals from our infrastructure protection branch, so the comment about FEMA may have been miscommunications. But we have been engaged and engaging with his organization, focusing on EMP.

Ms. RICHARDSON. How much of your time, would you say, is spent on the issue of what we are talking about today? Cybersecurity within your jurisdiction?

Mr. MCGURK. I have the luxury, if you will, to focus my entire time on control systems, cybersecurity. That is what my program was created to do. So in all of the Department of Homeland Security, my organization focused specifically on cybersecurity and physical security threats to industrial control systems.

Ms. RICHARDSON. Who do you report directly to?

Mr. MCGURK. I report to the director of the national cybersecurity division.

Ms. RICHARDSON. Which eventually, who reports to the Secretary?

Mr. MCGURK. The under secretary for national preparedness and protection.

Ms. RICHARDSON. Is how far away from you?

Mr. MCGURK. Two steps removed. It is the director of the national cybersecurity division reports to the assistant secretary for cybersecurity and communications, who reports to the under secretary for NPPD, who reports to the Secretary.

Ms. RICHARDSON. So how often do you have an opportunity to report to the under secretary or Secretary, if at all?

Mr. MCGURK. I have briefed both the previous under secretary and Secretary and I have had the opportunity to brief the current deputy under secretary. I have not had an opportunity to brief the current Under Secretary Beers.

Ms. RICHARDSON. Okay. Did you have an opportunity to read the testimony of Dr. Graham and Mr. Fabro?

Mr. MCGURK. No, I did not have an opportunity prior to this meeting.

Ms. RICHARDSON. Do you have a copy of their testimony?

Mr. MCGURK. I do not.

Ms. RICHARDSON. Okay. I will make sure that you personally get it. I would be curious for you to read both of their testimonies. Towards the end of Mr. Fabro, he gives several specific recommenda-

tions and Mr. Graham, on page 5, he gives very specific recommendations. Would you be willing to read those?

Mr. MCGURK. Oh, absolutely, Congresswoman.

Ms. RICHARDSON. Okay.

Mr. MCGURK. Thank you.

Ms. RICHARDSON. Based upon what you heard so far today, is there anything that you would be in opposition to of what folks shared, things that we could do better?

Mr. MCGURK. I do want to emphasize that the previous panel's comments on public-private partnership, I think that is the key element. As was previously mentioned, regulation is just part of the equation. It is not the final solution. So there has to be an understanding and a collaborative effort between the private sector and the Federal Government to ensure that we address these issues.

We often focus on the critical asset owners. We miss the responsibility and the opportunity of dealing with the vendor community.

We actually have a subgroup in the industrial control joint working group that focuses on the vendors and brings the vendors to the table so that we can incentivize the development of more secure products for the future. That was a key part in developing our procurement standards, which we published in August of last year, identifying those steps necessary to develop and distribute and integrate more secure devices.

Ms. RICHARDSON. So do you reach out to traditional partners, the same ones you have always had? Or what do you use to reach out to some others? Because unfortunately, the testimony today was not consistent with what you have said.

Mr. MCGURK. We are attempting to reach out. The industrial control systems working group is following on the efforts that were established by the process control systems forum. So we are maturing and growing that activity. Again, much of our focus in the past was on primarily the energy sector, specifically the electric sector. Unfortunately, we need to focus on all 18 critical infrastructures.

So we have invested heavily in developing the partnerships with water, chemical, transportation, critical manufacturing, across the board, because when it really comes down to it, these industrial control systems are pretty much the same across all these industries.

The components that we use have the same vulnerabilities, whether it is moving a robotic arm that builds the car or generating power.

Ms. RICHARDSON. Okay. My last question, I have got 13 seconds, so if you could be brief in your reply.

Mr. MCGURK. Yes.

Ms. RICHARDSON. One of the things that stuck out to me was the procurement process that we have, many private enterprises that own many aspects of this whole area for us, and yet we are really not putting the things in place to ensure that they are doing the security aspect as well. Do you see improvements that could be made?

Mr. MCGURK. Absolutely. We can definitely improve that procurement process.

Ms. RICHARDSON. So could you provide those comments to this committee?

Mr. MCGURK. I—yes, I can.

Ms. RICHARDSON. Thank you very much. I yield back. Fifteen seconds.

Ms. CLARKE. I now recognize the gentleman from Maryland, Mr. Bartlett, for 5 minutes.

Mr. BARTLETT. Thank you very much, and thank you again for convening this hearing.

Mr. McClelland, I would like you to help me clear up a definition problem. On page 2 of your testimony, written testimony, on page 2 of Mr. Assante's written testimony, there are definitions of bulk prices and they seem to be different. You have a fairly restrictive one that exempts all local distribution facilities, including virtually all of the grid facilities in certain large cities.

The definition in Mr. Assante's written testimony says bulk power system is defined by, and he gives the section of the law, distributes and controls systems necessary for operating an interconnected electric energy transmission network or any portion thereof. Electric energy from generation facility needed to maintain transmission system facilities.

So his would appear to include anything and everything and yours would appear to exclude large portions of the system. Which one is correct?

Mr. MCCLELLAND. The NERC definition for bulk power system is defined as generally 100 kv and above. It is actually bulk electric system.

When EPAct 2005 was passed, it used a new term. Bulk power system. The commission, as you are probably aware, the commission issues a notice of proposal making, collects comments, considers the comments and then issues a final rule.

This was a section or a definition that was heavily commented on in the industry——

Mr. BARTLETT. Could you help us in getting, for your two agencies, a consistent definition, so we know what we are dealing with? I would appreciate that. Thank you very much.

I want to make a brief comment about a comment that Dr. Graham made about a robust EMP attack bringing down the power grid, and it might be out for several months or a year or more, and some might wonder how could that be? That is because if the grid comes down, it is very likely to take out large transformers. We don't make them. There are no spares. They are made somewhere overseas. If you order one, they will deliver one in a year or 18 months or so. That is how long it takes to make them, which is why that observation—why that observation.

Mr. McClelland, don't you think this might have been a good place to use the stimulus money, in hardening the grid? Wouldn't it make a lot of pretty good jobs?

Mr. MCCLELLAND. It sounds like a good idea.

Mr. BARTLETT. Thank you, sir. I agree. I agree. Okay.

Ms. Hoffman, you had mentioned that—does not have a program that would allow for private or publicly-owned facilities to receive Federal grants. What do we need to do to fix it? Could you fix it administratively? Or does that need legislation to fix that? Because we certainly ought to be helpful, don't you think? How much—do we have to do something or can you do it?

Ms. HOFFMAN. Within the Department, we set our priorities and there is no priority at this—or there is no activity at this time for that effort.

Mr. BARTLETT. Well, I would hope after this hearing that there would be. I would hope.

Mr. McGurk, this strikes me as a great idea, but the reality is that the more effective we are in producing a Smart Grid, the less secure we are from an EMP attack. Because that just increases our vulnerability. We really do need to do something about that.

You mentioned the state of units that are out there that are controlling all of this. Many of those components, nobody is around who made them. I have no idea where we get new ones.

Mr. MCGURK. Yes.

Mr. BARTLETT. They are saying that those are really, really old.

You mentioned national strategy to secure cyberspace. Sir, if there is, if Dr. Graham is correct, then there is a robust EMP lay down, there will be no cyberspace to secure. Do you think he is wrong?

Mr. MCGURK. Oh, absolutely not, sir.

Mr. BARTLETT. Good. Well, then, I hope we are doing something more than we are now doing because I see us doing—if it is zero to 100, I see us doing something about 0.05 in terms of hardening our system.

Ms. Furlani, how is EMP incorporated among the factors for developing Smart Grid standards? Are you doing that? Is this new grid going to be hardened for EMP?

Ms. FURLANI. It is one of the areas that we have in our long list. We are certainly taking it under consideration with our partners in BOE and SBC to understand where the standards needs might be.

Mr. BARTLETT. Well, I hope that this gets higher priority than it has had because as the testimony today indicated, we are enormously vulnerable here. Vulnerability encourages attack. It doesn't have to be a state actor, it could be a non-state actor.

I had a guy from the Department of Defense tell me there were no platforms out there from which these guys could launch this. Any tramp steamer is an adequate platform. A scud launcher goes up 180 miles apogee, that is plenty high enough to take out all of New England or all of California and other territories. A crude nuclear weapon, if you miss the target by 100 miles, it is just as good as a bull's eye. This is clearly, clearly, the most asymmetric weapon that any potential foe has.

Thank you very much. I yield back.

Ms. CLARKE. Thank you, Mr. Bartlett. You certainly have raised some very key and critical points that we must be vigilant around. Ms. Hoffman, you may not—we are telling you that this is really a priority. We want to ask you to please, take this back to Secretary Chu.

I now recognize, the gentleman from New Mexico, Mr. Luján for 5 minutes.

Mr. LUJÁN. Thank you very much, Madame Chairwoman. My questions go along the same questions that I asked the first panel. Around, my question is to if all G&T, generation and transmission companies, all distribution networks, and best-run utilities, rural

cooperatives are included in this broad definition of bulk power system, knowing that they are not.

With that being said, what are we doing to prepare to be able to address all those needs that fall outside of NERC's authority? I would pose that to the panel.

Mr. MCCLELLAND. I guess I would like to start by asking a clarifying question.

Is the premise that bulk power system includes all the G&T and distribution facilities?

Mr. LUJÁN. Well, for the most part, most G&Ts do fall under bulk power systems, with the exception of, I would say, a few that do fall out. But, the specific question is, for those that are not included under the definition of a bulk power system, G&Ts, IOUs, rural cooperatives, wherever they may be, including their distribution networks, what is occurring for the coordination there?

Because, according to some of the testimony from the last panel, that has already seems to have fallen, to some extent, under NERC. But, the remaining authority is presumed to fall upon Fed regulatory authorities or other entities, depending on the make-up of the utility.

So, what are we doing to include them as we begin to deploy some of the Smart Grid technologies that will be invested in?

Mr. MCCLELLAND. I guess, I would like to start with the bulk power system definition, is defined per region. So, the definition of bulk power system is very different in New England, for instance, than it is in the West that excludes many more facilities.

Now having said that, even the CIP standard, the NERC CIP standards for cybersecurity, it is this staff members' position and our Chairman's position, that Section 215 of the Federal Power Act, which is the reliability standard, is inadequate to protect the grid from a national security threat.

It is fine for everyday reliability matters. But, if there is an emergency action that is necessary to protect the grid from either a physical or a cyber attack, it is inadequate. That is why the commission has advocated, the Chairman has advocated, that the commission receive additional authority if the expectation is that the commission could protect it.

On the facilities that could fall outside of the bulk power system, the commission did issue a policy statement last week. It did say that, one of the items necessary for rate recovery is its Smart Grid appliances and devices must demonstrate conformity to cybersecurity. They must be protected from a cybersecurity standpoint.

So, the commission has used its authority that is advocating for additional authority to protect against national security threats.

Mr. LUJÁN. With that, Ms. Hoffman, if you could address that question as well? And go on to—based on the position that has been put out by FERC, with the position that Smart Grid investments have to comply with cybersecurity technology. Can grants also be applied for those reasons?

Or, can the funds be used in that way to make sure that they are investing in necessary cybersecurity preparation, or tools, platforms, software, whatever the application may be, or technology may be included in so many investments they will be making?

Ms. HOFFMAN. Yes, Congressman, your first question, the Department of Energy's program does not distinguish between the bulk power system. So, we are indifferent. So, we look at projects that will get the cybersecurity for the energy sector, looks at the energy sector as a whole.

As well as the Smart Grid activity does not distinguish projects between the bulk power system. We look at the bulk system as a whole, with respect to the Smart Grid. With respect to the Smart Grid, projects must look at cybersecurity aspects. So, it will be baked in, or as part of their proposal.

Mr. LUJÁN. Mr. McGurk.

Anything that you would like to add in regard there?

Mr. MCGURK. Congressman, I would just like to add that we are working with both the Department of Energy and also with the private industry to identify those requirements, doing the end-to-end.

As Ms. Hoffman had identified, we also, in the Department, look from the end-user, home delivery system back up without having a regard to any defined division between bulk power or the distribution networks.

So, we work across the board along with the Department of Energy to assist in identifying those cybersecurity vulnerabilities.

Mr. LUJÁN. Just a clarifying question, Ms. Hoffman. Does EMP also fall under what can be included with some of the dollars associated with the Smart Grid implementation? Do those safety standards, can they be included in some of the investments that will be made?

Ms. HOFFMAN. Right now, the Department does not have any activities for EMP hardening.

Mr. LUJÁN. Okay, thank you very much.

Then, Madame Chairwoman, just one question that I would like to pose to Ms. Furlani, and maybe she could submit it into the record in a written format?

But, just the same question I posed to the panel earlier as far as the lack of standards that do exist for the platforms, from a cybersecurity perspective, or some of the data systems that exist for energy companies. Should some standards be included there?

What is the Department looking at in order to be able to facilitate or respond to some of those questions? Or how do they evaluate them?

Thank you very much, Madame Chairwoman.

Ms. CLARKE. Thank you, we will do that.

I now recognize the gentleman from Ohio, Mr. Austria, for questions.

Mr. AUSTRIA. Thank you, Madame Chairwoman. Let me—I will keep my remarks brief. I know we have votes going on right now.

But, I think we all agree here today in this panel, that the electric grid remains highly vulnerable to the cyber and physical attack. That it could possibly disable a wide portion of the grid for weeks, months, and even possibly years.

As we move into the 21st century, moving towards new technology, and we push towards making electric infrastructure, electronic and digital, on the one hand, we are saving money, billions of dollars possibly, and we are making it much more quicker, much more reliable, a much more reliable system.

But on the other hand, we are also creating cyber and physical making vulnerable—the word just wouldn't come out, becoming more vulnerable.

I am, concerned that we don't have a comprehensive plan in place with that protection in place right now. Today, most of the critical electric infrastructure is owned and operated by the private sector.

Regulators of the electric grid currently have limited authority and require these electric utilities to secure their systems against cyber and physical attacks. This hearing has been very informative and eye-opening.

Just to recap on a couple of things, I want to ask Mr. McClelland first, and recap on what the Ranking Member started to go down this route, as far as—first of all, what should utilities do to better identify those critical cyber assets that are out there?

Then, the question has come up multiple times, as far as incentives. Should there be—are statutory requirements necessary to put those incentives in place to move to that direction?

Mr. MCCLELLAND. I will start starting with the identification of critical assets, which subsequent comes the identification of critical cyber assets, which then puts the facilities under the CIP standards.

NERC, itself, has begun the process to rectify this problem. The amount of critical assets that were identified was low. So, Mr. Assante, who is on the power panel, wrote a letter to industry saying, "Hey, rather than assume that your one particular facility in isolation on the whole power grid is not critical, you need to start from the assumption that you have to justify that it isn't critical."

In other words, you have to opt it out of the mix.

NERC is also preparing guidance documents to help entities review in aggregate, what everyone else is doing, a guidance document to identify critical assets.

Finally, when the commission approves its CIP standards, the commission identified this as a deficient area. So, it is not going to work if the utilities that are under regulation get to identify what is a critical asset, a critical cyber asset and what isn't.

Therefore, the commission directed BER to rewrite the standard, and bring the standards back to the commission. From that point on, from the time the standards would be revised, there will be a regional review process. Then those determinations will be subject to the commissions review.

Unfortunately, it is going to use the standards development process which can take years for it to get through, ballot through, and then come back to the commission. It may not be entirely responsive to the commissions directive.

That is the process under Federal Power Act——

Mr. AUSTRIA. I appreciate that. From a time constraint, let me have, Ms. Hoffman, your perspective on, since acting assistant secretary for the electricity delivery and energy reliability, DOE, as a specific sector agency for the energy sector, are you getting industry member cooperation for developing risk management strategies? And implementing security measures to protect their critical infrastructures?

Ms. HOFFMAN. My apologies. We are getting cooperation. We have focused on the vendor communities. We have taken several different approaches to looking at security improvements within the sector, working with the vendors, and working with the electric or energy companies directly, in assessing the technology for vulnerabilities, as well as improving the technology.

Mr. AUSTRIA. Madame Chairwoman, I am going to yield back my time. Because I know we have votes going. We don't want to miss the votes.

Ms. CLARKE. I want to thank each of you for your valuable testimony here today. I want to thank the Members for their questions.

Mr. Bartlett, thank you for your wisdom on this matter. Also, let the Members of the subcommittee know that if you have additional questions for the witnesses, we will ask for you to, you can submit them, and we will get it to you.

We ask that you will respond to us expeditiously in writing to those questions.

Hearing no further business, I want to thank you once again for your testimony here today. I know that there is a lot of inquiry coming from the membership with regard to this matter, a lot of interest and concern.

So, this is probably what we would call Part 1 of what will be a number of other hearings around this matter during this session. So, I want to thank you and just alert you to that.

This meeting is adjourned.

[Whereupon, at 5:42 p.m., the subcommittee was adjourned.]

APPENDIX I

LETTER FROM MICHAEL J. ASSANTE, CHIEF SECURITY OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

APRIL 7, 2009.

TO: Industry Stakeholders
RE: Critical Cyber Asset Identification

LADIES AND GENTLEMEN: In the interests of supporting NERC's mission to ensure the reliability of the bulk power system in North America, I'd like to take this opportunity to share my perspectives with you on the results of NERC's recently completed self-certification compliance survey for NERC Reliability Standard *CIP–002–1—Critical Cyber Asset Identification* for the period July 1–December 31, 2008 along with our plans for responding to the survey results. As you may already be aware, compliance audits on this standard will begin July 1, 2009.

The survey results, on their surface, raise concern about the identification of Critical Assets (CA) and the associated Critical Cyber Assets (CCA) which could be used to manipulate them. In this second survey, only 31 percent of separate (i.e. non-affiliated) entities responding to the survey reported they had at least one CA and 23 percent a CCA. These results are not altogether unexpected, because the majority of smaller entities registered with NERC do not own or operate assets that would be deemed to have the highest priority for cyber protection. In that sense, these figures are indicative of progress toward one of the goals of the existing CIP standards: To prioritize asset protection relative to each asset's importance to the reliability of the bulk electric system. On-going standards development work on the CIP standards seeks to broaden the net of assets that would be included under the mandatory standards framework in the future, but this prioritization is an important first step to ensuring reliability.

Closer analysis of the data, however, suggests that certain qualifying assets may not have been identified as "Critical." Of particular concern are qualifying assets owned and operated by Generation Owners and Generation Operators, only 29 percent of which reported identifying at least one CA, and Transmission Owners, fewer than 63 percent of which identified at least one CA.

Standard CIP–002 "requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System." The standard goes on to specify that these assets are to be "identified through the application of a risk-based assessment." Although significant focus has been placed on the development of risk-based assessments, the ultimate outcome of those assessments must be a comprehensive list of all assets critical to the reliability of the bulk electric system.

A quick reference to NERC's glossary of terms defines a CA as those "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Most of us who have spent any amount of time in the industry understand that the bulk power system is designed and operated in such a way to withstand the most severe single contingency, and in some cases multiple contingencies, without incurring significant loss of customer load or risking system instability. This engineering construct works extremely well in the operation and planning of the system to deal with expected and random unexpected events. It also works, although to a lesser extent, in a physical security world. In this traditional paradigm, fewer assets may be considered "critical" to the reliability of the bulk electric system.

But as we consider cybersecurity, a host of new considerations arise. Rather than considering the unexpected failure of a digital protection and control device within a substation, for example, system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations. I have intentionally used the word "manipu-

late" here, as it is very important to consider the misuse, not just loss or denial, of a cyber asset and the resulting consequences, to accurately identify CAs under this new "cybersecurity" paradigm. A number of system disturbances, including those referenced in NERC's March 30 advisory on protection system single points of failure, have resulted from similar, non-cyber-related events in the past 5 years, clearly showing that this type of failure can significantly "affect the reliability (and) operability of the bulk electric system," sometimes over wide geographic areas.

Taking this one step further, we, as an industry, must also consider the effect that the loss of that substation, or an attack resulting in the concurrent loss of multiple facilities, or its malicious operation, could have on the generation connected to it.

One of the more significant elements of a cyber threat, contributing to the uniqueness of cyber risk, is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyber attacker to impact multiple assets at once, and from a distance. The majority of reliability risks that challenge the bulk power system today result in probabilistic failures that can be studied and accounted for in planning and operating assumptions. For cybersecurity, we must recognize the potential for simultaneous loss of assets and common modal failure in scale in identifying what needs to be protected. This is why protection planning requires additional, new thinking on top of sound operating and planning analysis.

"Identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System" necessitates a comprehensive review of these considerations. The data submitted to us through the survey suggests entities may not have taken such a comprehensive approach in all cases, and instead relied on an "add-in" approach, starting with an assumption that no assets are critical. A "rule-out" approach (assuming every asset is a CA until demonstrated otherwise) may be better suited to this identification process.

Accordingly, NERC is requesting that entities take a fresh, comprehensive look at their risk-based methodology and their resulting list of CAs with a broader perspective on the potential consequences to the entire interconnected system of not only the loss of assets that they own or control, but also the potential misuse of those assets by intelligent threat actors.

Although it is the responsibility of the Registered Entities to identify and safeguard applicable CAs, NERC and the Regional Entities will jointly review the significant number of Table 3 and 4 entities [1] that reported having no CAs to determine the root cause(s) and suggest appropriate corrective actions, if necessary. We will also carry out more detailed analyses to determine whether it is possible that 73 percent of Table 3 and 4 Registered Entities do not possess any assets that, "if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

Additionally, NERC plans to host a series of educational webinars in the coming weeks to help Registered Entities understand CIP standards requirements and what will be required of them to demonstrate compliance with the standards once audits begin in July. NERC also plans to incorporate a set of informational sessions into this series, designed to allow the industry to share practices and ask questions of each other in an open, but facilitated, dialogue.

We expect to see a shift in the current self-certification survey results as entities respond to the next iteration of the survey covering the period of January 1–June 30, 2009 and when the Regional Entities begin to conduct audits in July.

I look forward to an on-going dialogue with you on these important issues. As always, please do not hesitate to contact me, or any of my staff, with any questions or concerns.

Sincerely,

MICHAEL ASSANTE,
Chief Security Officer.

STATEMENT OF THE NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

JULY 17, 2005

The National Association of Regulatory Utility Commissioners (NARUC) was requested to provide responses to a number of questions presented to NARUC staff

[1] Table 3 and 4 entities refers to those entities identified in the *Implementation Plan for Cyber Security Standards CIP–002–1 through CIP–009–1.*

by the subcommittee. The responses provided below are an attempt by the NARUC staff to provide factual responses to the questions posed by the subcommittee and do not necessarily reflect the official policy positions or views of NARUC and or its membership. We respectfully request that these responses be placed into the record of these proceedings.

What assets do State utility commissioners have jurisdiction over? How does this differ from the jurisdiction of FERC? Is there any cross-over?

The Federal Power Act gives FERC authority over the sale of electricity in inter-State commerce ("bulk power") and inter-State transmission. The States retain jurisdiction over unbundled transmission, generation, distribution, and retail rates.

There is some jurisdictional overlap. For example, the States and FERC have concurrent jurisdiction over reliability. Section 215 of the Federal Power Act provides FERC and NERC authority over reliability, but simultaneously asserts that this section does not preempt State authority "to take action to ensure the safety, adequacy, or reliability of electric service within the State, as long as such action is not inconsistent with any reliability standard." FPA § 215(i)(3). Similarly, transmission tariffs approved by FERC are folded into retail rates.

How does cost recovery work?

Cost recovery is generally established through a rate proceeding whereby a regulatory authority evaluates the costs that the utility requests to recover through rates. These costs may be initiated by the utility, or the utility make seek recovery for investments made in response to a Government mandate for something like increased security. Through a rate hearing, the regulatory authority evaluates the requested cost recovery to ensure that the cost conforms to their standards for approving the costs. These standards vary, including evaluations of whether the incurred cost was "used and useful," "just and reasonable," or prudently incurred. After evaluating the cost to see if it is recoverable, the regulatory authority generally specifies a mechanism by which the utility will recover the actual cost recovery. Cost recovery mechanisms include base rate changes to tariffs, adjustment clauses, deferral accounts, line item changes, or closed proceedings that allow for the confidential treatment of security costs.

What cost recovery mechanisms exist for utilities to recover costs for physical and cybersecurity protections?

State regulators are committed to allowing cost recovery of critical infrastructure costs that are prudently incurred. Generally this cost recovery goes through the standard rate case. Regulators have found that the existing inventory of cost recovery protocols and cost recovery mechanisms is sufficient. In some cases, State legislatures have stepped into reaffirm that required security costs are eligible for recovery, as long as the costs are reasonable and prudently incurred.

Does the current FERC/NERC standards-setting process for infrastructure protection (i.e. NERC writes, FERC approves or remands) make sense in a national security context? Does NARUC believe that industry-written standards are appropriate to protect assets as critical to national security as the electric system?

The NERC standards approval process meets the majority of grid challenges. The NERC process engages industry in the development of standards that FERC approves. This process results in mandatory standards for the bulk power system that are clear, technically sound and enforceable, and that garner broad support within the industry. NERC is continually improving its standards; it is striving to draw from the state-of-the-art in cybersecurity, through consideration of the National Institute of Standards and Technology (NIST) framework for cybersecurity, and to integrate that framework into NERC's existing Critical Infrastructure Protection standards. NERC has also implemented policies that allow for the confidential and expedient development of standards, including those related to cyber- and physical security.

Have any States required utilities to meet physical or cybersecurity standards that go beyond the NERC mandatory standards? If so, please provide States and standards required.

We are unaware of such State standards, but would be happy to contact our members and get back to you if we learn of any examples.

What are the key aspects of any piece of legislation that seeks to secure the electric grid from cyber and physical attack?

Cybersecurity legislation should not reinvent the wheel. It should continue to recognize and, if necessary, make more robust the FERC-NERC standards-setting proc-

ess. It should also recognize and respect the power system's existing State and the Federal jurisdictional boundaries.

The legislation should create a framework for improved information flow from the Federal Government to State regulators and industry of any known threat or vulnerability. This information flow would facilitate increased security for the grid infrastructure. It is critical that any information conveyed from the Federal Government to States or industry about a specific threat be timely and actionable to best enable a response. This information can enable a utility's expert operators and cybersecurity staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system.

In the case of actionable intelligence about an imminent threat to the bulk power system, it may be necessary for Government authorities to issue an order, which could require certain actions to be taken by the electric power industry. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC should be the Government agency that directs the electric power industry on the needed emergency actions.

Do the commissioners that comprise NARUC maintain any existing authorities that would allow them to require owners and operators of electric facilities to harden their equipment to mitigate the effects of an electromagnetic pulse?

Commission-authorized reliability investments generally require that the utilities protect against "all hazards." Although commissions generally do not prescribe against specific threats, "all hazards" standard of review mandates that utilities protect against, or create mitigation measures to limit detrimental reliability effects, from any anticipated threat, including an electromagnetic pulse.

Do the commissioners that comprise NARUC maintain any existing authorities that would allow them to require owners and operators of electric facilities to harden their equipment to mitigate the effects of a cyber attack?

Again, State regulatory authorities generally require utilities to protect against all hazards. NERC sets the cybersecurity standards. The commissions, including FERC within its authority over transmission, approve costs based on investments the utilities make to conform to these standards.

How many Smart Grid projects have been funded by commissioners thus far? In general terms, what are the security requirements for these projects?

California and Texas have approved the rollout of advanced metering infrastructure (AMI) with cost recovery. Texas requires that the electric utility have an independent security audit of the advanced meters and report the results of the security audit to the commission. (See Texas Substantive Rule §25.130, *http://www.puc.state.tx.us/rules/subrules/electric/25.130/25.130.pdf).* I believe that California is still evaluating the rules for the AMI rollout.

There may be additional Smart Grid projects that have qualified for cost recovery of which we are not aware.

With the rollout of the Smart Grid investment grants and Smart Grid demonstration projects under the American Reinvestment and Recovery Act of 2009, there will be a larger number of Smart Grid projects developed. These funding opportunity announcements discuss and prioritize security, and will certainly be a factor for consideration in the selection of these projects. Smart Grid projects, like all projects, must meet NERC's cybersecurity requirements. Additional security requirements and standards are under development. For example, NIST is working to develop cybersecurity standards for the Smart Grid, with a domain expert working group dedicated to the task. State commission staffs participate in the NIST cybersecurity working group. State commissions may choose to adopt and mandate the standards NIST develops for Smart Grid deployment within its jurisdiction.

Further, NARUC Critical Infrastructure Committee continues to monitor and educate its members on security threats and the evolution of the Smart Grid.

STATEMENT OF WILLIAM RADASKY AND JOHN KAPPENMAN

INTRODUCTION

We wish to thank the House Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology for inviting us to submit this written statement with regard to the protection of the critical electric infrastructure of the United States against cyber and other physical threats.

While this statement will draw upon the experience and capabilities of Metatech Corporation, headquartered in California with its largest operation in New Mexico, the opinions expressed in this statement are those of Dr. William Radasky, Ph.D., P.E., President of Metatech and Mr. John Kappenman, P.E., Metatech Consultant.

OUR CAPABILITIES AND EXPERIENCE

Metatech Corporation was founded in 1984, and in its early years focused its work completely on the understanding of the various forms of electromagnetic pulse (EMP) created by nuclear detonations (HEMP, SREMP, SGEMP, etc.). The purpose of understanding these intense electromagnetic fields was to determine the appropriate protection for military electronic systems so that these systems could still operate in the case of a nuclear burst. A burst at high-altitudes (defined as above 30 km) can create a high-altitude electromagnetic pulse (HEMP) that can illuminate the Earth within a line of sight. Two bursts at several hundred kilometers altitude could fully expose the entire United States. This type of EMP is considered one of the most severe due to its wide area of coverage and it near simultaneous illumination of electronic equipment and systems.

With the end of the Cold War and the subsequent reduction of nuclear stockpiles in the world, the threat of a major nuclear war has been reduced. On the other hand, the possibility of one or two nuclear bursts at high-altitudes launched by a terrorist organization over the United States seems to have increased (as suggested by the EMP Commission). In the early 1990s, Dr. Radasky began his work with the International Electrotechnical Commission (IEC) to examine the threat of HEMP to civil society. He has chaired IEC SC 77C since 1991, and this subcommittee has produced 20 voluntary standards and publications covering both HEMP and more recently the threat of electromagnetic weapons to civil society (known as IEMI). This committee has drawn upon the standard types of protection that are available within the electromagnetic compatibility (EMC) community and extended them to these more severe threats.

In the 1990s Dr. Radasky and Mr. Kappenman joined forces to examine the threat of geomagnetic (solar) storms on high voltage power grids. Mr. Kappenman had worked in this field for many years with the power industry, studying the impacts of storms on power grids, and Dr. Radasky and his colleagues had worked on advanced forms of electromagnetic numerical analysis stimulated by their earlier work on EMP. It was during this time that we discovered the very strong relationship between the impacts of geomagnetic storms and the late-time portion of the HEMP (known as E3) on the electric power grid. While the generation mechanisms of these disturbances are completely different, the waveforms produced and their impacts on the power grid are very similar.

At the present time Metatech Corporation is the leading company worldwide providing new developments and understandings relating to space weather (geomagnetic storms due to intense solar activity) and its impact on large power grids. Our company has in fact been involved in the vulnerability and risk assessment for the power grids in England and Wales, Norway, Sweden and portions of Japan. Metatech developed and provided continuous space weather forecasting services for the company that operates the electric power grid for England and Wales. Since May 2002, Metatech has been providing similar vulnerability and risk assessments for the U.S. electric power grid to the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP Commission). Metatech has carried out investigations for FEMA under Executive Order 13407 to examine the potential impacts on the U.S. electric power grid for severe geomagnetic storm events. In addition, Metatech work has been formative in the January 2009 Report by National Academy of Sciences "Severe Space Weather Events—Understanding Societal and Economic Impacts Workshop Report". The assessments performed by Metatech indicate that severe geomagnetic storms pose a serious risk for long-term outages to major portions of the North American grid. While a severe storm is a low frequency of occurrence event, it has the potential for long-duration catastrophic impacts to the power grid and the country. The impacts could persist for multiple years with the potential of significant societal impacts; in addition the economic costs could be measured in the several trillion dollars per year range and could pose the risk of the largest natural disaster that could affect the United States.

WHAT IS HEMP AND HOW DOES IT IMPACT THE POWER SYSTEM?

As indicated earlier, HEMP is produced by a nuclear detonation above 30 kilometers altitude. Intense electromagnetic fields are produced in space by the high-energy radiation leaving the detonation, and these fields propagate downward to the Earth's surface. Because of different types of interactions, there are actually three

main pulses created, covering three time frames: Less than 1 microsecond, from one microsecond to 1 second, and beyond 1 second. These time regimes have been given the notations of E1, E2, and E3, respectively. As we will discuss in this statement, each of these "pulses" creates different types of problems in modern electric and electronic equipment and systems; this is due to the "coupling" of the electromagnetic fields to the electric power lines themselves and to the control wiring in substations and power generation facilities.

WHAT ARE OTHER SIMILAR EM THREATS THAT CAN BE DEALT WITH AT THE SAME TIME?

There are two other significant power system electromagnetic threats of concern to power systems. One is a geomagnetic storm, which begins with the ejection of charged particles from the Sun; these particles travel to the Earth and create large current flows in the ionosphere at levels of up to millions of amperes for a severe storm. The frequency of occurrence of geomagnetic storms follows the solar cycle (~11 years), but it is expected that severe storms with the potential for catastrophic impacts to power grids in the United States occur once every ~30 years, based on historical evidence. As in the case of the E3 HEMP, this electromagnetic disturbance couples well to long transmission lines and creates geomagnetically induced currents (GICs) that can create power blackouts and damage to large transformers.

Another electromagnetic threat of concern is that produced by electromagnetic weapons used by criminals or terrorists producing intentional electromagnetic interference or IEMI. These weapons have become more powerful and easier to obtain in recent years due to advances in solid-state electronics. These electromagnetic fields are very similar to those produced by E1 HEMP and will impact the electric power system in a similar fashion. The main difference is that the area affected by IEMI is much less than for HEMP, although the attack is silent and would not be understood in the same way as a cyber attack. In addition an IEMI attack would not leave any trace to determine how the attack occurred, since the electromagnetic fields would arrive simultaneously at several locations in a system, creating multiple failures of hardware and software.

WHAT EFFECTS ARE EXPECTED ON THE POWER GRID FROM HEMP?

For the operation of the electric power grid, the HEMP E1 and E3 pulses are the most important. Research performed for the EMP Commission clearly indicates the following concerns:

(1) Malfunctions and damage to solid-state relays in electric substations (E1);
(2) Malfunctions and damage to computer controls in power generation facilities, substations, and control centers (E1);
(3) Malfunctions and damage to power system communications (E1);
(4) Flashover and damage to distribution class insulators (E1);
(5) Voltage collapse of the power grid due to transformer saturation (E3);
(6) Damage to HV and EHV transformers due to internal heating (E3).

It should be noted that these effects could result in widespread blackouts due to the large geographic footprint of these environments and the fact that they are simultaneous in nature. In particular a single high-altitude burst above the United States would create an E1 pulse that would arrive at all locations within one power cycle. In addition, widespread damage, especially to HV and EHV transformers could require years to recover due to worldwide production limits.

COSTS OF HARDENING

Given the potentially enormous implications of power system threats due to space weather, it is important to develop effective means to prevent a catastrophic and crippling failure of the electric power grid. Recent detailed examinations also conclude that the United States and other world electric power grid infrastructures are becoming more vulnerable to disruption from geomagnetic storms and E3 HEMP environment interactions for a wide variety of reasons. This trend line suggests that even more severe impacts can occur in the future for reoccurrences of large geomagnetic storms. These trends of increasing vulnerability remain unchecked, as no design codes have been adopted to reduce geomagnetically induced current (GIC) flows in the power grid during such a storm. Present operational procedures utilized by U.S. power grid operators largely stem from experiences in recent storms, including the March 1989 storm, while storms as much as ten times larger than this storm are only recently understood to have occurred before with the certainty they will occur again. In retrospect, it is also now clear that present U.S. power grid operational procedures are based largely on this out-of-date storm experience, and these procedures will not reduce GIC flows sufficiently; therefore these current procedures are unlikely to be adequate to prevent widespread blackout or damage to

key equipment for historically large disturbance events in the future. The same trend line and theme of increasing vulnerability is also true with respect to the fast transient effects of the HEMP E1 and IEMI threat conditions.

Since both hardening and improved operational mitigation development is necessary, it may be helpful to define these terms more clearly. Hardening is a process of modifying the power grid in order to block or reduce GIC in key transformer assets. Operational mitigation is the action of taking various operational actions for the purpose of posturing the power grid (or key assets) to minimize GIC exposure (e.g., removing spare transformers from service based upon an alert/forecast of a severe storm). This combination provides a layered and complimentary approach, in that both act to improve the security of the grid. It is also important that both actions are functionally independent, in that failure to enact a timely or proper operational procedure does not defeat the hardening measures, which reduce the GIC. Infrastructure hardening is clearly the more effective and reliable approach; operational mitigation is highly dependent on the quality of alert/forecast capability and the fact that the varying states of power system operation during a storm may limit the range of effectiveness and flexibility for taking meaningful actions.

E1 HEMP standards and network upgrades

Presently in substations and other power grid facilities, relay and control devices span many generations of designs from electromechanically operated relays to multi-function microprocessor based relays and control devices. The widespread applications of multi-function devices are being used to provide added capabilities to the operation of the power grid; however these devices introduce new vulnerabilities to the E1 HEMP environment. Existing standards have taken into consideration the unique and harsh electromagnetic environment common in a high-voltage substation. As a result there are a variety of standards for substation-based protective relays and relay support systems that have evolved over the years. While these evolutions provide protection against some of the threats posed by the E1 HEMP environment, some gaps and shortfalls in immunity test threshold levels continue to exist that if filled would make these devices more robust in their ability to withstand the E1 HEMP or IEMI threats. While the current electromagnetic transient test levels of concern are from sources not related to the E1 HEMP or IEMI environments, some of the similarities illustrate the significant opportunities that are possible for dual application.

Many activities are currently underway within the IEEE and International Electrotechnical Commission (IEC) to update and improve the EMC immunity of electronic equipment used in factories, power substations and power-generating stations including nuclear power plants. The IEC has developed a set of electric fast transient (EFT) tests that are very similar to the waveforms coupled by E1 HEMP to cables. The EFT test pulse has a rise time of 5 ns and a pulse width of 50 ns. The typical EMC test levels suggested are between 1 and 4 kV. As noted in Metatech's work, EI HEMP can under some circumstances produce more than 10 kV, with a similar waveform. Of particular interest is the fact that some companies in the European power industry have suggested that higher levels of immunity test standards be applied to power system control electronics. It is clear that if EM standards are developed that have a dual application (normal usage and HEMP), then the possibility of acceptance of these standards will be more positive. In addition, recent work led by Metatech with Cigré is examining the additional protection that would be required in substations to eliminate the threat of IEMI. Protection against IEMI would provide protection against E1 HEMP.

Given the on-going work and the fact that the United States has several HEMP and power system experts involved in the work of the IEC, these new international standards could be analyzed for their application to power system equipment in the United States to improve the hardness of the overall power system to HEMP. In addition to the EMC work, there is also continuing work in the IEC to develop further HEMP standards for the civil infrastructure with heavy participation of several U.S. HEMP experts. This work should be directly supported through research funding to develop cost-effective ways to apply the new IEC standards to improve the hardness of important civil systems.

As the EMP Commission Report has noted, there are several thousand major substations and other high-value components on the transmission grid. With the development of standardized and hardened equipment, a continual program of replacement and upgrade with HEMP-hardened components will substantially reduce the cost. The estimated cost for HEMP-hardened replacement units and HEMP protection schemes is in the range of $250 million to $500 million. Approximately 5,000 generating plants of significance will need some form of added protection against

HEMP, particularly for their control systems. As the EMP Commission noted, these costs are in the range of $100 million to $250 million.

Power grid hardening and mitigation for E3 HEMP and geomagnetic storms

Both the E3 portion of a HEMP environments and naturally occurring geomagnetic storms can cause the flow of geomagnetically induced currents (GIC) through transformers in an exposed power grid. The GIC, if large enough, can disrupt the AC performance of the grid causing initial blackouts and also creating the potential for permanent damage to large transformers, which can lead to restoration delays of the power grid. Hardening of the power system is optimally done through the application of passive devices or circuit modifications that block or reduce the flow of GIC in a power grid. Because GIC accesses power systems through the multiplicity of grounded neutral leads of wye-connected transformers, the most effective point at which to place blocking or limiting devices is also in these neutral-to-ground leads. Neutral GIC blocking devices have been actively researched since the early 1990s, and several hardware versions have been successfully deployed for blocking stray DC or GIC flows into exposed transformers.

The analysis performed to date for the EMP Commission by Metatech indicates that the conceptual design of installing neutral resistors on the transformer neutral-to-ground connections is the preferred option of protection. These resistors would be low resistance—on the order of 5 ohms. Even though small, they would substantially increase the resistance in the power line network; since they are located in the neutral to ground connection, they would not substantially decrease the efficiency of operation of the power grid. These devices would allow a significant reduction of the GIC currents induced (around 60% reduction in overall GIC levels are estimated from the studies). The advantage of this design is that it will be relatively simple to develop with lower engineering trade-off risks and lower overall installed costs compared other more exotic devices. In order to evaluate this option more completely, it will be necessary to carefully study the economic aspects of this approach and to move forward with a funded R&D effort to fully engineer and test the prototypes.

The EMP Commission in their report estimated costs for switchable ground resistors for high-value transformers are estimated to be in the range of $150 million. Further studies are needed to determine the number and location of high-value transformers, but preliminary estimates are for some ~5,000 such transformers to be considered on the 230 kV, 345 kV, 500 kV and 765 kV networks. These cost estimates are based upon simple devices that are still at a conceptual stage of development. Metatech has been briefing various interested Government agencies and organizations on a comprehensive R&D program that would finalize the design requirements for the protection system and would develop better estimates of costs; therefore total costs several times larger than the previous EMP Commission estimate might be foreseeable.

With respect to the overall cost of hardening, it is also important to keep in mind the cost of outages, even when they are of short duration. A hardening program that expends even as much as ~$1 billion to protect the U.S. power grid against a severe geomagnetic storm, an event that has occurred before and is certain to occur again, is still far cheaper than the costs of a widespread blackout to the U.S. economy. For example the DOE estimated that the August 2003 blackout, (affecting ~60 million people in Midwestern and NE United States) cost about $10 billion. If we instead only elect to black out or shut down the power grid based on forecast alerts of this sort of event, it would cost more than 10 times the hardening cost just in terms of the economic impact to the United States. When one factors in that forecasts will no doubt come with false alerts, then the costs of hardening are indeed quite prudent.

OPERATIONAL MITIGATION TRAINING

The EMP Commission also recognized the importance of developing a capability to monitor and evaluate the unique set of adverse effects on critical systems and to speed their restoration. Operators and others in a position of authority must be trained to recognize that a HEMP attack, an IEMI attack or a severe geomagnetic storm is occurring or is about to take place. This should be done in order "to understand the wide range of effects it can produce, to analyze the status of their infrastructure systems, to avoid further system degradation, to dispatch resources to begin effective system restoration, and to sustain the most critical functions while the system is being repaired".

The detailed power grid models that have been employed by Metatech for the EMP Commission and FEMA studies provide an excellent starting point to develop a comprehensive training program and operational avoidance procedures for the

U.S. power industry to counter the harmful impacts from the E3 HEMP and severe geomagnetic storm environments.

As the EMP Commission and others have suggested, efforts to promote training centers that would have the mission of simulating, training, exercising, and testing both operational avoidance and recovery plans are important for the country. These training centers would allow the comprehensive simulation of HEMP and other major system threats, such as geomagnetic storms or coordinated terrorist attacks, whether they are physical or electromagnetic in nature (IEMI). These training centers would aid in the development of procedures for addressing the impact of such attacks to identify weaknesses, to provide training for personnel and to develop HEMP response procedures and coordination of all activities across appropriate agencies and industry.

Better and more appropriate procedures can be developed such as:

- Making decisions to remove certain high-value assets (such as EHV transformers) from operation in the network to reduce their exposure to damaging GIC levels.
- Making decisions to remove key generating plant transformers from operation again to reduce their exposure to damaging GIC levels.
- Making decisions to reduce or shed load (or to create limited blackouts) in portions of the grid to reduce exposure of high-value assets to damaging E1, E3, or severe geomagnetic storm environments.
- Making decisions on additional staffing under alert conditions to perform manual overrides, where possible, of operational controls that could be compromised due to E1 impacts.

ALERT CAPABILITIES

In 1998, the National Grid Company, which operates the power grid for all of England and Wales, awarded Metatech a contract to develop and operate the world's first geomagnetic storm forecasting service using solar wind electrojet models. These operational electrojet models are driven by solar wind data from the ACE L1 satellite. This detailed electrojet model provided a predictive forecast capability needed by the electric power industry. Large and sudden storm onsets can erupt on a planetary scale within a matter of minutes, meaning that power systems that are concerned about the impact of these disturbances will not have any meaningful lead-time available if they depend upon local real-time monitoring alone. In the famous geomagnetic storm of March 13–14, 1989, the Hydro Quebec power grid went from completely normal operating conditions to complete province-wide blackout in an elapsed time of only 90 seconds. The electrojet predictive model will instead provide these power system operators a nominal lead-time of approximately 45 minutes for most storm events, and a somewhat smaller lead-time for major events.

The advanced geomagnetic storm forecasting system was developed to provide forecasts for the entire Northern Hemisphere, and detailed impacts of these storm conditions were further assessed for the NGC power grid across England and Wales. This system updated the forecast on a continuous 1-minute cadence and became operational in May 1999. This system was deployed in the NGC System Control Room in Wokingham, England where it was continuously used as the primary space weather tool for the control of the entire national grid. In addition to these forecast capabilities, Metatech with NGC deployed 16 real-time remote monitoring locations throughout England and Wales to monitor the storm environment and impacts on the power grid. Nearly 2,000 channels of data are continuously collected in real-time from this sophisticated network and made available for nowcast and system status displays in the NGC System Control Room. This geomagnetic storm forecasting system, which is highly tailored to electric power grids, is the most-advanced in the world, even exceeding the capability of the NOAA–SEC.

In addition, Metatech has successfully modeled and validated detailed power grid models throughout the world. A complete U.S. Power grid model has been fully developed for the United States. EHV Power Grid infrastructure and was employed in both the EMP Commission studies and also in FEMA investigations under Executive Order 13407.

While it is possible to install a geomagnetic storm forecasting system in the United States using the approach applied in the case of England and Wales, it should be noted that this system provided the forecast to a single location, where action could be taken for the entire grid. In the United States the situation is different, and both for geomagnetic storms and a HEMP attack, it is necessary to develop a procedure to send the geomagnetic forecast or information concerning a missile launch at the United States to all power grid operators within minutes. In addition a coordinated response of the power grid operators needs to be determined

ahead of time for different scenarios. It is important that action be taken to allow this information to be sent to those who require it.

CONCERNS ABOUT SMART GRID SECURITY

While the current situation with regard to the vulnerability of the power grid to HEMP and other high-level electromagnetic disturbances is serious, national discussions of future changes to the power grid could well make things worse. In particular the concept of the "Smart Grid" is under active consideration, and while the precise details of such a plan are not clear, it is clear that a major objective is to collect more data on the grid and to provide that data to the operators of the grid.

The problem with many proposals for the Smart Grid is that there will be a proliferation of millions of computers (Smart Meters), which will be placed at homes and businesses to monitor the use of power in real time. These data will allow the system operators to operate their grids more efficiently and to eliminate the need for extra margins. These distributed computers will be vulnerable to the threat of radiated and conducted high frequency threats (such as E1 HEMP and IEMI) and will be impacted by severe harmonics created during E3 HEMP and geomagnetic storms. It is clear that very high levels of electromagnetic protection should be required for these meters, yet in discussions concerning Smart Meters today, security seems to be a second thought. We recommend that the physical and electromagnetic security of Smart Grid components be raised to the highest level of consideration.

Another area of concern is the plan to build a new super-grid to connect wind power in the Midwest with the Eastern and Western grid with the construction of a new 765 kV grid. It is important to recognize that the higher voltage levels of this transmission network (relative to the 500 kV grid in most of the country) increase its vulnerability to E3 HEMP and geomagnetic storms, potentially increasing the vulnerability of the grid by a factor of 2 or more over what exists today. Plans to build such a grid should definitely consider the protection of the high voltage transformers.

ROLE OF STANDARDS

As alluded to at several points in this statement, it is first important to make a decision that the power grid needs to be protected against HEMP and other similar electromagnetic threats such as geomagnetic storms and IEMI. Once this is done then the means to accomplish the goal should be through standards. While standards often take years to develop, in this case much of the HEMP and IEMI work has already been done in the IEC for generic systems (e.g., computers). Standards can therefore be developed rapidly to improve the hardening of hardware currently in service and also for the development of new products. This approach will allow the fastest time to reach a hardened state, while keeping the costs at a reasonable level.

CONCLUSIONS REGARDING FERC REGULATORY AUTHORITY

Given that the United States has a very diverse, mostly private ownership of the power grid, it is difficult for industry to deal with the threats of HEMP, geomagnetic storms and/or IEMI on their own and certainly not in a piecemeal fashion. There is an argument that if a power company makes improvements to their portions of the grid and others do not, then wide area geographic threats can still have a catastrophic impact.

During the beginning of the power system work in the EMP Commission, NERC was invited to provide its recommendations regarding which power system electronics were the most important to the operation of the grid. A prioritized equipment list was provided and used by the EMP Commission to perform susceptibility tests. While this part of the collaboration was successful, follow-up discussions with NERC were not as successful. It seemed that the working level people within NERC were not willing to recommend protection standards against HEMP in spite of overwhelming evidence that this threat falls into the low-probability, high-consequence area. Indeed the potential consequences are so serious that it should be viewed as a Systemic Risk, one that could threaten the lives of many and alter the course of the history of this country, if ever allowed to unfold.

For this reason, we would recommend that FERC, which has already shown a strong interest in the protection of the power grid from HEMP, be given the regulatory authority to deal with the threat of HEMP and other related electromagnetic threats.

STATEMENT OF EMPRIMUS LLC

JULY 21, 2009

Chairwoman Clarke, Ranking Member Lungren, Chairman Thompson, Ranking Member King, and Members of the subcommittee: Thank you for the opportunity to share with you our thoughts about the present vulnerability of the U.S. electric grid and other critical civilian infrastructure to growing electromagnetic threats, and our recommendations for steps towards remediation of these threats. Emprimus is deeply concerned about our national infrastructure electrical, electronic, and cyber vulnerabilities in a number of areas, and has already been involved in several discussions with Congressional members and their staffs, and other agency personnel about these issues, as well as providing briefings to relevant industry and technical associations in recent months. Emprimus has a multi-disciplined background which includes a private testing program to evaluate and understand the vulnerability of many types of civilian electronic equipment to these growing threats, as well as new ways to remediate them.

We strongly support legislation to amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack and the related intentional electromagnetic interference (IEMI) attacks, as well as hardening the electric grid against high altitude electromagnetic pulse (EMP) and severe geomagnetic storms. For conciseness in this record, we will generically refer to all electromagnetic threats as "EMP." As we will show, all three of these threats are related in that they have similar effects and share common remediation solutions. It is important to note at the outset that EMP is also a cyber threat just as surely as internet hackers are, since data states can be destructively altered.

1. What are the severe electromagnetic threats to our electric system and other critical infrastructure?

Every year, the modern infrastructure of the United States becomes increasingly dependent on integrated circuit-based electronic control systems, computers, servers and burgeoning masses of electronically stored data. The emerging threat and growing use of non-nuclear EMP/IEMI (Intentional Electromagnetic Interference, including Radio Frequency [RF] weapons) poses grave dangers to all of our civilian infrastructure, including our national electric grid, civilian facilities' data and data assets, and can damage computer systems, their electronic equipment and the data they contain, control and monitoring systems, and support systems which would impede operations of most critical civilian infrastructure installations. Support systems at risk range from security systems to communication links to fire protection to all HVAC systems.

For instance, recent research and testing shows how power distribution can be shut down for a multi-State area by mobile non-nuclear EMP attacks. Major metropolitan areas in the United States have a number of critical choke points. For example, some electrical substations in each area of the country connect a large amount of electric generation to the bulk electric transmission system, and similar electrical substations are used to connect the transmission system to the metropolitan distribution system. A mobile non-nuclear attack perpetrated by terrorists or other parties in an innocent-looking truck at the typically unguarded perimeter of a single substation would cause connection faults and trips, resulting in dropping generators off-line similar to recent blackouts in New York and Florida. A coordinated attack at several of these substations could lead to a cascading collapse condition, leading to prolonged large multi-State power outage conditions. A multi-city coordinated attack could have an even more serious national effect. With proper attention to shielding and filtering of substation electronics controls, communications equipment, and data centers as part of a mandated improvement program, the impacts of these intentional EMP events can be minimized.

The military has shielded their facilities for decades against EMP. Now, high levels of EMP can be delivered locally by either hand-held devices, or via more powerful vehicle-borne weapons, and create disruption and damage similar to that caused by high-altitude EMP, but on a local scale. The threat of a severe geomagnetic storm is always with us, and will occur at some time in the future with near certainty. (A solar event similar to the 1859 storm would cause catastrophic damage to our modern electricity-based infrastructure.) The recent Quebec grid collapse as a result of a serious solar storm has resulted in Canadian action to improve its grid.

The following chart shows how all three types of electromagnetic threats to our infrastructure are related with regard to their damage and disruption effects.

	Damage to Electric Grid Transformers	Damage to Grid Electronic Controls and Data	Damage to Other Infrastructure Electronics and Data
High-altitude Electromagnetic Pulse (EMP).	Yes, National Scale.	Yes, Serious ...	Yes, Serious.
Intentional Electromagnetic Interference, or Non-nuclear EMP.	Local or Regional Effects.	Yes, Serious Local.	Yes, Serious Local.
Severe Geo-magnetic Storms	Yes, Regional or National Scale.	Sporadic	Sporadic.

This chart shows how the impacts of these threats are related. Fortunately, appropriately mandated national action can significantly reduce the impacts of all three threat classes.

The International Electrotechnical Commission (IEC) has defined non-nuclear EMP/IEMI as the "intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems thus disrupting, confusing, or damaging these systems for terrorist or criminal purposes." The insidious aspect of this class of EMP for the energy sector and other key sectors of our national infrastructure is that it attacks both cyber- and physical security aspects of our electronics-based systems in manners that can completely circumvent firewalls, tier structures, layered networks, passwords, physical barriers, security procedures, etc. Unlike traditional cyber threats to data security, non-nuclear EMP may be extremely covert and difficult to detect and trace with forensics, and with the ability to impede digital forensics by corrupting the data. There are remediation approaches to help diminish this threat class if appropriate steps are taken.

2. What are the effects of an EMP event on the electric system?

Non-nuclear EMP attack.—As demonstrated in the example above of a relatively modest attack by a small number of individuals on several critical electric power substations, substantial damage and disruption can be inflicted by the use of these uncontrolled and easy-to-deploy electromagnetic weapons. The U.S. Navy has shown how plans for many of these devices are available on the internet, has tested and demonstrated the vulnerability of computer and SCADA systems, and has demonstrated the fabrication and use of such a device built with a total parts cost of $500.00. These man-portable or vehicle-borne weapons are becoming a modern tool of those wishing to conduct highly asymmetrical warfare, including disgruntled employees, criminals, extremists, and terrorists. These devices can be deployed against electric power substations and other electronics, and in fact against all 18 segments of the DHS sectors of critical civilian infrastructure with similar results.

High-altitude EMP attack.—A high-altitude EMP event detonated several hundred miles above the center of the contiguous United States would cause catastrophic damage to the present national electrical grid, as was detailed by the recent Congressional EMP Commission: "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," April 2008. An EMP event of this type has an initial fast burst lasting nanoseconds that will damage or destroy most modern electronics within line of sight that are based on integrated circuitry, and a slower burst lasting up to several minutes that will create very large voltages over hundreds and thousands of miles that will result in disastrous damage to the high-voltage transformers and electronics that power our national electric distribution system. As the EMP Commission states, "The electromagnetic pulse generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences. The increasingly pervasive use of electronics of all forms represents the greatest source of vulnerability to attack by EMP. Electronics are used to control, communicate, compute, store, manage, and implement nearly every aspect of United States (U.S.) civilian systems. When a nuclear explosion occurs at high altitude, the EMP signal it produces will cover the wide geographic region within the line of sight of the detonation. This broad-band, high-amplitude EMP, when coupled into sensitive electronics, has the capability to produce widespread and long lasting disruption and damage to the critical infrastructures that underpin the fabric of U.S. society." This is not a short duration problem: The high voltage grid transformers that will be destroyed have few spares, little commonality, and most are now manufactured offshore. Lead times for small quantities of these transformers are years, but hundreds or thousands would be destroyed.

Severe geomagnetic storms.—The impact on electric power transformers deployed at the ends of our long high-voltage transmission lines would be essentially the same as that from a high-altitude EMP event described above. The geomagnetic induced currents (GIC) from these events will also generate high, damaging voltage surges over any long conductive paths (communications, telecom, data lines, etc.) leading to computer systems, data storage, and any other electronic equipment. An expert in GIC has indicated that uninterruptable power supplies are especially vulnerable. An 1859-class event would shut down most of our grid for years, if our critical transformers remain unprotected.

3. What technological fixes are required to secure infrastructure from an EMP event?

Electronic and data dependent infrastructure.—The 18 Department of Homeland Security sectors of Critical non-military Infrastructure all have a vital dependence on digital data, electronic sensing, computing, controls, and data storage that can be corrupted and/or damaged by both high-altitude EMP and non-nuclear EMP. It is important to point out that these threats are CYBER threats, since they can corrupt and destroy data just as surely as the more publicized internet hacker attacks we are so familiar with these days. In fact, EMP is probably more insidious, since these attacks leave no network footprints and destroy evidence amenable to digital forensics, and they can cause physical damage to the electronic equipment attacked. It is conceivable that EMP could be used to cover up traditional cyber attacks. Critical equipment in the DHS Critical Infrastructure segments such as data centers, supervisory control and data acquisition (SCADA) systems, process control equipment, etc. can be protected by appropriate electromagnetic shielding, filtering, and security procedures, along with enhanced threat detection. It is especially important that facilities responsible for meeting regulatory data retention requirements rapidly acquire this protection, especially trading institutions and banking data centers. The 2008 EMP Commission Final Report has much more detail on the effects of EMP on telecommunications, banking, refineries and pipelines, and other infrastructure, recommending that mandated fixes proceed promptly.

High-voltage transformers.—The national power grid high-voltage transformers must be remediated to withstand the huge direct current voltages they would be exposed to in a high altitude EMP event or severe geomagnetic storm. The 2008 EMP Commission Final Report has a number of specific recommendations regarding transformer protection, improving grid communications and control, safer islanding of grid segments (permitting a damaged portion of the grid to be safely isolated), and other key remediations. Some of these critical fixes can be started immediately and at relatively low cost, especially with regard to high-voltage transformer protection. These protections are needed to protect against severe geomagnetic storms, as well as EMP, since at least a severe storm will occur sooner or later.

4. Why does the modernization of the American electric grid create new vulnerabilities that may not have existed before?

There are several factors that are working to increase the vulnerability of our critical electric grid.

Interconnectivity

Heavy reliance on interconnectivity to meet peak load demands has increased the probability of cascading failures in the event of an EMP event. This is related to the existence of choke points or critical substations which present attractive asymmetrical targets.

Longer transmission lines

Increasing distances encourage use of very high voltage transmission of power from generation source to point of use, and both the high voltage and distance make the system more susceptible to the high-altitude EMP and geomagnetic storm threats.

Renewable power sources

As more long distance lines are added to deliver power from renewable sources of wind and solar located in sparsely populated areas to distant high-population-density areas, the exposure of the grid to high-altitude EMP and geomagnetic storm damage will be significantly increased. Intelligent planning now can mitigate this danger.

Smart Grid

The addition of "Smart Grid" electronic processing and communications between users and generation sources adds many additional points of failure to the operation of the grid if it is attacked by an EMP event.

Electric utility operation

Electric utility data centers and control centers for grid operation, customer account management, and business management including regulatory data retention requirements are highly dependent on the operation of electronic equipment, which is at serious risk of data corruption and equipment damage from the fast EMP transients and from more localized EMP/IEMI attacks.

Critical substations

These substations transmit huge blocks of power from large generating plants which, if the controls are damaged, could disrupt large multi-State areas.

As reported by the EMP Commission, each of these vulnerabilities can be greatly diminished by timely action, but the solutions need to be initiated now.

5. Why is the U.S. electric grid different from other nations?

The size and technology of the U.S. electric grid differentiates it from most other third-world nation grids. For example, differentiating features include:

- Longer transmission lines due to lower population density and large area;
- More critical substations;
- More prevalent conversion from coal to natural gas, in more vulnerable automated and unmanned facilities;
- Many more high-voltage transformers susceptible to EMP damage.

As described previously, each of these factors contributes to increased EMP risk. In contrast to most other developed countries that have one or two electrical power entities, the United States has over 400 transmission-owning entities, greatly complicating coordinated remediation efforts. Also, the R&D and electrical infrastructure capital improvement expenditures have been in serious decline in recent years. These factors complicate implementing a coordinated remediation of our Nation's electrical power system against the three EMP threats. It will require additional Federal authority to mandate swift and coordinated action, along with appropriate Federal funding to initiate these appropriate steps.

6. What is the cost of securing our electric and other critical infrastructure from an electromagnetic event such as EMP, severe geomagnetic storms, or non-nuclear EMP/IEMI?

On June 10, 2009, Emprimus gave a briefing on the subject at a meeting sponsored by the National Defense University and the National Defense Industrial Association on Capitol Hill. The following estimates for infrastructure protection were presented:

REQUESTED CONGRESSIONAL ACTION AND FUNDING FOR CRITICAL INFRASTRUCTURE REMEDIATION

	Amount
Protect High-Voltage Transformers and Critical Substations	$1,000,000,000
Pipelines, Water, and Waste Water	1,000,000,000
Utilities' Data Centers and Control	2,000,000,000
Smart Grid Remediation for Electromagnetic Threats	500,000,000
911 & State Emergency Ops (EOC) State Fed and County Data Centers	2,000,000,000
Key Financial Data Centers	2,000,000,000
Infrastructure Research	500,000,000
EMP Threat Detectors and Other External Threat Security	750,000,000

MINIMAL CONGRESSIONAL ACTION AND FUNDING FOR THE MOST CRITICAL FACILITIES IN EACH INFRASTRUCTURE

	Amount
Most Critical HV Transformers	$150,000,000
Pipelines, Water, and Wastewater	100,000,000
Utility Data Centers and Controls	150,000,000
Key Smart Grid Remediation	100,000,000
911 & State Emergency Ops (EOC) State Fed and County Data Centers	200,000,000
Critical Financial Data Centers	150,000,000
Key Infrastructure Research	75,000,000

MINIMAL CONGRESSIONAL ACTION AND FUNDING FOR THE MOST CRITICAL FACILITIES IN EACH INFRASTRUCTURE—Continued

	Amount
EMP Threat Detectors and Other External Threat Security	75,000,000

The first column shows the levels required to reduce our infrastructure risks to acceptable levels from the physical and cyber threats imposed by the subject electromagnetic threats, and the second column shows a minimal initial program to start actions on the most critical infrastructure reinforcement needs. Although it partitions the problem slightly differently, the Congressional EMP Commission Final Report of April, 2008, has similar numbers for the electric supply portion of the infrastructure hardening. The highest priority objective is to protect a subset of the most critical national infrastructure so that minimal services can be restored after a severe event to allow recovery to begin. The initial costs are obviously a function of the level of critically definition, numbers of protected facilities, and levels of protection.

The Final Report of the Congressional Commission on the Strategic Posture of the United States, May 2009, states that:

Findings: "The United Stated is highly vulnerable to attack with weapons designed to produce electromagnetic pulse effects."

Recommendations: "EMP vulnerabilities should be reduced as the United States modernizes its electric power grid."

Mme. Chairwoman, it is our hope that this has been useful information for the subcommittee on the serious national issue of EMP. Again, we strongly support legislation to amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack and the related non-nuclear EMP/IEMI attacks, as well as hardening the electric grid against high-altitude EMP and severe geomagnetic storms. We would look forward to answering any questions you may have, and we thank you, Ranking Member Lungren, and the Members of the subcommittee for your support in addressing this electric power vulnerability and the broader issue of the vulnerability of our critical national infrastructure sectors to these electromagnetic Achilles heels.

STATEMENT OF THE EMP COMMISSION

JULY 21, 2009

My name is Mike Frankel and I served as the executive director of the EMP Commission for the entire span of its activities, commencing with its authorization in the Floyd Spence National Defense Authorization Act of 2001 and culminating with the delivery of our final, classified, report to the Congressional oversight committees in February of this year. Presently, I am chief science officer for L–3 Communications/Applied Technologies Group. I am a physicist by training and avocation, and have spent many years developing technical expertise in nuclear weapon effects and managing WMD related programs for the Department of Defense in a career that spanned research work for the Navy, the Defense Nuclear Agency, the Defense Threat Reduction Agency, and the Office of the Secretary of Defense. The perspective of the EMP Commission is being more than adequately represented to this committee today by our very distinguished chairman, Dr. William Graham. I should like to submit instead complementary background information that addresses in part a topic that was not emphasized in our final report, and that is the nexus between cyber threats and EMP.

This committee is to be commended for holding this hearing which specifically includes the full spectrum of electronic threats to the power grid. While "ordinary" cyber and EMP are not usually thought of as coupled, this has been a mistake. The cyber threat is much in everyone's consciousness with an immediacy as current as yesterday's headlines, in this case the alleged North Korean source of cyber attacks on networks in South Korea and the United States. This committee has previously rendered valuable service by highlighting the dangerous cyber vulnerabilities of the power grid exposed in the "Aurora" test series conducted at the NNSA's Idaho National Laboratory. The EMP threat has been much less in the public consciousness to date, although the range of potential damage from such an event may, as described in the public portion of the EMP Commission's report, exceed that realizable from most cyber attack scenarios. I should like to advance the somewhat new per-

spective that electromagnetic pulse threats to our critical infrastructures, specifically including the power grid, need to be thought of as but a—hitherto neglected—component of the cybersecurity threat. More broadly speaking, there is a spectrum of electronics threats to the power grid, that range from conventional notions of cyber to different forms of EMP—both nuclear and non-nuclear, and even natural disasters—an electronic Katrina if you will.

The nature of a cyber threat is to reach out and touch something, electronically, through its connected network. This may be thought to occur through delivery of intelligent messages which encode information and/or instructions that direct a system to some unwanted activity that may prove very harmful to its owners' interests. A SCADA may be reached and instructed to open or close a valve controlling pressures in a natural gas pipeline, with a disastrous pipeline explosion as a result. Indeed, this has already happened through SCADA malfunction, albeit not deliberately intentioned. The Aurora test series exposed by this committee which destroyed an electrical generating system, at its base demonstrated the disastrous effects of the mischievous at-a-distance control of an electronic control system. EMP—both nuclear and non-nuclear—will also reach out and impress unwanted signals through the connected network. But in the case of EMP, the signals do not contain specific information or instructions. They are simply shot-gunned electronic pulses, without encoded information, which nevertheless, at low power levels, upon encountering vulnerable systems such as SCADAs, change their bit settings in unpredictable ways guaranteeing they will not operate as planned. Of course at higher power levels, as documented by the EMP Commission, they may cause actual physical damage to any encountered electronic system, up to the point of burning out and melting critical circuit elements. Thus, at low levels of intensity, EMP may rightly be thought of as a "stupid cyber" threat.

These hearings are also particularly timely in light of the current intellectual energy being invested in the pursuit of energy independence, in particular the development of "Smart Grid" technology as well as alternative energy sources such as wind and solar. While Smart Grid is an evolving concept and its architecture still a moving target, some outlines of its ultimate shape are emerging and it is clear that it will depend, to a much a greater degree than present, on the ability to fine tune the delivery of energy to where and when it will be needed. And this will necessitate the proliferation of more, and smarter, sensors and control systems than their already ubiquitous presence, to exercise the real-time capabilities of the newer and more agile grid architecture. With such a proliferation comes enhanced vulnerabilities, to both cyber and EMP threats. Similarly, commercial introduction of new technologies, such as ultra-high-voltage—>1,000 KV—transmission line systems as has been discussed in the context of exploitation of wind power and its delivery from the point of generation to where it's needed, entails critical new vulnerabilities as well. It is appropriate, that precisely now, at the cusp of such significant technological transformation, that proper attention be paid as well to new vulnerabilities which may be introduced in the rush to innovate. The historical economic lesson from the military systems development world is that designing protection into a system from scratch is more effective and much cheaper than attempting retrofit solutions when problems are discovered later on.

Finally, I'd like to return to the theme of a spectrum of electronic threats to the power grid which merit attention, of which "ordinary" cyber is but one component. We've discussed another component as well, electromagnetic pulses due to either nuclear or non-nuclear (RF) sources. But there are also electromagnetic pulses stemming from natural events which pose a grave danger and to which the present power grid remains highly vulnerable—the "electronic Katrina" attending a very massive geomagnetic solar storm. Solar storms—fluctuations induced in the earth's magnetic field due to eruptions of charged solar matter from the surface of the sun ("coronal mass ejections" in the astronomer's language) which are flung out in the direction of the earth, are rather common events. Most are of an intensity that present no danger to anything. Some however are significantly larger and, again on a fairly regular basis, may couple electromagnetic pulse energy to long transmission lines. These induced currents are thus a natural EMP and may overwhelm and physically damage (melt) huge and hard to replace components of the electrical grid. Just such a scenario played out in the huge solar storm of 1989 which took down the Hydro Quebec company system, rendered its many millions of Canadian customers powerless, and irreparably damaged one of their multi-million dollar extremely high-voltage transformers (house-sized units no longer manufactured domestically and which may take up to a year to deliver following a purchase).

But those are "ordinary" events. The EMP Commission also examined the results of a "100-year storm", a Katrina analog in the world of "space weather". Such an extreme event is guaranteed to come, it is only a question of when. Indeed such

storms have already visited us during the last 100 years but they occurred at a time previous to the deployment of our modern electric power grid with its long transmission lines capable of absorbing the unwanted solar EMP energy. Since the "receiving antenna" did not yet exist, except for the spectacularly unusual auroral displays—the aurora borealis was reportedly sighted near the equator—no harm was done. Absent some preparations which have not yet been taken, the next time will be very different with extraordinary permanent damage to hard to replace components and untold suffering lasting for extended periods in its wake. So taking steps to protect the system from cyber and EMP should proceed hand-in-hand with protection against the full spectrum of such electronic threats. And steps which are taken to protect against a singular threat should be considered from a perspective which seeks, as far as possible, solutions that confer dual or multi-benefits against a spectrum of threats. Understanding the need to approach EMP as one of a spectrum of electronically related insults and as a component of the more generalized cybersecurity problem, and a serious consideration of the prospects for remedies that confer multiple protective benefits, is the proper path forward to protect our uniquely valuable power grid from all electronic threats. And the time for such planning is now.

Unfortunately, it is hard to detect signs of concern, or even interest just yet on the part of those charged with reducing the vulnerability of the electric grid. Unlike the Department of Defense which considered the (classified) recommendations of the EMP Commission report seriously and initiated certain (classified) remedial activities, it hard to detect any similar resonance to date on the part of our civilian agencies.

I wish to thank the committee for this opportunity to present my views of this most important issue.

STATEMENT OF APPLIED CONTROL SOLUTIONS, LLC

I appreciate the opportunity to provide the following statement for the record. I have spent more than 35 years working in the commercial power industry designing, developing, implementing, and analyzing industrial instrumentation and control systems. I hold two patents on industrial control systems, and am a Fellow of the International Society of Automation. I have performed cybersecurity vulnerability assessments of power plants, substations, electric utility control centers, and water systems.[1] I am a member of many groups working to improve the reliability and availability of critical infrastructures and their control systems.

On October 17, 2007, I testified to this subcommittee on "Control Systems Cyber Security—The Need for Appropriate Regulations to Assure the Cyber Security of the Electric Grid".[2]

On March 19, 2009, I testified to the Senate Committee on Commerce, Science, and Transportation on "Control Systems Cyber Security—The Current Status of Cyber Security of Critical Infrastructures".[3]

I will provide an update on cybersecurity of the electric system including adequacy of the NERC CIPs and my views on Smart Grid cybersecurity. I will also provide my recommendations for DOE, DHS, and Congressional action to help secure the electric grid from cyber incidents.

BACKGROUND

First of all, I believe it is any utility's obligation to maintain a high level of electric service reliability. For the most part, the utility industry takes this responsibility very seriously and focuses very strongly on electric system reliability. The grid has been designed to be resilient and accommodate failures (the N–1 criteria). The equipment in place (older legacy and new equipment) has demonstrated a high level of reliability. However, as the older equipment is replaced with new equipment such as for Smart Grid applications an interesting paradox occurs—as reliability increases from the installation of new equipment, the cyber vulnerability also increases.

First, I believe a major point of discontinuity has been the unsuccessful equating of the terms Critical Infrastructure Protection (CIP) and cybersecurity.

CIP (or "functional security") is focused on the function of the electric grid being maintained regardless of the status of the computers. Cybersecurity, on the other hand, focuses on protecting the computers independent of whether electric reliability

---

[1] Because much of my information is not in the public domain, I am not at liberty to identify specific utilities on the record.

[2] *http://homeland.house.gov/SiteDocuments/20071017164638-60716.pdf.*

[3] *http://commerce.senate.gov/public/_files/WeissTestimony.pdf.*

is being maintained. For the sake of semantics, I will use the term "cybersecurity" but my intention is that the operation of the computers is focused on "keeping the lights on," or what is becoming increasingly referred to as "functional security."

Secondly, cyber events can be either intentional attacks or unintentional incidents.

NIST defines a cyber incident as "An occurrence that actually or potentially jeopardizes the Confidentiality, Integrity, or Availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional."[4]

Cyber incidents are also more than just malware or botnet attacks. Cyber incidents include all forms of impacts on electronic communications.

Man-made Electromagnetic Interference (EMI) has already impacted North American and European electric and water Supervisory Control and Data Acquisition (SCADA) systems and ruptured a natural gas pipeline.

In industry control systems, the most probable cyber incident is unintentional. Moreover, in a stellar application of the "law of unintended consequences," I believe that "blindly" following the NERC CIPs[5] will result in more unintentional cyber incidents.

Unintentional cyber incidents have already killed people, caused significant outages, and large economic impacts. Additionally, if the incident can be caused unintentionally, the same type of incident, if intentional, could have even more damaging effect.

RECENT HISTORY

What has been happening since I testified to this subcommittee in October 2007? It is not a pretty picture and the power industry clearly needs Congress's help.

Knowledge Base.—Figure 1 characterizes the relationship of the different types of special technical skills needed for control system cybersecurity expertise, and the relative quantities of each at work in the industry today.

Most people now becoming involved with control system cybersecurity typically come from a mainstream business Information Technology (IT) security background and not a control system background. This trend is certainly being accelerated by the Smart Grid initiatives, where the apparent lines between IT and control systems are blurring. Many of the entities responsible for control system cybersecurity, industry, equipment suppliers, and Government personnel (e.g., DHS NCSD and S&T, DOE, EPA, etc.) do not entirely appreciate the difficulties created by this trend.

This lack of appreciation has resulted in the repackaging of IT business security techniques for control systems rather than addressing the needs of field control system devices that often have no security or lack the capability to implement modern security mitigation technologies. This, in some cases, has resulted in making control systems less reliable without providing increased security. An example of the uninformed use of mainstream IT technologies is utilizing port scanners on Programmable Logic Controller (PLC) networks. This has the unintended consequence of shutting them down. This specific type of cyber incident has occurred more than once in both the nuclear power and conventional power portions of the industry, with negative consequences.

As can be seen in Figure 1, IT encompasses a large realm, but does not include control system processes. Arguably, there are less than several hundred people world-wide that fit into the tiny dot called control system cybersecurity. Of that very small number, an even smaller fraction exists within the electric power community.

---

[4] FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information System,* March 2006.

[5] *http://www.nerc.com/page.php?cid=2|20.*

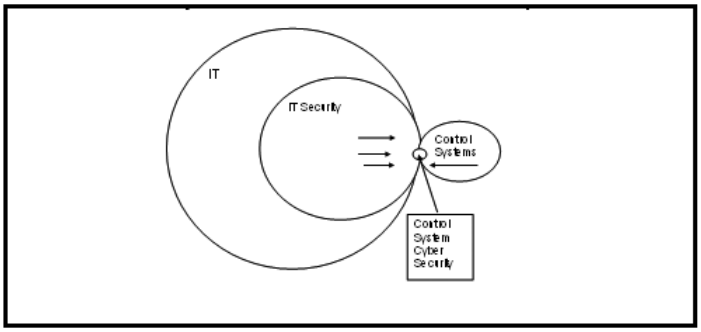


Figure 1 - Relationship and Relative Availability of Control System Cyber Security Expertise

Control System Cyber Incidents.—Since I testified to this subcommittee in October 2007, I have documented more than 30 control system cyber incidents, more than 20 of which were in the North American electric power industry! These incidents affected nuclear and fossil plants, substations, and control centers. Impacts ranged from loss of displays, controller slowdowns and shutdowns, plant shutdowns, and a major regional power outage. Geographically, these incidents occurred in more than ten States and a Canadian province. None of the incidents were actually identified as "cyber".

Meeting the NERC CIPs would not have prevented many of these incidents. In fact, some could have actually been caused or exacerbated by following the NERC CIPs.

Equipment Suppliers.—It is important to understand that suppliers provide equipment with the features their customers' request. Given that fact, the report card on our control system suppliers is a mixed bag. Responding to industry requests, the major Distributed Control System (DCS) and SCADA suppliers have been addressing security at the master station level. However, suppliers of field control and equipment monitoring systems have not had those industry requests and thus are continuing to include dial-up or wireless modems, Blue Tooth and Zigbee connections, and/or direct Internet connections as part of their product offerings. This also applies to equipment used in the Smart Grid and nuclear plants.

Business IT-focused suppliers continue to supply equipment and testing tools designed for IT applications not for legacy control systems applications. This has resulted in control system equipment impacts including shutdown or even hardware failures.

Consultants and System Integrators.—Most of the consultants and system integrators that are focusing on "cybersecurity" are really focusing on compliance for NERC CIPs. Most are focusing on the SCADA or DCS master stations as they are IT-like systems that non-control system personnel can understand. That leaves the legacy field equipment that has essentially no security hardly even addressed as part of the NERC CIP process. The consultants and system integrators that are focused on equipment upgrades or new equipment installation generally do not address security.

Utilities.—The original intention of the NERC CIPs (even before they were called the CIPs) were to make the bulk electric grid secure. Unfortunately, the "letter of the law" of the NERC CIPs is not security, but compliance. It is a critically important distinction to make, and to understand. I know of only one utility that is trying to assure their systems are secure independent of compliance considerations. Almost all utilities are playing the game of compliance rather than securing their systems. This has resulted in industry's lukewarm attempt to meet NERC Advisories such as Aurora.[6] This lack of will has directly led to the significant number of actual electric industry cyber incidents many of which were not even addressed by the NERC CIPs!

NERC.—The North American Electric Reliability Corporation (NERC) was established in 1968 to ensure the reliability of the bulk power system in North America. NERC is a self-regulatory organization, subject to oversight by FERC and governmental authorities in Canada. As of June 18, 2007, FERC granted NERC the legal

[6] *http://homeland.house.gov/SiteDocuments/20080521142118-53954.pdf*.

authority to enforce reliability standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable making NERC the Electric Reliability Organization (ERO). NERC's status as a self-regulatory organization means that it is a non-Government organization which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical, and efficient practices.[7] Prior to becoming the ERO, NERC was an American National Standards Institute (ANSI)-accredited organization meaning it was a consensus standards organization and was subject to the direction of its member utility organizations. The ANSI accreditation requires standards need to go through a formal ballot process. This is a time-consuming effort and tends to favor setting a "very low bar." This consensus process has resulted in cybersecurity standards that are very weak and ambiguous assets and even exclude some of the most important recommendations from the Final Report of the Northeast Outage.[8] In the past, NERC has been a clear obstructionist to adequately securing the electric grid. NERC has used the ANSI process to reject more comprehensive requirements. That obstructionism included public responses denigrating Project Aurora.[9] The consensus approach is adequate for subjects like tree-trimming but is not appropriate for critical infrastructure protection.

I was part of the NIST/MITRE team that performed a line-by-line comparison of the NERC CIPs to NIST Special Publication (SP) 800–53 [10] which is mandatory for all Federal agencies including Federal power agencies.[11] The report demonstrates that NIST SP800–53 is more comprehensive than the NERC CIPs. However, NERC and many utilities are fighting the implementation of NIST SP800–53. Are the utilities trying to say that the computers at the Department of Housing and Urban Development need a more comprehensive set of cybersecurity rules than every non-Federal power plant, substation, and control center in the United States? Unless an asset is classified as "critical" in CIP–002, no further cybersecurity evaluation is necessary. A large segment of the utility industry is using the amorphous requirements in CIP–002 to exclude most of their control system assets from even being assessed. Michael Assante, Vice President and Chief Security Officer of NERC wrote a public open letter on April 7 [12] in which he makes it very clear that the industry is not doing an adequate job of even meeting the weakened intent of the NERC CIPs. Specifically, Assante's letter states that only 29 percent of Generation Owners and Operators identified at least one Critical Asset and fewer than 63 percent of the transmission owners identified at least one Critical Asset. This means that 71% of generation owners did not identify a single critical asset and 37% of transmission owners did not identify a single critical asset. I am personally aware of utilities that have identified ZERO Critical Assets even though they have automated their plants and substations and have control centers.

Despite Assante's attempts to change NERC's approach on cybersecurity, NERC has continued its focus as a utility-directed organization. NERC's Board of Trustees approved revisions to the NERC CIPs on May 6, 2009 after passage by the electric industry with an 88 percent approval rating. However, the revisions did not address any of the technical limitations such as exclusions of telecom, distribution, non-routable protocols or strengthening CIP–002 to address Assante's April 7 letter. A second example would be the June 30, 2009 Alert on the Conficker Worm.[13] The Alert states the ES–ISAC estimates the risk to bulk power system reliability from Conficker is LOW due to the limited exploitation of this vulnerability and generally widespread awareness of the issue even though NERC acknowledges the potential consequence is high and the awareness among control system users is very low.

Smart Grid.—The intent of the Smart Grid is to embed intelligence into the electric grid to allow two-way communications between devices and control centers for monitoring and control. The Smart Grid's use of the Internet and Internet Protocols (IP) is blurring the line between business IT and control systems resulting in more people without knowledge of the electric system being involved in securing these systems.

This is a recipe for disaster—there has already been at least one case of a denial of service attack (DDOS) to a distribution automation system.

---

[7] *http://www.nerc.com/page.php?cid=1*.
[8] *https://reports.energy.gov/BlackoutFinal-Web.pdf*.
[9] *http://www.cnn.com/2007/US/09/27/power.at.risk/index.html*.
[10] *http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-Rev.%203*.
[11] Marshall Abrams, MITRE Technical Report, MTR70050, Addressing Industrial Control Systems in NIST Special Publication 800–53, March 2007.
[12] Letter from Mike Assante to NERC Industry Stakeholders, "Critical Cyber Asset Identification", April 7, 2009.
[13] *http://www.nerc.com/page.php?cid=5%7C63*.

From a Regulatory standpoint, the situation is convoluted because the NERC CIPs explicitly exclude electric distribution which is the heart of the Smart Grid and yet the NIST Smart Grid security efforts point to the NERC CIPs.

Unless Congress passes legislation to allow FERC to include distribution or the individual public utility commissions mandate that the NERC CIPs must be followed for their distribution systems, there are no regulations for securing the Smart Grid.

Education.—To the best of my knowledge, there are no technical, interdisciplinary university curricula for control systems cybersecurity. There are universities starting to address this subject in an ad hoc manner such as the University of Illinois and Mississippi State University. Congress might well seek ways to encourage and fund more such curricula as a significant way to improve cybersecurity in all control systems.

Certifications.—There are no personnel certifications for control system cybersecurity.

IT certifications such as the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM) do not address control systems. Professional engineering examinations do not include security.

There needs to be a certification demonstrating knowledge of control systems as well as security by organizations competent to oversee this requirement. One organization could be the CSFE [14] which certifies Functional Safety experts. There are ongoing efforts by individual companies and organizations such as ISA to certify industrial control systems for cybersecurity.

Government R&D.—R&D has been focused on effectively "repackaging IT". Very little work has been devoted to legacy and even new field equipment, even though these devices have limited or no security, and can cause the biggest impacts.

There has also been no attempt to analyze actual cyber incidents to learn what policies and technologies should be developed to protect them.

NIST.—NIST has effectively two disjointed programs on cybersecurity that impact the electric grid. The NIST Information Technology (IT) Laboratory has been responsible for updating NIST SP800–53 and the daughter standard NIST SP800–82.[15] There has been a significant amount of effort addressing industrial control systems and applicability to the electric industry. NIST is also acting as the standards coordinator for the Smart Grid.

As a member of the Smart Grid Cyber Security Working Group and the Industry-to-Grid Working Group, I see a dichotomy that troubles me. Instead of mandating NIST SP800–53 for the Smart Grid, it appears as if NIST doesn't want to be seen as pushing their own standards. Not only is NIST SP800–53 the best cybersecurity standard currently available, it is mandatory for all Federal power agencies. Why shouldn't NIST SP800–53 be mandated for all power utilities, not just Federal ones?

RECOMMENDATIONS

Traditional reliability threats such as tree trimming to prevent power line damage could be handled by private industry. However cyber is a new threat that requires a joint effort by the Government and private industry. I believe there are a number of roles for the Federal Government to play in defending against cyber incidents and/or physical attacks against electric facilities.

Articles such as the recent Wall Street Journal article on Chinese and Russian hackers imply that the electric industry is unaware of computer intrusions.[16] This is probably true on several accounts. As mentioned, the electric industry is not doing an adequate job of even looking. Additionally, there is a lack of adequate cyber forensics for control systems. This leads to the fact that is it difficult to have an early detection and warning capability for cyber threats for the electric industry today. However, that same difficulty is also an opportunity for the Government and private industry to develop appropriate forensics. A non-technical challenge is the industry's continuing reticence to provide control system cyber incident data to the Government and for law enforcement to share relevant information on actual attacks to the industry so they can protect themselves.

What can DHS and DOE do?

I cannot speak for the division in responsibilities between DHS and DOE, but I can point out what needs to be done:

- Provide intelligence on threats to those needing to know—that does not mean only security-cleared individuals, but all individuals working in the area;

[14] *www.csfe.org*.
[15] *http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf*.
[16] *http://online.wsj.com/article/SB123914805204099085.html*.

- Make use of available technical talent—there is very little, and the safety and security of our country depend on these efforts;
- Analyze actual control system cyber incidents to develop appropriate cyber technologies and policies—there are few places to get the information as most of it has not been provided to the Government—and what has is often classified and unavailable;
- Establish benchmarks for how much security is enough, what is an acceptable vulnerability assessment, what is an acceptable risk assessment, audit metrics, trade-offs between security and functionality, etc.;
- Support first-of-kind technology development, particularly for legacy field devices;
- Support development of college technical as well as policy curricula;
- Support the establishment of a CERT (Computer Emergency Response Team) for control systems that is not under the purview of the Government, because industry is still uncomfortable about providing what they consider to be confidential data to Government agencies like the FBI.

What can Congress do?

Currently FERC is constrained by the Energy Policy Act of 2005.[17] It cannot write standards and its scope is restricted to the bulk electric system. There are several steps that Congress can take to help maintain the reliability of the electric system from cyber threats:

1. Provide cybersecurity legislation that gives FERC the scope to write standards including mandating NIST SP800–53 for the bulk electric grid and the Smart Grid.
2. For cybersecurity, increase FERC's scope to include electric distribution. There are technical as well as administrative reasons. Low voltage transmission and high voltage distribution systems electronically communicate with each other; utilities electronically communicate with each other; and the utilities use common systems. We cannot afford to have a "Tower of Babel" set of rules for each State and for the same equipment.
3. NERC is in a conflict-of-interest position because its fundamental purpose has changed. If NERC can not do the job of assuring cybersecurity of the electric grid, find an organization with the will power and authority to do so.
4. HR 2195[18] would go a long way toward providing effective legislation. I would add the following: Mandate the NIST FISMA guidance documents, such as SP800–53 and require the establishment of a program to develop expertise in electric grid cybersecurity. The expertise gained from this program should be shared with every electric grid owner and operator.

SUMMARY

It has been almost 10 years since I helped start the control system cybersecurity program at the Electric Power Research Institute (EPRI). Ten years should have been sufficient time for the industry to make significant progress. Unfortunately, it has not happened. Actual control system cyber incidents continue to occur—in fact, they appear to be getting more numerous. An unsecured electric grid is dangerous to the safety and economic well-being of this country. Congress needs to step in and provide regulation to give FERC the additional powers necessary and mandate NIST SP800–53.

STATEMENT OF ADVANCED FUSION SYSTEMS, LLC

JULY 19, 2009

My name is Curtis Birnbach and I am the president of Advanced Fusion Systems. While the main thrust of my company is fusion energy research, one of our subsidiaries has developed technology to protect the electric power grid from EMP attack. I wish to address the threat to our Nation posed by both electromagnetic pulse (EMP) and solar storms. At the risk of sounding glib, I bring you good news and bad news.

The bad news is that this threat is all too real. I have been working on EMP-related technologies for many years. I have built electrically-driven EMP generators and have extensively studied the phenomenology of intense ultra-short pulses. I would like to summarize this work to help bring focus to the critical aspects of this

[17] *http://en.wikipedia.org/wiki/Energy_Policy_Act_of_2005*.
[18] *http://www.opencongress.org/bill/111-h2195/text*.

problem. EMP from a nuclear detonation or solar storms poses a unique threat in that it can instantly destroy our civilization. I do not make this statement lightly. Our society is totally dependent on the continuous supply of electricity. Should our electricity be suddenly withheld, our society would immediately collapse.

While I am sure that you have already been briefed on the general aspects of this problem, I wish to focus on the two most critical components we use to deliver: Transformers and generators. If they don't function, we can't deliver electricity and life as we know it stops. The generators and transformers have two very important things in common: They are very expensive and they take years to replace. The worst-case victims of either an EMP attack or a solar storm are our generators and large substation transformers.

This brings me to the first of two points in my testimony: The United States does not have a domestic transformer manufacturing capability for large substation-class transformers. These devices are made exclusively on the Pacific Rim and in Europe. Large transformers typically take 3 to 5 years to obtain and put into operation. The production capacity of existing overseas manufacturers is quite limited. Should the sudden need for rapid delivery of a couple of hundred transformers occur, these manufacturers would be unable to supply our requirement. Further, as they are not U.S. corporations, they have no incentive to delay other existing customers to supply our needs in the event of an emergency. Also, a solar-sourced EMP event may well affect electric power equipment in many other countries exacerbating the supply situation.

The situation with generators has common elements. While we do have some manufacturing capacity for large generators in the United States, it is limited and should a large number be suddenly needed, it would take years to meet that need. If equipment manufacturers are also unable to function because of a lack of electricity we end up with a chicken-and-egg situation; we can't have one without the other.

There is no way that this country can exist for a couple of months, no less many years without electricity. To compound this situation, our utilities may not be insured against this type of loss. Even if they were insured, the insurance companies would suffer potentially crippling losses if utilities were destroyed over a wide area. Our financial system, our medical system, our communication systems, our public safety systems—none could function without electricity. Most companies including utilities would simply cease to exist. There is a real likelihood of civil unrest.

Stockpiling transformers will not work. According to Platts Energy Reporting, there are over a quarter of a million large transformers, and close to 20,000 generators. The transformers are not standardized so the number that would have to be stockpiled is prohibitively large. For every large transformer there are about a thousand smaller transformers, of which only a small fraction are produced domestically. DARPA tried to run a program to build "universal transformers" that could be stockpiled. This effort proved impractical as there is too much variation among transformers.

I did promise some good news. My company has developed a grid-level protection system. This system can protect our country from these threats. We have developed an EMP Protective System (EPS). Each EPS unit will protect a single phase which is one of three wires (phases) that are typically used in high-power electrical devices. Generators have three wires while transformers have 6 wires. Once an EPS is installed, it will detect the pulse of an EMP, safely conduct it to ground, and immediately be ready for the next pulse. These switches were originally designed to operate under conditions similar to those encountered in an EMP attack or solar storm. They are totally autonomous and react in a small fraction of a billionth of a second. They contain a built-in detection system which is the only way you can get a protective device to work quickly enough to be of use.

We have looked at some representative sites for installation of these protective devices. As an example, I would like to discuss protection of the Niagara Hydroelectric Plant. This is one of the most important power stations in this country. While I will not go into specific details for security reasons, based on what limited information is available to me, I have estimated that the entire complex could be protected for somewhere between $75 million and $100 million. The cost of this protection would also be expected to be included in the rate base for the utility so that ultimately the small cost of the protection is borne by consumers who will be receiving a more secure supply of electricity. Compared to the $10 billion that this station might be expected to cost to replace, this one-time cost of 1% is a small cost to protect the plant. This one-time cost of the equipment to protect the plant is all or partially offset by the reduced insurance premiums for a plant that has this protection in place. Obviously, a detailed engineering study would be necessary to refine this number, but it provides an order of magnitude of the cost of this protection.

I have also done estimates on transmission substations. Large transformers cost around $1.5 million to protect. All incoming and outgoing lines in a substation must be protected, but in most cases, this protection is also the same devices that are protecting the transformers. A typical large substation, has at least ten lines of 115 KV or more, and dozens of transformers. When balanced against the cost of a large substation, which can cost a half billion dollars, the cost of protection is typically 10% of the total cost. In either case, the cost is a fraction of the replacement cost of substations or generators, or the lost revenues that the utilities would suffer over a period of several years as a result of the attack. The loss of revenue far exceeds the replacement cost of the equipment. The economic and societal costs of being without electricity are of course far greater than the losses of the utility.

While these numbers may seem large, remember that this is not a single-year expenditure. It will take several years to fully implement this type of protection. Implementation of EPS protection is cheap insurance in the face of such losses. These estimates do not include the deaths, injuries, civil unrest and such that would be likely consequences of these events, particularly once it became clear that the disruption would last for extended periods of time.

My company is committed to help resolve this problem. By making these protective devices available, we are offering a viable option to the unthinkable scenarios I have described. We are funded through the private sector. We are only looking to have the Government support the purchase of these devices. There has been significant interest in this technology overseas.

In order to make grid protection available and affordable in a reasonable period of time, State and Federal legislation encouraging the purchase of EPS technology for critical elements of the electric grid is needed. Three legislative measures should be considered:

1. Tax credits for private utilities purchasing EPS equipment for the purpose of grid protection;
2. Grants to utilities for installation of critical EPS equipment at vital locations;
3. Providing Government-backed bonding authority to raise money to provide EPS funding to rural electric systems and others who need it;
4. FERC agreement to include these devices in the rate base.

STATEMENT OF THE CANADIAN ELECTRICITY ASSOCIATION

JULY 21, 2009

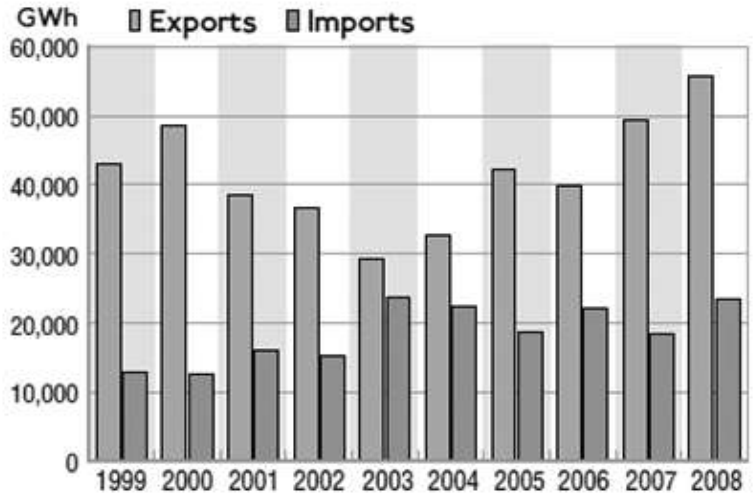
The Canadian Electricity Association ("CEA"), the national forum and voice of the evolving electricity business in Canada, is pleased to provide the following statement regarding the appropriate actions that the U.S. Congress should take to protect the electric grid from cybersecurity threats and vulnerabilities. CEA's members account for the majority of Canada's installed generating capacity and high voltage transmission. In this statement, CEA explains the importance of taking cybersecurity actions in the United States that are mindful of the interconnected nature of the North American transmission grid and the importance of avoiding actions that could undermine the reliability of the transmission grid and impact cross-border trade. CEA further provides suggestions for this subcommittee to consider before developing legislation to address physical and cybersecurity in the electricity sector. Specifically, CEA suggests that: (1) The North American Electric Reliability Corporation remain the primary body for addressing cybersecurity matters on the North American transmission grid; (2) any authority given to U.S. Governmental authorities to address emergency situations be of a limited duration and be coordinated with Canadian governmental authorities; (3) consultation and information sharing between the U.S. and Canadian governmental authorities should be provided for in any legislation; and, (4) U.S. legislation should be respectful of Canadian sovereignty and jurisdiction.

BACKGROUND

The electric transmission systems of U.S. and Canadian utilities are interconnected with one another at numerous points, forming a highly integrated North American transmission grid, as can be seen in the following map:

Of the 211,152 circuit miles of transmission lines greater than 200 kilovolts in North America, 46,499 circuit miles, or 22 percent, are located in Canada. This integration allows for cross-border trading, which facilitates a higher level of reliability for consumers, efficiencies in fuel and resource management, and efficiencies in system operation. These benefits, and the activities of companies investing and participating in markets on both sides of the border, serve citizens of the United States and Canada extremely well.

To provide perspective on the importance of the U.S./Canadian trading relationship, the chart below shows both exports from Canada to the United States and imports into Canada from the United States between 1999 and 2008:



Source: NEB Electricity Exports and Imports. Monthly Statistics, various years.

Canada is a net exporter of electricity to the United States. The quantity of electricity exported from Canada to the United States has typically been 6 to 10 percent of Canadian production. At the same time, as the chart above demonstrates, electricity imports to Canada from the United States have also increased over time. The North American market is borderless, and supply meets demand north to south or south to north as the market requires, to the advantage of consumers across the continent. Such electricity trade enhances the reliability of each country's electricity supply and mitigates risk by providing power during times of emergency outages or periods of high electricity demand. Canadian utilities are part of and therefore critical to the energy security of the United States, and the reliability of the North American transmission grid.

ANY ACTIONS TAKEN IN THE UNITED STATES TO ADDRESS CYBERSECURITY ON THE BULK-POWER SYSTEM MUST BE COORDINATED WITH CANADIAN GOVERNMENTAL AUTHORITIES

CEA recognizes the serious risks that cybersecurity threats and vulnerabilities present to the international grid. Nevertheless, CEA believes that any actions to address cybersecurity threats and vulnerabilities must be accomplished in a manner that recognizes the mutual inter-dependency of the interconnected Canada-U.S. transmission systems, and must not unintentionally imperil or downgrade reliability and erect barriers to cross-border trade.

The President of the United States recently directed a 60-day, comprehensive review to assess U.S. policies and structures for cybersecurity, and the result was the release of "Cyberspace Policy Review" on May 29, 2009. In the report, the White House concluded that "the United States needs a comprehensive framework to ensure coordinated response and recovery by the government, the private sector, and our allies to a significant incident or threat." Understanding that the United States cannot act in a unilateral fashion, the report concluded:

"The United States cannot succeed by acting in isolation, because cyberspace crosses geographic and jurisdictional boundaries. The United States must work actively with countries around the world to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations."

CEA supports the concept of cross-border cooperation between Canada and the United States to prevent cybersecurity attacks.

NERC IS THE APPROPRIATE STANDARD-SETTING BODY FOR THE NORTH AMERICAN TRANSMISSION GRID

CEA believes that the best venue to address cybersecurity matters on the North American transmission grid is the North American Electric Reliability Corporation ("NERC"). Through the reliability standard-setting model included in section 215 of the Federal Power Act, the NERC reliability standard-setting process allows for a balance of interests ensuring access to expertise from industry across the continent for the development of standards with continental application that can be approved by authorities on both sides of the border—be it FERC in the United States, or any of the jurisdictional authorities in the Canadian provinces. This model recognizes jurisdictional sovereignty through the existence of the remand provision in the U.S. legislation, which is also incorporated into the processes for standards approval in a number of Canadian provinces and which is incorporated into the existing NERC standard-setting procedures. This component assures that no governmental authority has the ability to unilaterally modify standards which would apply to the whole system, and that any variances are accommodated through the collective process. At the same time, it gives public authorities the confidence that the system has a Government backstop, providing Governmental authorities on both sides of the border with the confidence that standards developed through that process reflect their concerns.

NERC also has the ability to effectively incorporate the experiences and knowledge of the private sector in both the United States and Canada, which is especially important in this very technical industry. Any legislative directive must avoid placing the regulator in an operational role in terms of issuing detailed emergency procedures to address a present or imminent threat or vulnerability to electric system reliability. Such an approach would be consistent with the conclusions reached in "Cyberspace Policy Review" about the importance of a public-private partnership to address network security issues. As the President explained when the report was issued, "My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

Recognizing the need to better respond to cybersecurity challenges, NERC has recently established processes to allow for the expedited development of cybersecurity standards. NERC is developing approaches that allow cybersecurity standards to be developed in a less public manner and in a way that allows for quick action to respond to ever-changing threats. Importantly, this process follows the NERC standard-setting model, thereby allowing for the development of cybersecurity standards that are respectful of Canadian jurisdictional sovereignty and allowing for the development of standards that can be approved by Canadian governmental authorities. In addition, CEA is encouraged that NERC has elevated the profile of its Critical Infrastructure Protection Program, to increase its cybersecurity expertise and to better coordinate with Governmental authorities. We believe such steps allow NERC to better respond to cybersecurity issues.

CONSIDERATIONS FOR U.S. LEGISLATION

CEA believes much of what needs to be done to address cybersecurity issues on the North American transmission grid can be accomplished through the NERC standards development process. Nevertheless, CEA recognizes that U.S. legislation may be necessary to address certain gaps in NERC authority. CEA has attached to this statement as an appendix a paper prepared by the major electric utility trade associations in Canada and the United States on the appropriate approach to take on cybersecurity. CEA also provides the following comments should this subcommittee pursue a legislative strategy.

Authority to Take Action on an Emergency Basis

CEA recognizes situations can arise requiring emergency actions to be taken immediately to protect the reliability of the bulk power system. To the extent that NERC does not have the information or authority to respond to such an emergency situation, CEA agrees that Governmental bodies should be able to respond expeditiously to ensure industry acts to protect the grid. In terms of U.S. Governmental authority to respond to imminent cybersecurity threats, CEA understands the need for authority to address emergency situations, although we believe that such authority must be limited only to specific, credible, and imminent cybersecurity emergencies, be of a limited duration, and be coordinated with Canadian governmental authorities.

Consultation and Sharing of Information

In any cybersecurity legislation, CEA strongly supports the inclusion of a requirement that the appropriate U.S. Governmental agency consult with appropriate Canadian authorities before taking measures to address cybersecurity threats. Unlike the U.S. system, transmission is regulated in Canada primarily by provincial governmental authorities. Moreover, reliability standards are authorized and enforced by provincial governmental authorities. Consulting with the appropriate governmental authorities in the relevant provinces will help to ensure that actions taken are respectful of Canadian jurisdictional sovereignty and avoid unintended impacts on reliability and cross-border trade. The absence of consultation between and among governmental authorities could further result in the elimination of, or reduction in, the sharing of critical cybersecurity information—not a good result at a time when the sharing of information is becoming more and more important.[1]

Consultation and information sharing is absent, for example, in H.R. 2195, a bill introduced by Homeland Security Chairman Bennie Thompson. The absence of a process for coordination between Canadian and U.S. Governmental officials prior to any actions taken by FERC to address a cyber vulnerability or threat could undermine both reliability and security on the North American transmission grid. As noted in "Cyberspace Policy Review," such coordination among Governmental officials is critical to effectively addressing cybersecurity issues.

Any U.S. Legislation Should be Respectful of Canadian Sovereignty and Jurisdiction

In addition to the need for coordination between Canadian and U.S. Governmental officials, this subcommittee should also be mindful that U.S. legislation should avoid interfering with Canadian sovereignty and jurisdiction, which could undermine both cybersecurity and reliability. For example, in H.R. 2195, "critical electric infrastructure" is defined so broadly as to include Canadian systems and assets, since those systems and assets, if incapacitated or destroyed, could cause significant harm to the U.S. grid. Such a broad definition would, under this language, bring Canadian utilities within the scope of FERC authority under Section 224(e). Moreover, the Interim Measures authority under Section 224B would allow FERC to supplement, replace, or modify existing cybersecurity reliability standards approved by NERC. Since existing cybersecurity standards are in effect in the majority of Canadian provinces, the replacement of such standards in the United States by FERC could result in inconsistent reliability standards on the North American grid, thereby potentially undermining reliability and potentially making the system more vulnerable to a cyber attack. CEA therefore requests this subcommittee to consider the impact that provisions in any proposed legislation could have on Canadian sovereignty and jurisdiction.

NEED FOR COORDINATION AMONG INDUSTRY SECTORS

As a final matter, CEA is concerned with any legislative actions taken by Congress that fail to take into account the scope of the cybersecurity problem. As noted in "Cyberspace Policy Review," cybersecurity affects all sectors and must be addressed in a comprehensive manner. CEA believes any cybersecurity bill would be greatly improved by requiring that the necessary information sharing and collaboration take place between governmental agencies and all the critical infrastructure sectors, not just electricity. A focus on just the electricity sector addresses only one piece of a much larger puzzle, and could, in fact, miss important elements to effectively addressing cybersecurity in the bulk power sector. The President's report recognizes that the cybersecurity issue "transcends the jurisdictional purview of individual departments and agencies because, although each agency has a unique contribution to make, no single agency has a broad enough perspective or authority to match the sweep of the problem." Given the complexity of the cybersecurity problem, and the need for coordination on an international basis, CEA asks this subcommittee to exercise caution before developing legislation to address cybersecurity in the electricity sector.

CEA appreciates this opportunity to provide this statement and would be happy to answer any questions that may arise during the hearing.

[1] CEA also believes strongly that orders or measures to address known or imminent cybersecurity threats must be accompanied by sufficient information sharing regarding the threat such that those implementing the order or measure can do so effectively.

THE NORTH AMERICAN ELECTRIC POWER INDUSTRY'S TOP PRIORITY IS A RELIABLE AND SECURE BULK POWER SYSTEM

The stakeholders of the electric power industry continue to work closely and in partnership with governmental authorities at the Federal, State/provincial and local levels in both the United States and Canada in order to maintain and improve upon the high level of reliability consumers expect. Cybersecurity is an important element of bulk power system reliability that the electric power industry takes very seriously.

ELECTRIC POWER INDUSTRY IN STRONG PARTNERSHIP WITH GOVERNMENT

The electric power industry works closely with various government agencies on bulk power system security. On an on-going basis, we communicate and collaborate in the United States with the Department of Homeland Security, the Department of Energy, and the Federal Energy Regulatory Commission (FERC), and in Canada with the various Federal and provincial authorities to gain needed information about potential threats and vulnerabilities related to the bulk power system. The electric power industry also works very closely with the North American Electric Reliability Corporation (NERC) to develop mandatory reliability standards, including cybersecurity standards. In addition, NERC has an "alert and advisory" procedure that provides the electric power industry with timely and actionable information to assure the continued reliability and security of the bulk power system.

THE ELECTRIC POWER INDUSTRY CONTINUOUSLY MONITORS AND ACTS QUICKLY TO ENSURE BULK POWER SYSTEM RELIABILITY AND SECURITY

Every day, the electric power industry continuously monitors the bulk power system and mitigates the effects of transmission grid incidents—large and small. Consumers and government are rarely aware of these incidents because of the sector's advance planning and coordination activities which reflect the quick and often seamless response the sector takes to address reliability and security events. This response includes prevention and response/recovery strategies—both are equally important. The industry's strong track record on reliability and security continues as we work diligently to adhere to mandatory NERC reliability standards, which are approved by FERC, including standards that address cybersecurity.

NERC FLEXIBLE STANDARDS APPROVAL PROCESSES MEET MAJORITY OF GRID CHALLENGES

NERC's industry-based and FERC-approved standards development process yields mandatory standards for the bulk power system that are clear, technically sound, and enforceable, yet garner broad support within the industry. NERC is striving to draw from the state-of-the-art in cybersecurity, through consideration of the National Institute of Standards and Technology (NIST) framework for cybersecurity, and to integrate that framework into NERC's existing Critical Infrastructure Protection standards. NERC has also made important revisions to its standards development process by putting in place policies that allow, when necessary, for the confidential and expedient development of standards, including those related to cyber- and physical security.

EMERGENCY CYBER SITUATIONS REQUIRE AN EXPEDITIOUS AND EFFICIENT APPROACH

If the Federal Government has actionable intelligence about an imminent threat to the bulk power system, the electric power industry is ready, willing, and able to respond. We understand it may be necessary for Government authorities to issue an order, which could require certain actions to be taken by the electric power industry. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC in the United States and the appropriate corresponding authorities in Canada should be the Government agencies that direct the electric power industry on the needed emergency actions. These actions should only remain in effect until the threat subsides or upon FERC approval of related NERC reliability standards. In the United States, Section 215 of the Federal Power Act (Energy Policy Act of 2005) invested FERC with a significant role in bulk power system reliability, and it would be duplicative and inefficient to recreate that responsibility at another agency. As FERC, NERC and the electric power industry relationships move forward and mature in the area of reliability and security, any disruption of this would be counterproductive.

IMPROVED ELECTRIC POWER INDUSTRY-GOVERNMENT PARTNERSHIP WITH BETTER INFORMATION FLOW

In nearly all situations the electric power industry can protect the reliability and security of the bulk power system without Government intelligence information. However, in the limited circumstances when the industry does need Government intelligence information on a particular threat or vulnerability, it is critical that such information is timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cybersecurity staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system. The electric power industry is fully committed to taking the needed steps to maintain and improve bulk power system reliability and security, and stands ready to work with Congress, FERC, other Government agencies and NERC on these critical issues.

Supporting Associations and Contacts.—American Public Power Association, Joy Ditto; Canadian Electricity Association, Bonnie Suchman; Edison Electric Institute, Scott Aaronson; Electric Power Supply Association, Con Lass; Electricity Consumers Resource Council, John Anderson; Large Public Power Council, Jessica Matlock; National Association of Regulatory Utility Commissioners, Charles Gray; National Rural Electric Cooperative Association, Laura M. Schepis; Transmission Access Policy Study Group, Deborah Sliz.

STATEMENT OF INDUSTRIAL DEFENDER, INC.

Thank you for the opportunity to submit written testimony regarding efforts to secure the modern electric grid from physical and cyber attacks. I appreciate the subcommittee examining these important issues and am grateful for your willingness to consider my views.

I am the president and CEO of Industrial Defender, Inc., a provider of cyber risk protection with over 18 years of industrial control system and SCADA industry experience and more than 7 years of industrial cybersecurity experience. Industrial Defender has completed more than 100 process control/SCADA cybersecurity assessments, more than 10,000 global technology deployments in securing critical infrastructure systems, more than 3,000 mission-critical SCADA deployments and provides managed security services for 170 process control plants in 21 countries. My comments on the subcommittee's hearing topic follow.

PROTECTING THE U.S. ELECTRIC POWER INFRASTRUCTURE FROM PHYSICAL AND CYBER ATTACKS

The Federal Government has a responsibility to protect our Nation's electric power infrastructure from physical or cyber attacks to ensure the social, economic, health, and safety of our citizens. There has been a significant increase in malicious cyber attack attempts on critical infrastructure electric power entities from suspected terrorists and even adversarial nations and more action is needed to fortify our Nation's electric power cyber defenses in order to combat the potentially dangerous threats. A recent coordinated cyber attack on the United States and South Korea, which may have originated in North Korea, involved the malicious use of more than 100,000 computers. Though this particular attack was not targeted at

U.S. electric power interests, it does suggest that more needs to be done in order to improve our Nation's cyber defenses.

The majority of electric power assets in the United States are owned and operated by private sector entities. Based upon private sector contracts executed by Industrial Defender over the past 7 years to assess and mitigate cyber risk specific to critical infrastructure industries, including electric power, oil and gas, water, transportation, and chemical sectors, we have found that industries with cybersecurity regulatory mandates in place, including the Chemical and Electric Power sectors, are industries taking a leadership role in protecting their digital infrastructure assets. Having regulations in place, however, does not guarantee 100 percent compliance or protection. There have been significant challenges within industries for which mandatory compliance standards have been implemented. A recent letter to electricity industry stakeholders from Michael Assante, the Chief Security Officer for the North American Electric Reliability Corporation (NERC) dated April 7, 2009, raised concern over the identification of Critical Assets and Critical Cyber Assets (NERC CIP–002), which are defined as those "facilities, systems and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." Results from a survey published for the July 1–December 31, 2008 period suggest that certain qualifying assets may not have been identified as "Critical". Of particular concern were qualifying assets owned and operated by electric power generation owners and operators, of which only 29 percent reported identifying at least one critical asset, and transmission owners, fewer than 63 percent of which identified at least one critical asset. This inaction by electricity asset owners and operators regarding mandatory compliance requirements gives rise to great concern over the ability of any voluntary private sector compliance program to be effective. There is a risk that industries that do not have compliance mandates may be willing to play the percentages that a critical infrastructure incident will not happen at their company, rather than spend thousands or even millions of dollars to mitigate any known risks and vulnerabilities.

Ensuring the reliability and security of the bulk electric system must be a cooperative and shared responsibility between private sector organizations and the Federal Government. This should include the Federal Government overseeing a coordinated effort between public sector and private sector entities to enhance and enforce the NERC CIP standards; drive cybersecurity awareness and education within the public and private sector; require vendor commercial information security credentials; provide crucial sharing of information regarding cyber incidents, vulnerabilities, and best practices; provide a cybersecurity implementation funding incentive; and, offer "Safe Harbor Protection" for private sector companies, ensuring the elevation of threat and vulnerability information to the Federal Government while at the same time increasing public awareness and protection.

INDUSTRY COMPLIANCE WITH NERC STANDARDS

In addition to the North American Electric Reliability (NERC) survey, which raises concerns over the inaction of bulk electricity asset owners and operators, some bulk electricity providers may be taking a "defensible audit position" in lieu of a well-designed cyber risk mitigation strategy. It is our opinion that this behavior is the result of non-descriptive and prescriptive requirements in the current NERC CIP standards that leave determination of a risk-mitigation strategy solely to the discretion of industry. Additionally, it is important to note that up to the latest revision of the NERC CIP standards, asset owners and operators were permitted to apply "reasonable business judgment" in determining risk-mitigation strategy for critical assets.

The current industry spread relative to interpretation and action around the current NERC CIP standards is extremely broad. Based upon experience, significant action was taken by industry in assessing cyber risk through contracting third parties to provide independent NERC CIP gap analysis, network design reviews, vulnerability assessments, penetration testing, and NERC CIP compliance training. Much of this work was done in advance of the December 31, 2008 deadline; however, many utilities remain very active in performing this work relative to their operational assets. What is more concerning, regarding NERC CIP compliance, is the slow pace at which industry is adopting technology required to meet NERC CIP–005 and NERC CIP–007 compliance, specifically, establishing Electronic Security Perimeter and System Security management for all Critical Cyber-Assets. It is evident, as represented in Mr. Assante's April 7, 2009 letter to Industry Stakeholders, that the definition of a "Critical Asset", and associated "Critical Cyber-Asset", has been viewed differently between the private sector and NERC. The pri-

vate sector's interpretation, and hence subsequent identification of critical assets, has resulted in actions that seem contrary to the defined objectives of securing the Nation's critical infrastructure.

In one example, a major U.S. electric power provider considered implementing intrusion detection monitoring technology to mitigate cybersecurity risks and vulnerabilities in order to secure its substations and meet the required NERC CIP compliance standards. Currently, the NERC CIP compliance standards focus on "routable communication protocols" and exclude "non-routable communication protocols" and "communication links". The electric power entity eventually made a cost-conscious decision to convert all of its substations to a non-routable communication protocol SCADA network. As a result, it did not move forward with the substation equipment upgrade, resulting in a move backwards instead of using technology to enhance cybersecurity, workplace efficiency, and productivity.

With over 150 investor-owned utilities, Government-owned and -operated utilities and a number of smaller municipal electric entities falling under the jurisdiction of the NERC CIP standards, there should be significant demand for monitoring technology to support NERC CIP requirements. Unfortunately, the purchasing behavior of bulk electricity providers does not match the number of monitoring sensors needed to support the NERC CIP standards.

GOVERNMENT EFFORTS TO SECURE CONTROL SYSTEMS AND THE ELECTRIC INDUSTRY FROM PHYSICAL AND CYBER ATTACKS

Escalation of threats and exposure of incidences are essential components of successfully thwarting cyber attacks against the Nation's critical infrastructure. With 85 percent of the Nation's critical infrastructure owned and operated by the private sector, the public and private sectors must work collaboratively, with trusted and open lines of communication, to ensure the timeliest communication of critical cybersecurity information. Relying solely on Federal Government intelligence agencies to identify the threat is a shortsighted strategy. The private sector represents the most valuable source of operational intelligence, which must be harnessed in order to effectively communicate and drive action to reduce the consequences of pending attacks.

Operational systems (SCADA/Process Control Systems) used to safely and reliably operate critical infrastructure in electric power, water, energy, chemicals and transportation sectors lack the necessary security technology to escalate cyber threats and expose cyber incidences in real-time so that appropriate action (communication, emergency orders/actions, etc) can be taken to minimize the impact on national security, public safety, and economic interests.

Greater investments in "Defense in Depth Sensor Technology," including electronic security perimeter, remote access and authentication, network intrusion detection, host intrusion detection, and patch monitoring and management, will enable real-time aggregation of threats and incidences for real-time reporting. FERC Order 706 also calls for "defense-in-depth" subject to technical feasibility considerations with NERC oversight.

Through the deployment of Defense in Depth Sensor Technology, the U.S. Department of Homeland Security (DHS) should assume the role of "Critical Infrastructure Threat Clearing House." The goal of the Critical Infrastructure Threat Clearing House is to establish lines of communication between asset owners and operators and DHS to warn the public of potentially dangerous, malicious, and non-malicious cybersecurity incidents. It is recommended that DHS establish a "cyber heat map," populated with intelligence by Defense in Depth Sensor Technology, which would provide transparency into the current cybersecurity threats facing the Nation, as well as supply access to detailed information on each specific threat occurrence. However, for this to be effective, safe harbor protection should be afforded to the private sector reporting party (see below).

PENDING LEGISLATION AND COVERAGE OF THE ELECTRIC SECTOR

Cooperation between private sector organizations and the Federal Government will need to be achieved to enable increased cybersecurity protection as well as flexibility to expand these infrastructure platforms to support future needs. To this end, legislation pending before Congress could be strengthened to better achieve the separate goals of the private and public sectors as well as increased public safety. Important issues that are not currently part of the legislative proposals are outlined below.

- A distinct lack of threat visibility due to the slow adoption of technology designed to both detect and protect against cybersecurity threats.

- Inclusion of safe harbor protection for private sector companies, ensuring the elevation of threats and vulnerabilities to the Federal Government, resulting in increased public awareness and protection.
- An absence of specific descriptive and prescription recommendations for critical infrastructure systems and requirements.
- Mechanisms to enable a more efficient and timely means of issuing standards through granting FERC "authorship" responsibility. Presently the NERC Standards processes are largely created and approved by industry and hence are somewhat self-policing.
- Require any full- or part-time contractor with privileged access to critical infrastructure control related information system to obtain commercial cybersecurity credentials.
- Provision to increase availability of funds for cybersecurity related equipment and staffing.

Any final legislation promoting public and private sector collaboration should include the following recommendations.

- *More Descriptive Definition of Critical Cyber-Assets*.—It is essential that any final legislation specifically identify which critical cyber assets need to be secured. As it relates to SCADA/Process Control System security requirements, all computer or microprocessor-based operational devices used to monitor, control, or analyze the critical infrastructure where accurate timing has been deemed necessary must be included to ensure the integrity of the critical infrastructure. These devices include, but are not limited to: Power Plant Automation Systems; Substation Automation Systems; Programmable Logic Controllers (PLC); Intelligent Electronic Devices (IED); sequence of event recorders; digital fault recorders; intelligent protective relay devices; Energy Management Systems (EMS); Supervisory Control and Data Acquisition (SCADA) Systems; Plant Control Systems; routers; firewalls; Intrusion Detection Systems (IDS); remote access systems; physical security access control systems; telephone and voice recording systems; video surveillance systems; and, log collection and analysis systems.
- *Remove the Exclusion of "Non-routable Protocols" and "Communication Links"*.—This exclusion is being used as a work-around to avoid implementation costs. FERC Order 706 includes comments from the ISA99 Industrial Automation and Control Systems Security Team objecting to the exclusion of communication links from CIP–002–1 and non-routable protocols from critical cyber assets. The comments argue that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable—through testing and experience.
- *Bolster Public/Private Clearing House*.—It is increasingly essential that private sector asset owners and operators work collaboratively with the Government to warn the public of potentially dangerous malicious and non-malicious cybersecurity incidents. Through the deployment of Defense-in-Depth Sensor Technology, the U.S. Department of Homeland Security (DHS) should assume the role of "Critical Infrastructure Threat Clearing House." The goal of the Critical Infrastructure Threat Clearing House is to establish lines of communication between asset owners and operators and DHS to warn the public of potentially dangerous, malicious, and non-malicious cybersecurity incidents. It is recommended that DHS establish a "cyber heat map" populated with intelligence by Defense in Depth Sensor Technology, which would provide transparency into the current cybersecurity threats the Nation faces, as well as supply access to detailed information on each specific threat occurrence. In order for this to be effective, safe harbor protection should be afforded to the private sector reporting party (see below).
- *Include Recommendation of Descriptive and Prescriptive Solutions*.—Any final legislation should require the deployment of Defense-in-Depth Sensor Technology throughout the entire SCADA/Process Control System network environment. Defense-in-Depth Sensor Technology includes electronic security perimeter, remote access and authentication, network intrusion detection, host intrusion detection, and patch monitoring and management. Equipping critical infrastructure systems with the appropriate security sensor technology enables real-time aggregation of threats and incidences for real-time reporting to the appropriate authorities.
- *Provide "Safe Harbor Protection"*.—Presently there is no "Safe Harbor Protection" afforded to the private sector for open "escalation of threats, exposure of incidences" with the Federal Government. Without these protections in place, private sector companies will be less inclined to share the information and risk potential negative public exposure. Legislation pending before Congress attempts to address this issue by providing protection to disclosed cybersecurity

data; however, the proposals do not provide a similar protection to the disclosing entity. In order to ensure open communication from the private sector, it is essential to provide privacy protection for both the disclosing entity and the disclosed cybersecurity data. As a means of bridging the communication gap between public sector and private sector, safe harbor protection should be provided to private sector companies escalating threats and/or exposing incidences with the Federal Government. This protection is not intended to provide a safe harbor from accountability, but instead to provide protection to share information with the appropriate authorities. The U.S. Department of Defense's (DOD) Defense Industrial Base Cyber Security and Information Assurance (CS/IA) pilot program initiative, launched in early 2008, offers a potential model on this issue. The DIB/CSIA has five major components: (1) A binding bilateral DOD-DIB company framework agreement to facilitate CS/IA cooperation; (2) threat and vulnerability information sharing; (3) DIB network incident reporting; (4) damage assessments; and (5) DOD acquisition and contract changes. Some of these components might be relevant to establishing a similar relationship between the Federal Government and private sector critical infrastructure companies.

- *Grant FERC Authorship Responsibility*.—Presently, the NERC Critical Infrastructure Protection (CIP) standards [CIP–002—CIP–009] provide electric utility private sector guidance on the subject of cybersecurity. Pending legislation would provide FERC with emergency authorities to issue actions/orders in the event of a known cybersecurity threat to the electric utility infrastructure. These actions/orders would remain in effect over a defined period of time until they are incorporated into a standard, and/or the threat is mitigated, or the order/action expires.

  The NERC CIP standards are self-policing in that they are created and approved by industry. According to FERC Chairman Jon Wellinghoff in his April 28, 2009 letter to U.S. Representative Edward J. Markey, "The commission is committed to exercising all of the authority that Congress has given it to help protect the power grid. However, Congress needs to be aware that the commission's current authority is not sufficient to ensure the cybersecurity of the grid. The existing process is based on industry consensus and is, therefore, too slow, subject to disclosure to potential attackers, and not responsive enough to adequately address matters that affect national security."

  Granting FERC emergency authorities to act in the event of a threat or incident is the reactive element of protecting our Nation's critical infrastructure. Who is responsible for the proactive element of mitigating our risks, escalating the threats and exposing our incidences?

  In addition to having emergency authorities, FERC should be granted authorship responsibilities for future cybersecurity standards to ensure the protection and integrity of the Nation's electric utility infrastructure. FERC can continue to leverage NERC for the creation of the standards; however, in the interest of ensuring timely, descriptive, and prescriptive cybersecurity standards, FERC must have the authority to author and issue such standards. Industry input is important to drive public sector-private sector collaboration; however, the present self-policing standards leave the Nation's ability to secure the electric utility infrastructure in a timely manner vulnerable.
- *Require a Commercial Cybersecurity Credential*.—Any full- or part-time contractor with privileged access to a critical infrastructure control information system, regardless of job or occupational series, would need to obtain a commercial cybersecurity credential accredited by ANSI or an equivalent authorized body. The credential would also require maintaining certified status with a certain number of hours of continuing professional education each year. This program would be phased in and have a similar framework as DOD Directive 8570.1 Information Assurance Training, Certification, and Workforce Program.
- *Cybersecurity Implementation Monetary Incentives*.—This could be similar in concept and scope to the renewable energy incentives passed in the Emergency Economic Stabilization Act of 2008 and/or the Smart Grid incentives of the American Recovery and Reinvestment Act of 2009 (ARRA).

INTRUSION DETECTION TECHNOLOGY AND IDENTIFICATION OF CYBER ATTACKS

Industrial networks, while sharing many of the same technologies as business networks, differ enough from business networks to make many conventional threat management approaches ineffective. Industrial networks tend to be more static and predictable than business networks. Safety and effectiveness testing costs for industrial networks are very high, and the effects of technologies like anti-virus scanning

and even security patch management on these computers is unpredictable enough that no such technologies can be used safely without incurring very high costs. Industrial networks tend to be tightly controlled—generally conventional office tools such as word processors, presentation tools, and email clients are not found on legacy industrial networks. However, modern industrial leverage base internet protocols like TCP and HTTP layer on top of these base protocols a large variety of control-system-custom protocols like Modbus, DNP3, ICCP and IEC 61850, which are never seen on business networks.

The present lack of investment in equipping industrial network systems with real-time security sensors to provide visibility into the current cybersecurity threats, vulnerabilities and incidences plaguing them has emerged as both a necessary and dangerous initiative in terms of cybersecurity protection. Based on historical risk and vulnerability assessment data captured from Industrial Defender professional services field teams, most SCADA environments contain latent vulnerabilities, likely with compiled exploits, and are not discovered, on average, until almost a year later (331 days).

As a result, it is necessary to carefully evaluate security technologies and techniques before deploying them on industrial networks and computers. Through the evaluation of many technologies over the last 5 years, Industrial Defender has found results that span the entire spectrum from security technologies and procedures that actively impair the effectiveness of industrial networks and control systems, through technologies that do not impair networks, but add no value either, to technologies and approaches that are, in fact, effective and worthwhile at securing industrial networks.

Network intrusion detection systems (NIDS) are an essential component of a defense-in-depth strategy, and there are real benefits in the form of specialized expertise when an outsourced managed service provider manages NIDS sensors. NIDS sensors developed for industrial control systems need to be customized with knowledge of industrial network protocols and systems. The sensors are routinely deployed inside the security perimeter of the industrial network, monitoring traffic exchanged between the industrial computers and between those computers and the business network.

Conventional NIDS technologies are "signature-based." That is, much like the well-known anti-virus (AV) products used on PC workstations, signature-based NIDS use a large set of rules called "signatures" to scan network traffic. Any traffic that matches the signature triggers an alert and may trigger corrective action, as well. A key limitation of conventional signature-based NIDS is that like signature-based AV, signature-based NIDS can only detect attacks that it has a signature for. As new vulnerabilities are found in common computer and network components, new signatures are written to identify communications patterns of attackers trying to take advantage of those vulnerabilities. If an attacker discovers a vulnerability or somehow manages to create an attack vector for a vulnerability before a patch/fix or signature for the vulnerability is available, that attack is called a "zero day" attack. Signature-based NIDS are by definition unable to detect zero-day attacks, because those attacks occur before signatures are available to detect the attacks.

Host intrusion detection systems (HIDS) monitor the operation of computer systems and alert when suspicious activity is detected. The archetypical example of HIDS is an anti-virus system. With NIDS, it is generally possible to monitor networks in a completely passive way, receiving a copy of every message exchanged on a switch, for example, without impairing the communications on the switch in any way. This is important because of the prohibitive cost of re-testing an industrial solution for safety and effectiveness if an after-the-fact security monitoring solution changes the behavior of the network significantly.

Control system HIDS have the same imperative—first do no harm. After-market HIDS must not interfere with the operation of the control system and must not reduce confidence in the correctness of a control system to the point where a prohibitively expensive re-test is required. An industrial HIDS solution must be designed with exactly this criterion in mind. Most enterprise class HIDS interfere with the operation of the host, either by accident or by design, or they insert themselves so deeply into the operating system and kernel of the host computer, that they destroy all confidence in the continued correct and safe operation of the control system.

GOVERNMENT INVESTMENT IN CONTROL SYSTEMS R&D

One area of focus should be a centralized clearing house for the correlation of alerts and traffic statistics. Such central oversight would provide intelligence regarding widespread information gathering and other attacks. For the central correlation to work, cooperation of large, managed service providers and large, self-

managed networks is needed, in order to send the necessary standardized alerts, and traffic statistics to the U.S. Government. If a central agency was the real-time clearing house for conclusions about traffic patterns and the correlation of such conclusions, that agency would be able to correlate suspicious activities across many industrial networks. Such correlation, especially correlation of traffic profiling results, might allow the central monitoring agency to identify widespread information-gathering activities targeted at critical infrastructure networks. Such activity is a logical precursor to a widespread attack on infrastructure. It would also allow a central clearing house to draw conclusions about widespread infections calling out to the internet for instructions from time to time, which might be a sign of a coordinated attack on many sites.

Industrial Defender recommends that the Federal Government investigate establishing a program, correlation infrastructures and technologies, and the necessary data exchange standards to permit real-time alerts and traffic statistics to be aggregated centrally. Individually managed security service providers and large industrial security/network control centers would be encouraged—or required—to participate in the program and provide the central authority with the statistics and other information that the agency requires to calculate high level correlations. Such a program could provide government and intelligence agencies with important insights into the health of industrial networks overall, and with insight into sudden changes or widespread patterns indicative of preparations for a large-scale attack.

A second area of focus is to strongly encourage control system vendor partnerships with the U.S. Department of Energy's National Supervisory Control and Data Acquisition (SCADA) Test Bed programs at Idaho National Laboratory and Sandia National Laboratory. There needs to be a continued and raised emphasis on control system security product and technology assessments to identify vulnerabilities and corresponding mitigation approaches when systems are being designed and built.

STATEMENT OF SOUTHERN CALIFORNIA EDISON

A LIFECYCLE FRAMEWORK FOR SELF-SUSTAINING IMPLEMENTATION OF SMART GRID INTEROPERABILITY AND CYBER SECURITY STANDARDS

INTRODUCTION

Advancing Smart Grid interoperability and security through standards adoption fosters innovation and accelerates robust, secure, and reliable Smart Grid deployments. This is achieved by lowering the barriers to entry for vendors; accelerating secure and interoperable product time to market; and ultimately lowering costs for consumers. With all the potential benefits associated with broad standards adoption it seems reasonable to institute a standards lifecycle framework to ensure the deployment of a robust and interoperable Smart Grid. Unfortunately, realizing the benefits of standardization requires more than just selection of a standard.

Several papers in circulation including papers developed by EnerNex [1] and EPRI [2] show that there are plenty of standards available. With so many available standards, why has the pace of adoption been slow? The answer is that the selection of a standard is but one aspect of a greater product lifecycle. Full realization of the benefits will require a shared Government and industry focus on a common set of Smart Grid functions, and a standards lifecycle framework supporting those functions. The goal of this standards lifecycle framework is to align policy, standards development, product development, and procurement actions to create a self-sustaining Smart Grid market. A successfully operating, self-sustaining Smart Grid product market is defined by public policy supported by standards that are rapidly adopted by product vendors seeking certification, and driven by utility procurement agents only buying products certified to those standards. The effect in the marketplace is that product vendors are incented to compete against each other to create products that are increasingly interoperable and secure. Within this context, it is clear that any approach needs to be comprehensive and cohesive.

Beyond the creation of a standards lifecycle framework, it should also be noted that the associated effects of validation, enforcement, certification, and accreditation are missing or in need of additional support. Certification and enforcement are critical elements of the lifecycle. Certification defines test cases that clarify standards

---

[1] Smart Grid Standards Assessment and Recommendations for Adoption and Development, draft v0.82, Enernex for California Energy Commission, February, 2009.

[2] EPRI Technical Report: Integration of Advanced Automation and Enterprise Information Infrastructures: Harmonization of IEC 61850 and IEC 61970/61968 Models, EPRI, Palo Alto, CA 2006. Product ID 1013802.

interpretation in products by vendors. In this manner, any ambiguity in standards interpretation is quickly identified and remedied in such a closed-loop process. Without such a process, vendors will interpret standards differently and interoperability will not be achieved.

This holistic approach to standards adoption allows for a more inclusive stakeholder representation. Achieving increasing levels of interoperability and robustness will require a concerted effort by all stakeholders including regulators, Government agencies, utilities, vendors, commercial organizations, and standards development organizations. These interests can be represented through a look at the applicable development and adoption lifecycles and how these lifecycles intersect. Two of the most relevant lifecycles are the procurement lifecycle and the standards development lifecycle. These two lifecycles are significant in that they cover both the development of the products and standards and the adoption and enforcement of the standards.

STANDARDS DEVELOPMENT LIFECYCLE

The standards development lifecycle is the realization of an operational need through the articulation of the need, followed by the development of standards, certification processes, and implementation validation. The standards process is better served when the organizations needing to procure the products are involved in this needs development. In the case of Smart Grid, these organizations are mostly utilities. Needs are typically represented through business objectives, use cases, and requirements. These needs should be the basis for both platform agnostic and platform specific standards development. The process for establishing and representing the needs through standards is well-established and actively practiced in the utility industry.

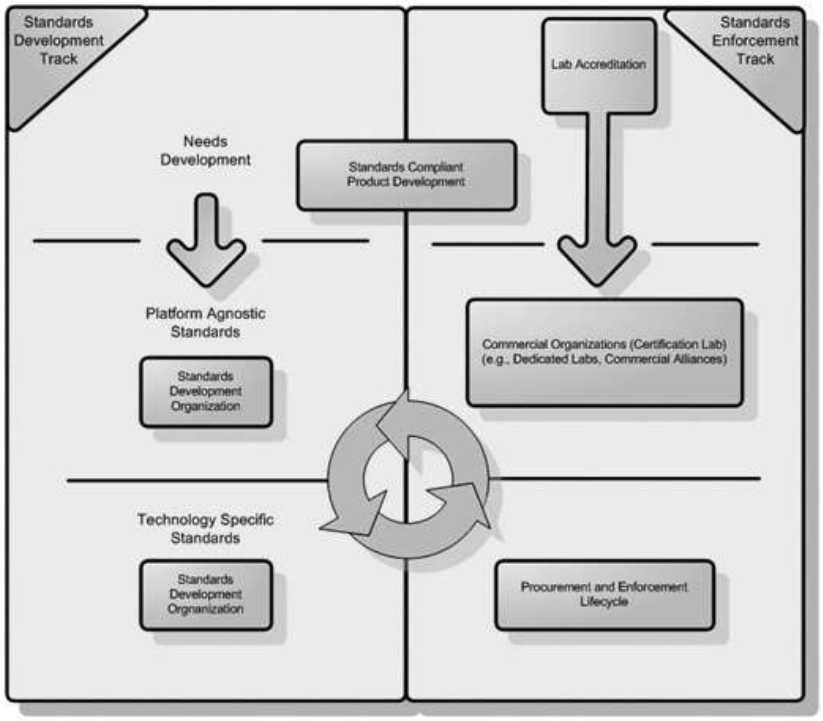


Figure 1: Standards Development Lifecycle

As shown above in Figure 1, the standards development lifecycle does not end with the development of the standard; this is simply the starting point. The standard needs to be implemented, validated and adopted. In most cases where standards are available but not widely used, the fault is not with the development of the

standard but rather with the enforcement of the standard. Fortunately, normal competitive market drivers can be used to enable this piece. Commercial organizations chartered to validate vendor implementations claiming to be compliant with a given standard are needed. These organizations play a critical role in the overall adoption of a standard. There are several commercial organizations currently providing certification services including ZigBee, HomePlug, Wi-Fi, and WiMAX. While the communications space is well-served by these organizations, other domains have no commercial equivalent. As an example for the electric grid, there are no commercial security certification organizations. Utilities and other organization have developed security-related needs statements and there are many security standards. Again, because there is no certifying organization the lifecycle is broken and the standards adoption becomes ad-hoc. Closing the loop with a certification process is a key to accelerating mature standards. In doing so, interoperability issues are discovered and regressed into the standards and the technologies. Without this closed-loop process, interoperability is almost impossible to achieve on a broad system spanning multiple vendors.

Ultimately, adoption is achieved through the procuring organization. The utilities procure devices which extend and enhance the capabilities of the electric grid. Using security as an example, devices which are certified as more robust or more secure will be procured over competing devices offering less robustness or security. In this way, both the utilities and the vendors have the necessary incentives to foster a sustainable Smart Grid ecosystem.

PROCUREMENT-DRIVEN STANDARDS LIFECYCLE FRAMEWORK

The standards development process relies on the utility procurement lifecycle for enforcement. This lifecycle also provides other key touch points with the standards development lifecycle beyond the final enforcement of a given standard. These touch points give visibility and provide context for participation of various stakeholders. The utility procurement lifecycle, at its core, is concerned with procuring products which meet a given set of criteria. These criteria include regulatory policy, operational needs, and business functionality as well as any standards compliance requirements. Regulators and standards organizations support the utility procurement process at several points in the lifecycle.

Regulators at both the State and Federal level can provide four key roles in the lifecycle.

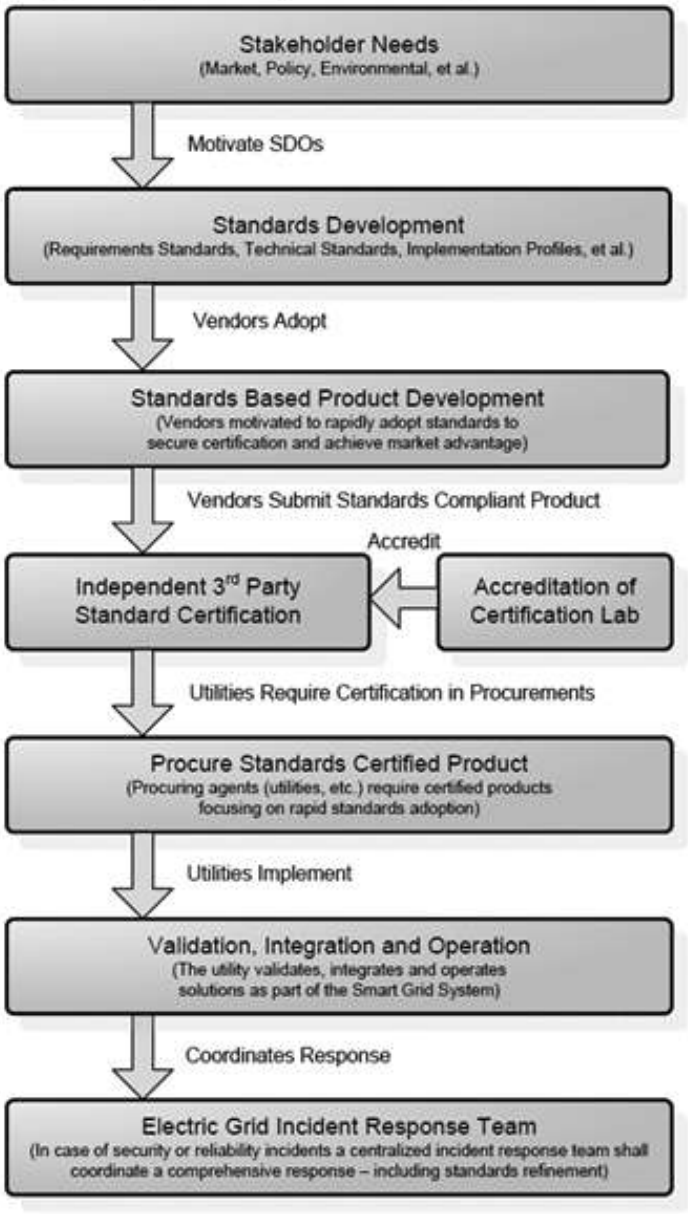
1. Define performance criteria in the context of meeting public policy objectives. California's "six criteria" for advanced metering is one example;
2. Provide oversight on utility expenditures and can enforce interoperability and cybersecurity standards adoption;
3. Ensure utility participation in a centralized incident response effort; and,
4. Refine performance criteria based on continuous improvement.

Continuing with the security example, the procurement lifecycle merged with the standards development lifecycle to create a procurement-driven, cybersecurity standards lifecycle framework, as shown in figure 2 below, provides for a more consistent and more secure electric grid. In fact, enabling the entire lifecycle is the only way to increase security capability across the entire grid.

As part of this standards lifecycle framework, various industry stakeholders are able to define operational needs within the context of regulatory objectives. These needs are carried into standards development by utilities and vendors, evaluated for risk and used to seed various technology-agnostic and technology-specific standards development by standards development organizations (SDOs). The resulting standards can be recognized by Federal and State regulators as meeting policy objectives. While standards development is often described as a long arduous process, today Smart Grid development can benefit from the many existing standards available. The current potential to accelerate standards adoption is described in the "Smart Grid Standards Adoption—Utility Industry Perspective"[3] white paper.

[3] Smart Grid Standards Adoption—Utility Industry Perspective v5.0, by Utility Smart Grid Executive Working Group and Open SmartGrid, March 23, 2009.

Figure 2: Cyber Security Standards Lifecycle Framework



As this lifecycle framework continues, products are developed by manufacturers and software developers and evaluated for standards compliance certification by independent commercial labs, which have been accredited by a Governmental agency such as NIST.

Devices/software are then procured by the utility for implementation. During the course of utility operations, performance information is gathered, new threats are

identified, and knowledge is shared. Any security risk that is realized is responded to by a central incident response team which coordinates the response to the security event. Again, using the touch points across the standards lifecycle framework, the industry is able to transfer this security knowledge to the appropriate organizations.

CONCLUSION

Lower product costs, operational costs, and improved resiliency are significant benefits associated with standards adoption. In order to truly realize these benefits, the entire product lifecycle needs to be considered. There are two complementary views of this lifecycle, the first view is the standard lifecycle, and the second is the procurement lifecycle. Certification is a key component of the lifecycle and without certification the cycle is broken and the ability to achieve broad interoperability is negated. These lifecycles should be unified by a comprehensive standards lifecycle framework described above. This more holistic view also clearly identifies the roles for key stakeholders' participation. For the energy sector, enabling and enhancing, this standards lifecycle framework should be the primary goal.

SCE RESPONSE TO QUESTIONS FOR THE DHS SUBCOMMITTEE FOR CYBERSECURITY, EMERGING THREATS, AND SCIENCE AND TECHNOLOGY ON JULY 21

How much of the total cost of its metering infrastructure does SCE expect to recoup from rate cases?

SCE's Smart Meter program is authorized for full rate recovery by the California Public Utilities Commission.

Are SCE's assets hardened against an intentional or unintentional electromagnetic pulse? If so, how did SCE go about mitigating this threat? How much did implementing protective measures cost? Was SCE able to recoup these costs in a rate case?

SCE understands the disruption potential of electromagnetic pulse (EMP) and other threats that pose risks to system availability. These threats are taken into account as part of our system design. The risk of the SCE assets being affected by EMP is a function of the probability, size, and nature of an EMP threat. As such, SCE's risk-adaptive process accounts for this and other threats through our system availability, disaster recovery, and business continuity designs.

Please describe how SCE implemented mitigations to the Aurora vulnerability.

In response to the Aurora Vulnerability, SCE first performed a detailed assessment of the system to identify and mitigate the associated vulnerabilities across our service territory in alignment with NERC recommendations. Additionally, SCE refined planning, engineering, procurement, security, and compliance policies to support NERC CIP standards.

What would industry like to see from Government in terms of an alert and warning system about an impending cyber attack? Does this early warning system exist today?

We believe the Government has an important role to play in the case of impending security events. This role should be played in the broader context of a well-defined structure as articulated in SCE's white paper "A Lifecycle Framework for Self-sustaining Implementation of Smart Grid Interoperability and Cyber Security Standards" which is attached to this response. Early warning processes in use today include US–CERT, the Electric Sector—ISAC (ES–ISAC) managed through NERC, as well as the DHS Daily Open Source Infrastructure Report. All existing early warning processes would benefit from participating in a broader self-sustaining, framework that includes the mechanisms for all stakeholders including policymakers, vendors, utilities and incident response teams to take actions so the overall electric infrastructure becomes increasingly secure.

What is the current role of the Federal Government be in defending against nation-state-level cyber or physical attacks against electric facilities? What should the role of the Federal Government be?

We believe the role of the Federal Government should be to work with industry to align collaborative efforts on policy, standards development, product development and procurement actions to create the self-sustaining Smart Grid market as outlined in the attached white paper "A Lifecycle Framework for Self-sustaining Implementation of Smart Grid Interoperability and Cyber Security Standards". A successfully operating, self-sustaining market is defined by public policy supported by standards that are rapidly adopted by product vendors seeking certification, and

driven by utility procurements buying products certified to those standards. The effect in the marketplace is that product vendors are incented to compete against each other to create Smart Grid solutions that are increasingly interoperable and secure.

Does SCE use the Energy ISAC today? Does SCE believe that the Energy ISAC is effective in producing timely and relevant analysis and warnings for the industry? If not, what measures can be undertaken to improve this capability?

Yes, SCE utilizes the Electric Sector—ISAC (ES–ISAC), managed through NERC, for warnings applicable to the electric sector. The ES–ISAC, notifications are supplemented by US–CERT, as a source for our Anti-vulnerability Emergency Response Team, a 24x7 group of SCE subject matter experts tasked with vulnerability and incident response.

We do believe the ES–ISAC represents an effective mechanism for timely and relevant analysis and warnings for the industry. ES–ISAC participation in the broader industry lifecycle framework, as stated in the attached white paper, would improve communication on security events and known vulnerabilities across a broad set of industry stakeholders.

What are the key aspects of any piece of legislation that seeks to secure the electric grid from cyber and physical attack?

Legislation seeking to secure the electric grid should consider the ability to facilitate the standards-driven process which motivates the market to produce and adopt increasingly secure and interoperable products.

Are industry-written security standards appropriate to protect assets as critical to national security as the electric system? If so, why? If not, should a Federal entity write the standards?

Yes, SCE believes a public/private partnership is the most effective way to develop cybersecurity specifications and standards. An example is the current effort between the industry, NIST and the Department of Energy, known as ASAP–SG, the goal of which is to organize and articulate Smart Grid cybersecurity standards by leveraging an existing set of standards will help provide the guidance necessary for vendors to develop secure product; certification labs to certify secure product; and utility companies the ability to confidently procure and implement secure products.

SCE has published three papers on the topic of security and standards please see: *http://www.sce.com/PowerandEnvironment/smartgrid/*.

APPENDIX II

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR DR. WILLIAM R. GRAHAM, CHAIRMAN, COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE

Question 1. The EMP commission report looked at several infrastructure sectors, the first of which was electric power. Please tell us about the vulnerabilities you found there, and if you could prioritize their criticality. To the best of your knowledge, has the electric industry attempted to address these vulnerabilities? Where are we right now in protecting the electric grid and what more must be done?

Answer. The vulnerabilities found in the electric power infrastructure include:

a. High-voltage transformer damage due to low frequency (E3) High Altitude EMP. These transformers are only produced outside the United States, and at a very low rate. Lead time for delivery under normal circumstances is months to years.

b. Damage to relays and other control electronics in high-voltage substations due to high frequency (E1) EMP.

c. Distribution transmission line insulator damage due to E1 EMP.

d. Damage to power control center electronics due to E1 EMP.

e. Widespread blackout of power grids due to simultaneous failures of controls, transformers, and the loss of load (due to insulator damage).

As far as I have been able to determine, the electric industry has not attempted to address these vulnerabilities. The Federal Energy Regulatory Commission (FERC) has been active in trying to understand EMP and other electromagnetic threats to the power grid, and they are encouraging the North American Electric Reliability Corporation (NERC) to take action with mandatory standards. FERC has asked the Department of Energy (DoE) to begin the development and demonstration of protection technologies against EMP, geomagnetic storms, and Intentional Electromagnetic Interference (IEMI). NERC has also recently been briefed about EMP and geomagnetic storms by representatives of the EMP Commission.

While the level of discussion concerning the threat of EMP to the power grid is increasing, until NERC and the power industry take action in developing standards and implementing a schedule for protection, nothing will move forward. It is clear that a national leadership from the National Security Council, the Department of Homeland Security, and the DoE is required to move this protection issue forward. Such leadership has not been forthcoming.

Question 2. Would installing the protections necessary to protect the electric grid from EMP be costly?

Answer. Protection for the vulnerabilities indicated above would not be expensive in terms of the initial costs of the equipment, the replacement costs, or certainly when compared with the cost to the economy of the United States of an extended electrical blackout.

a. It is recommended that the work of the EMP Commission be studied by those in charge of ensuring the reliability of the U.S. power system, with an emphasis on relative vulnerabilities (e.g. 765 kV network) and in terms of applying protection first to new construction, where the cost will be at the low end for such protection. The U.S. experience with military systems indicates that the cost of protecting new systems from EMP is in the 1–2% range when carried out by knowledgeable and experienced engineers. Unfortunately, the number of such engineers has been declining since the end of the Cold War.

b. It is urgent that work begins on adapting international standards on EMP protection to the U.S. power grid as soon as possible. It appears that FERC is in the best position to ensure that NERC develops the proper protection standards and sets a schedule to accomplish the protection.

Question 3. The "Smart Grid" concept means putting more computerized systems, similar to Systems Control and Data Acquisition ("SCADA") systems throughout the

grid, down to the level of individual users such as homes and buildings. Aren't these systems even more sensitive and susceptible to damage by EMP than the other components of the electrical grid? In your opinion, would the "Smart Grid" be even more likely to be taken down by EMP than our current grid if the computer controls were not protected from EMP?

Answer. It is very clear that one of the primary objectives of the "Smart Grid" is to reduce the peak power needs by controlling the power usage by the customer (primarily through time of day pricing or mandatory reductions in use of electricity at times of high usage of electricity in various regions). While this approach may be beneficial in the short run, the information from electronic meters at homes and buildings will essentially be used to operate the grid, without proper leadership and systems engineering, will lead to much less margin for electric power reliability.

Based on experiments performed by the EMP Commission, substation safety relays have been found to be vulnerable to EMP, but at much higher levels of threat than standard PC equipment (PCs are extremely vulnerable to EMP). The point is that Smart Meters (essentially PC technology) will require a strong, comprehensive effort for both Electromagnetic Interference (EMI) and EMP protection.

If these meters are not well-protected against EMP, as well as normal EMI, geomagnetic storms, and IEMI (EM weapons), then EMP will likely cause a more rapid failure of the new "Smart" Grid. The IEEE Electromagnetic Compatibility (EMC) Society met recently in Austin, Texas and registered alarm at the lack of basic EMC and EMP protection standards being referenced by the National Institute of Standards and Technology (NIST) and the Electric Power Research Institute (EPRI) in their review of existing important protection standards for the "Smart Grid". A letter from the Society is being prepared to indicate this concern.

Question 4. New "Green Generation" such as wind power will also require the addition of thousands of miles of new high-voltage transmission, because most of the wind farms will be located far from population centers. Aren't these very long high-voltage lines the most vulnerable to Geomagnetically Induced Currents (GIC), and if that is the case, shouldn't we be building these transmission lines with EMP protective technologies?

Answer. Some of the planning performed by industry has indicated, a preference for 765 kV lines leading from the Midwest, where wind power can easily be obtained, to Chicago. Studies performed for the EMP Commission clearly indicated that long high-voltage power transmission systems (including their connected transformers) are highly vulnerable to geomagnetic storms. For example, 765 kV systems are more vulnerable to geomagnetic storms than the lower voltage systems found in most of the United States. The reason for the use of higher voltages is to minimize power loss, but protection is needed for the transformers. Clearly the protection of transformer neutrals, as discussed during the EMP Commission research, should be applied to all such new transmission systems as they are built, thereby reducing the cost of installation compared to the cost of retrofitting. Such geomagnetic storm protection will also provide protection against E3 EMP.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR MR. MICHAEL J. ASSANTE, VICE PRESIDENT AND CHIEF SECURITY OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Question 1. Why did the Critical Infrastructure Protection Committee decide against taking action on the EMP Commission findings during the September 11, 2008 meeting?

Answer. The Critical Infrastructure Protection Committee ("CIPC") is a NERC-sponsored, self-governed committee of volunteers representing users, owners, and operators of the bulk power system and other interested entities with a mission to advance the physical and cybersecurity of the critical electricity infrastructure of North America. The CIPC does not constitute all of the activities related to Critical Infrastructure Protection undertaken by NERC, nor does it definitively represent NERC's full position on any matter. The CIPC advises NERC's Board of Trustees and Electric Sector Steering Group, along with NERC staff, on matters relating to Critical Infrastructure Protection.

NERC is not in a position to explain the conclusion stated in the minutes of CIPC's September 11, 2008 meeting regarding the EMP Commission report. The CIPC has worked with the EMP Commission in the past. A subgroup of CIPC, the High Altitude Electromagnetic Pulse Task Force, was formed during 2002 and 2003 specifically for the purpose of working with the EMP Commission and providing industry insight and support for its efforts. That industry participation is referenced repeatedly throughout the EMP Commission's April 2008 report. At CIPC's invitation, Dr. Michael Frankel, Executive Director of the EMP Commission, made a pres-

entation to the committee at its March 2009 meeting about the work of the EMP Commission and the EMP Commission report.

Question 2. It is our understanding from the April 2009 letter sent by Mike Assante that a large portion of the electrical industry has not identified "critical cyber assets," which is a requirement under the NERC standards. Please explain why this letter was sent and what the response to the letter has been.

Answer. The prioritization of critical assets for protection is the foundation upon which NERC's Critical Infrastructure Protection ("CIP") standards are built. In developing the standards, the industry standards drafting team recognized that the protection of assets must occur in a staged approach, with appropriate focus being given to those elements of the system deemed "critical" to reliability. This approach was approved by the Federal Energy Regulatory Commission ("FERC") in its conditional approval of NERC's Reliability Standards CIP–002—CIP–009 in Order No. 706 on January 18, 2008.

"Critical assets" are defined in NERC's glossary of terms as those "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."[1]

Reliability Standard CIP–002 "requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."[2]

Due to the nature of the system, not all Registered Entities own or operate critical assets. Many Registered Entities, for example, own or operate a single small generating station, which would not necessarily be deemed "critical" under the definition above.

As part of the implementation plan for the CIP standards, NERC requires Registered Entities to self-certify their progress in coming into compliance with certain Reliability Standards. Responses received from the industry for the period of July–December 2008 raised a concern that all respondents may not have applied a suitable approach in identifying critical assets and their associated critical cyber assets. The April 7, 2009 letter sent by NERC's Chief Security Officer Michael Assante sought to bring clarity to the discussion of appropriate approaches to critical asset identification. The letter encouraged Registered Entities to take a fresh look at current risk-based assessment models to ensure they appropriately account for new considerations specific to cybersecurity, such as the need to consider misuse of a cyber asset, not simply the loss of such an asset. Final decisions regarding appropriate identification of critical assets and their associated critical cyber assets will be made through NERC's compliance and enforcement efforts. Compliance audits on the CIP standards have already begun.

The April 7 letter is part of the iterative process between NERC and industry stakeholders as we work together to improve reliability. In this case, NERC gathered information about the status of implementation of the Critical Infrastructure Protection standards and fed that information and its own insights back to the industry as part of a cycle of continuous improvement. NERC is working to address a critical element of the cybersecurity challenge: The educational learning curve and resulting compliance-related challenges that must be addressed to improve the cybersecurity of the bulk power system.

Question 3. Describe the expense and technical challenges in installing or implementing cyber and EMP protections for the grid?

Answer. The expense and technical challenges associated with implementing cyber and EMP protections for the grid depend upon the types of protections required and the grid systems being addressed. Thus, NERC cannot respond specifically, but we are able to provide a general response.

The nature of the Bulk Power System creates unique complexity in addressing security risk. The interconnected system includes approximately 5,000 generating plants, 165,000 miles of transmission lines, 20,000 substations, and millions of digital controls. These assets are widely dispersed, primarily located outside, and are owned and operated by approximately 1,800 different entities. The variance in size and organizational structure of these 1,800 entities present additional challenges. Entities range in size from thousands of employees to 20 or fewer employees. The organizations range from large investor-owned utilities like Exelon and Pacific Gas & Electric to non-profit electricity market operators like ISO New England; from small municipally owned utilities like the City of Orrville, OH to large Government agencies like the Tennessee Valley Authority and the U.S. Army Corps of Engineers; and from independent owners of individual generating plants like JP Morgan Ven-

[1] NERC Glossary of Terms. Version dated April 20, 2009. *http://www.nerc.com/files/Glossary__2009April20.pdf.*

[2] NERC Reliability Standard CIP–002–1. *http://www.nerc.com/files/CIP-002-1.pdf.*

tures to cooperatives of all sizes, from Great River Energy to Bluebonnet Electric Cooperative.

Systems are highly customized for specific environments, and, while common components are often used, unique configurations present challenges in providing uniform, specific guidance on protections. Actions that result in improved security on some systems could potentially result in degraded security on others. More effective approaches often involve a range of acceptable mitigation options.

The real-time operating environment also presents an important technical challenge, such that security controls that may be appropriate in other settings could present significant risks to the reliable operation of the system were they to be similarly applied to the bulk power system.

NERC believes that the asset owners would be in the best position to provide specific information on the costs and technical challenges of various protections.

Question 4. Do plans or procedures exist for the electric industry in the case of a known cyber attack or an imminent EMP? If so, can you outline them for us?

Answer. NERC's Critical Infrastructure Protection standards require an annual exercise for response to cybersecurity events. Standard CIP–009 requires that recovery plans be put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.[3]

To my knowledge, no electric industry plans or procedures have been developed specifically for an imminent EMP.

Initial planning for response to an imminent geomagnetic event was completed by many entities in response to the 1989 geomagnetic storm that triggered a widespread blackout in Quebec. Response to an imminent EMP threat would require similar measures for certain components of an EMP, but those measures would not deal with all aspects of an EMP.

Over the past year, NERC has been working to improve industry-wide responses to known or imminent threats of all kinds. NERC's alerts system allows it to reach nearly 5,000 industry professionals at operations centers, power plants, and other power system facilities across North America. A next-generation alerts tool is currently nearing completion, which will enable recipients to view and submit secure information to NERC. Contacts will be able to receive alert information via text message and e-mail.

Question 5. Does NERC have requirements for cyber and physical protections for new "Smart Grid" assets?

Answer. NERC Reliability Standards apply to the Bulk Power System as defined in Section 215 of the Federal Power Act:

(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

(B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.

Thus, "Smart Grid" assets that are necessary to the operation of the Bulk Power System can be covered under NERC Reliability Standards, but those located on facilities used in the local distribution of electric energy are not, unless such assets materially impact the bulk power system.

NERC is coordinating with NIST as it develops interoperability and system security standards for "Smart Grid" systems at the distribution level, as directed in FERC's July 2009 "Smart Grid Policy Statement".

Question 6. What efforts has NERC made to adopt NIST security standards? How do the current NERC standards differ from NIST 800–53 standards?

Answer. NERC currently has efforts underway to adapt the NIST framework for use in power system applications. The Cyber Security Order 706 Drafting Team recently posted a concept paper entitled *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions* for industry comment, which outlines a proposed framework for revising the existing Critical Infrastructure Protection Standards. Comments on the concept paper are due from industry on September 4, 2009.

Existing NERC standards primarily differ from the NIST framework in several ways:

(1) NERC standards do not presently assign a "level of risk" (Low-Medium-High) to an asset being protected;

(2) NERC standards do not include a graduated approach to controls to align with such a "level of risk" framework; and

(3) NERC standards apply to individual assets and do not comprehensively consider the systems or networks of which they are a part or the function for which they are employed.

---

[3] NERC Reliability Standard CIP–009. *http://www.nerc.com/files/CIP-009-1.pdf*.

Question 7. Is NERC required by law to follow an ANSI standards development process in writing CIP standards?

Answer. No, NERC is not required by law to have an ANSI-accredited standards process. Section 215 of the Federal Power Act does require that NERC's standards development process "provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards . . . ". (Sec. 215(c)(2)(D)). These factors are very similar to the central characteristics of an ANSI-accredited process, and in certifying NERC as the ERO, FERC found that NERC's ANSI-accredited standards development process meets the statutory requirements. NERC's standards development process is set forth in NERC's Rules of Procedure, which FERC has approved.

Question 8. Is it possible that foreign adversaries have penetrated the electric grid and are in position to cause significant damage at a time of their choosing? Are utilities capable of knowing this?

Answer. I am unable to discuss that question in an open forum. I would be prepared to work with the appropriate Government agencies to arrange a secure briefing for the subcommittee at its request.

As raised in my written testimony, the electric grid is placed at significant risk as a result of limited information-sharing between the Federal Government intelligence community and asset owners. In order to adequately protect their systems, asset owners need to know what to look for. The origin and signature of potentially dangerous code continually change and are identified by the Federal Government intelligence community. This information often remains classified, leaving asset owners without access to this classified information unable to protect and respond to potential threats.

Question 9. What are the largest risks to the electric grid, and what is NERC doing to mitigate those risks? In assessing the risk to these systems, how do you assess threat?

Answer. Some of the largest risks to the electric grid include frequent, uncontrollable events such as severe weather and other natural disasters. Other large risks are controllable events, such as the causal factors of the August 14, 2003 blackout: Untrimmed trees, untrained system operators, and malfunctioning equipment.

NERC's over 100 Reliability Standards focus on mitigating controllable risks, requiring that transmission owners maintain appropriate vegetation clearance around transmission lines, that all system operators are trained and certified, and that communications protocols are in place to ensure system operators are able to respond to events effectively.

Cybersecurity is another significant risk to the system. One of the most concerning aspects of this challenge is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyber attacker to impact multiple assets at once, and from a distance. The majority of reliability risks that challenge the bulk power system today result in probabilistic failures that can be studied and accounted for in planning and operating assumptions. Cybersecurity is unique; system planners and operators must recognize the potential for simultaneous loss of assets and common modal failure in scale in identifying what needs to be protected. This is why protection planning requires additional, new thinking on top of sound operating and planning analysis. NERC believes asset owners and system operators are critical to the protection planning process and to determining the appropriate and necessary protections for their operating environments.

High Impact, Low Frequency ("HILF") events, such as EMP events and pandemic illness, also present significant risk to the electric system. These events are the subject of an upcoming workshop to be conducted by NERC and the Department of Energy, presently targeted to be held in mid-November 2009. (Please refer to NERC's response to Question 15 for further information on this effort.)

Relative threat can be defined as a function of the probability and severity of a given event. HILF events are typically characterized by probability that is uncertain relative to other threats. Though, to NERC's knowledge, the North American Bulk Power System has never experienced a coordinated cyber attack that has affected reliability or a high-altitude detonation of a nuclear weapon, past experience is not a reliable indicator of future occurrence. NERC and the industry have no illusions of immunity to these threats.

Question 10. Has NERC done any analysis on the security of the electric grid from cyber or physical (EMP) attack? If so, how secure and resilient does NERC believe the grid is today?

Answer. NERC has several efforts underway to assess security and preparedness, including its Cyber Risk Preparedness Assessment, Bulk Power System threat assessment program, and the HILF initiative. NERC also supported and participated in the development of the EMP Commission report.

NERC believes that as Registered Entities are coming into compliance with NERC's CIP standards, the system as a whole is becoming more prepared to deal with the effects of a cyber attack to the bulk power system. Due to the ever-changing nature of this threat, however, the Bulk Power System may never be fully secure from all potential coordinated cybersecurity threats.

Certain of the measures and practices utilities put in place in response to the 1989 geomagnetic event in Quebec could provide some measure of protection against some, but clearly not all, manifestations of an EMP attack.

Question 11. What limitations does the term and definition of "bulk power system" have on the security of the electric grid at large? Assuming we can protect the "bulk power system" from attack, will that be adequate to protect the U.S. electric system?

Answer. The "Bulk Power System" is defined in Section 215(a)(1) of the Federal Power Act as:

(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

(B) electric energy from generation facilities needed to maintain transmission system reliability.

The term does not include facilities used in the local distribution of electric energy.

The authority granted by Section 215 to the Federal Energy Regulatory Commission and NERC as the "Electric Reliability Organization" places appropriate focus on the reliability of the "Bulk Power System," as outages and disturbances on that system have the potential for far greater impact than those on distribution systems. However, the terms "Bulk Power System" and "U.S. electric system" are not synonymous. Protecting the former does not guarantee that the latter will be entirely protected. Local distribution facilities are generally outside NERC's jurisdiction, except (as noted above) where local distribution facilities materially impact the Bulk Power System. The States of Alaska and Hawaii are also outside NERC's jurisdiction.

Question 12. Can the electric grid be significantly disrupted through attacks on assets that are not addressed by NERC CIP standards?

Answer. Yes. Beyond the electric sector, debilitating attacks on other critical infrastructures, such as natural gas pipelines, railways, and telecommunications, could significantly affect the Bulk Power System.

Question 13. What efforts have been initiated by NERC to require asset owners to secure this infrastructure from electromagnetic pulse events? Please provide specific details.

Answer. NERC has recently partnered with the Department of Energy on the "High Impact, Low Frequency" event workshop currently targeted to be held in mid-November. One of the goals of this workshop is to provide guidance for the development of future requirements of this nature. Please refer to NERC's response to Question 15 for further information on this effort.

Question 14. Does an early detection and warning capability for cyber and physical threats exist for the electric industry today? If not, why not?

Answer. Elements of an early detection capability exist, but mechanisms are needed to promote more information sharing between the Federal Government intelligence community and asset owners. When physical or cybersecurity events affecting critical cyber assets occur on the system, asset owners are required by NERC Reliability Standards to report this information to NERC. Asset owners are also encouraged, and many do, to report additional security events to NERC in its role as the ES–ISAC and submit an OE Form 417 to the Department of Energy regarding the event.

Mechanisms like NERC's alerts system and notifications from the United States Computer Emergency Response Team serve as effective warning capabilities for distributing critical information to the electric sector. Both mechanisms are capable of reaching wide audiences within the industry. Through its alerts system, NERC is able to require entities in receipt of the alert to acknowledge receipt and report to NERC on actions taken on recommendations included in the alert. NERC's last recommendation (December 2008) was met with a 96% response rate.

Question 15. What is the High Impact/Low Probability Working Group? When and why was it started? How will findings from this group affect the NERC CIP standards?

Answer. In partnership with the Department of Energy, NERC has recently begun an effort to assess "high impact, low frequency" risks—or, more accurately, those risks whose likelihood of occurrence is uncertain relative to other threats, but that could significantly impact the system were they to occur. Officially launched on July 2, the effort is a culmination of high-level discussions between leadership at NERC and the Department of Energy. NERC and DOE are currently recruiting members for the joint industry/Government working group, which will examine the

potential impacts of these events on the bulk power system. The group will focus on influenza pandemic, space weather, terrorist attacks, and electromagnetic pulse events and host an invitation-only workshop in the coming months to discuss their assessment and develop conclusions and recommendations to industry based on their work. These recommendations will be used to drive needed technology research, development, and investment and also to evaluate NERC's current standards and initiatives, potentially driving the creation of new standards to address these issues.

The workshop is currently slotted for mid-November 2009.

Question 16. What responsibility and involvement does NERC have in Smart Grid development and deployment?

Answer. NERC has supported the development of certain "Smart Grid" resources on the transmission system through its support of the North American Synchro-Phasor Initiative ("NASPI"). Coordinated with industry and the Department of Energy, this initiative is designed to improve power system reliability and visibility through wide area measurement and control using "phasor measurement units" or "PMUs". The NASPI community is working to advance the deployment and use of networked phasor measurement devices, phasor data-sharing, applications development and use, and research and analysis.

NERC also referenced the development of the "Smart Grid" and its potential effects on the reliability of the bulk power system in its *2008 Long-Term Reliability Assessment,* briefly mentioning cybersecurity as a primary concern when deploying "Smart Grid" infrastructure. NERC's technical committees are currently forming a "Smart Grid Task Force" to further review this issue.

As mentioned above, NERC is also coordinating with NIST through its development of Smart Grid interoperability and system security standards.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR MR. STEVEN T. NAUMANN, ON BEHALF OF EDISON ELECTRIC INSTITUTE, ELECTRIC POWER SUPPLY ASSOCIATION

Question 1. Does the industry believe that physical or cyber events are serious issues to the functioning of the electric grid?

Answer. Yes. The industry takes all threats to the reliability of the bulk power system seriously.

Question 2. Is it possible that foreign adversaries have penetrated the electric grid and are in position to cause significant damage at a time of their choosing? Are utilities capable of knowing this?

Answer. I do not know. Utilities continually monitor their systems for intrusions. I do not know whether all utilities are capable of detecting all intrusions.

Question 3. What are the largest risks to the electric grid, and what is EEI doing to mitigate those risks? In assessing the risk to these systems, how do you assess threat?

Answer. Historically, the largest risks to the grid have been created by acts of nature including hurricanes, ice storms, wildfires, and flooding. The interconnected nature of the electric grid has led to traditional coordination by the North American electric power companies in responding to those risks.

EEI member companies continually assess operational risks be they natural or manmade and work to put appropriate risk mitigation measures in place.

Most organizations perform risk assessments that include the following elements:

- Identifying threats that could harm and, thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.
- Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs.
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.

Companies throughout North America maintain strong programs to anticipate events such as hurricanes and winter storms, and to efficiently mitigate damage and restore service when such events happen. Coordination with Federal, State, and local governments, including law enforcement and emergency management, is a

critically important part of these planning processes. Through decades of experience with these extremely challenging events, electric companies understand systemic risks, including especially the nature of the reliance of the electric industry on other key infrastructure industries such as natural gas pipelines and telecommunications. In recent years, the electric utility industry has added a strong emphasis on physical and cybersecurity in response to potential terrorist attacks on critical infrastructure.

Question 4. What would industry like to see from Government in terms of an alert and warning system about an impending cyber attack? Does this early warning system exist today?

Answer. The industry is strongly interested in receiving timely, actionable and specific threat information, and having the opportunity to engage in consultation with Federal agencies as to appropriate response/attack mitigation strategies. Some elements of warning systems exist today. However, timely delivery of specific threat/threat actor information has been a challenge, due to barriers posed by sharing of classified information, as well as the time required by Government agency staff to obtain approval to release information to private industry participants. The approval and communications challenges are magnified when multiple Government agencies are involved. If the Congress wishes the electric sector to be in a position to respond to an impending cyber attack it simply must take steps to provide specific threat/threat actor information to the sector—with appropriate mechanisms to protect against inappropriate distribution and release of classified or other security-sensitive information.

Question 5. What is the current role of the Federal Government in defending against nation-state-level cyber or physical attacks against electric facilities? What should the role of the Federal Government be?

Answer. There are multiple Federal agencies involved in defending against cyber or physical attacks perpetrated by nation-states and other adversaries against electric facilities, including: The Department of Defense, the Department of Energy, the Department of Homeland Security, the Federal Bureau of Investigation, and the Office of the Director of National Intelligence, among others. While it would be difficult to describe their mission profiles with precision, the industry is very interested in receiving timely, actionable, and specific threat information from these various entities.

Question 6. What are EEI and its industry representatives doing to address the April 8, 2009 Wall Street Journal article discussing the existence of "cyberspies" in the electric grid?

Answer. NERC has been charged by Congress with overseeing the reliability of the bulk power system and addressing issues substantively. In light of this, I suggest that NERC is the appropriate entity within our sector to address and answer this question in detail.

Question 7. Have each of the EEI member companies fully implemented the mitigation measures for the Aurora vulnerability? How much did the security upgrades cost and how long did it take to mitigate these vulnerabilities?

Answer. I do not have first-hand knowledge of the actions of other companies in response to Aurora, nor the costs to mitigate any vulnerabilities. I believe that Exelon has fully implemented the mitigation measures for the Aurora vulnerability. The costs incurred by the Exelon Companies, Commonwealth Edison Company, Exelon Generation LLC and PECO Energy, in complying with the Aurora Advisory were approximately $1.2 million.

EEI does not have specific knowledge of how many companies have mitigated the Aurora vulnerability, or the costs incurred.

Question 8. EEI has a program called the Spare Transformer Equipment Program, or "STEP" program, which is supposed to increase the electric industry's inventory of spare transformers in the event of a transmission outage caused by a terrorist attack. How many extra transformers have been acquired as a result of that program?

Answer. The purpose of the STEP program is to facilitate a contract-based business program to support more efficient management of existing inventories of transformers for dealing with a triggering event, specifically a deliberate destruction of electrical transformers in connection with a terrorist event. The program is not intended to increase stockpiles per se, but to set terms and conditions for the sharing of inventories among the owners of these kinds of equipment. Thus, when a company orders a new transformer, it is difficult to specifically determine whether that order has been triggered by ordinary business needs, or, by the terms of the STEP contract. In addition, confidentiality provisions of the STEP agreement prohibit disclosure of various kinds of information.

Question 9. What are EEI's concerns about granting FERC authority to set standards for security?

Answer. The legislative discussion to date has focused on how best to ensure that electric companies will take actions in response to immediate cyber-related emergency threats. Whether conducted by FERC or NERC, EEI believes that a standards process is ill-suited for addressing this need. The present focus of the discussions is on the need for FERC to address cybersecurity issues for the bulk power system, over which it has reliability jurisdiction. EEI believes that this is the appropriate FERC role.

Legislation should define a single agency for issuing national emergency actions to the electric sector. For the kinds of broad cyber-related threats and vulnerabilities that might relate to needs for national emergency actions, EEI believes that the primary authorities located within both DOE and DHS are the appropriate locations for dealing with these matters. For DOE, its role as lead agency for the Electricity Sector Coordinating Council ("ESCC") under the National Infrastructure Protection Plan ("NIPP") suggests a broad coordination and communication role. For DHS, its broad agency role and activities with the electric industry to date suggests such a role.

For other threats and vulnerabilities that are not of an imminent national emergency nature, the Self Regulatory Organization ("SRO") model for setting standards throughout North America is strong and should be sustained. The electric industry recognizes that the NERC Critical Infrastructure Protection Standards need improvement. Development of the next version of Critical Infrastructure Protection Standards has just begun. In addition to addressing security-related concerns at NERC through the standards development process, various NERC communications processes and technical committee reviews can be used to discuss and communicate security-related reliability issues.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR MR. JOSEPH H. MCCLELLAND, DIRECTOR OF RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

Question 1. What is the current role of the Federal Government in defending against nation-state or terrorist cyber or physical attacks against electric facilities? Should the security of the electric grid rely on voluntary private sector measures? What should the role of the Federal Government be?

Answer. The commission currently has a limited role in defending against nation-state or terrorist cyber or physical attacks against electric facilities. Section 215 of the Federal Power Act (FPA) authorizes the commission to approve and enforce mandatory reliability standards for the bulk-power system, including cybersecurity standards. The commission does not, however, have authority to author or modify cyber- or physical security standards, and it has no authority to order immediate steps to mitigate a threat or vulnerability that is not addressed by current standards. The commission can only approve or remand reliability standards submitted to it by the North American Electric Reliability Corporation (NERC), the commission-certified Electric Reliability Organization (ERO). The commission can direct NERC to submit a reliability standard or a modification to a reliability standard that addresses a specific matter, but it cannot control the content of the draft standard to ensure that it sufficiently addresses the commission's directive. In the event that an inadequate standard is submitted, the commission can either approve the inadequate standard and direct modifications, or reject the standard and thereby have no standard in-place until a replacement standard is drafted by NERC and filed with the commission.

Cyber or physical attacks on the bulk-power system may constitute threats to national security, military readiness, public safety, and our Nation's economic well-being. Because of the wide-spread effects and serious consequences that a successful cyber attack may bring, it is important that swift, consistent, and effective action is taken by entities to prevent such attacks. Such action cannot be assured through a voluntary or decentralized process. The Federal Government should have the ability to protect against such attacks by having emergency authority to order mitigation measures when necessary.

Question 2. Does an early detection and warning capability for cyber and physical threats exist for the electric industry today? Is this an appropriate role for the Federal Government? What are the technical and political challenges in creating such a system?

Answer. Currently, there is no true early detection and warning capability for cyber and physical threats. Although the electric industry voluntarily created the Electric Sector—Information Sharing and Analysis Center (ES–ISAC) to share infor-

mation on certain physical and cybersecurity events (such as surveillance issues, break-ins, thefts, viruses, computer worms, etc), the scope and amount of shared information is limited.

An early detection and warning system by itself, however, is not sufficient. Considering the potential impact that a successful cyber or physical attack on the power grid could have on the safety, economy, and military readiness of the United States, the Federal Government should have the ability to order specific measures to protect against such attacks, in addition to warning entities of imminent threats.

In addition to challenges related to the secure and coordinated communication of sensitive information, including protecting such information from public disclosure, the challenges to implementing any new Federal authority would include: The ability to protect critical information about physical and cybersecurity threats and vulnerabilities and the mitigation measures employed to address them, the ability to provide cost recovery for utilities that comply with a directive to perform mitigations, and determining which power grid facilities in the United States should be subject to the commission's jurisdiction. Turning to technical challenges, it will be important to work with other agencies that can quickly identify critical system vulnerabilities and threats in order to rapidly develop effective solutions, thereby equipping the affected members of the electric industry to implement timely and effective mitigation measures.

Question 3. Who within FERC is charged with protection of the electric grid from electromagnetic pulse? Who within FERC is charged with protection of the electric grid from cyber attack?

Answer. As previously mentioned, section 215 of the FPA creates a limited role for the commission with respect to overseeing the cyber- and physical security of the bulk power system. The commission can only approve or reject reliability standards as they are developed and proposed by the ERO. Although the commission can direct the ERO to develop or modify a reliability standard to address a specific matter, it cannot author or modify the standards.

My office, the Office of Electric Reliability, has primary responsibility for monitoring the ERO's development of reliability standards and modifications to reliability standards. The Office of Enforcement has primary responsibility for overseeing the enforcement of existing standards, including the eight cybersecurity standards approved by the commission in Order No. 706. Currently, there are no standards to protect against electromagnetic pulse, and therefore there is no group or person at the commission charged with protecting the electric grid from electromagnetic pulse.

Question 4. What are the current shortcomings in FERC authority to regulate physical and cybersecurity practices throughout the electric grid?

The commission's primary authority in this area is section 215 of the FPA. Under the current statutory framework, however, the commission cannot author or modify reliability standards, and it has no authority to order emergency mitigation measures. The commission can direct NERC, as the ERO, to develop reliability standards or modifications to reliability standards that address specific matters, but this requires action through NERC's standard development process.

The commission's current authority is not sufficient to protect the electric grid from cyber- or physical security vulnerabilities and threats that endanger national security. The NERC standard development process is an open and inclusive stakeholder ballot process that typically takes time and can produce results that inadequately respond to the commission's directives. Although NERC has an expedited process, that expedited process has never been used, and even the expedited process is not likely to allow a timely, adequate response to an imminent threat. If the commission has to rely on the NERC process, and that process results in a standard that does not adequately address the threat, the commission has no authority to modify the standard and would be limited to remanding it back for additional "expedited" processes, leaving the grid vulnerable in the meantime.

Question 5. What limitations does the term and definition of "bulk power system" have on the security of the electric grid at large? Assuming we can protect the "bulk power system" from attack, will that be adequate to protect the U.S. electric system? Are all cities protected? Are facilities in Alaska and Hawaii protected? Are all generation, transmission, and distribution systems protected?

Answer. Currently, the commission defines the term "bulk power system," based on an industry-developed definition, as "the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher." However, the definition is subject to the interpretation of the regions and therefore can vary considerably from place to place. This results in inconsistent designations of what constitutes the "bulk power system" and therefore what facilities are regulated by the reliability stand-

ards. For instance, this definition excludes some major metropolitan areas such as New York City.

Additionally, section 215 of the FPA precludes the application of reliability standards to Alaska and Hawaii and to "facilities used in the local distribution of energy." Consequently, the commission cannot use its limited authority to protect Alaska, Hawaii, and distribution systems from physical and cyber threats.

Question 6. Can the electric grid be significantly disrupted through attacks on assets that are not regulated by FERC (i.e. assets that do not belong to "bulk power system")?

Answer. Yes. For example, a city or region with a large number of Smart Meters without appropriate cybersecurity protections that allow for remote disconnect is vulnerable to an attack that could cause significant disruption. If an attacker commanded all the meters to disconnect, the entire load would be dropped rapidly, which could cause large amounts of generation to be dropped, thereby potentially creating cascading outages through the transmission system. In addition, attacks could cause more permanent damage to the meters, to the point that they would need to be manually replaced and reprogrammed before they could be used again. Such repair could take several weeks, delaying power restoration to affected areas.

Question 7. Why should FERC be given authority to protect systems and assets from physical attack? What kinds of dangers are posed by physical threats like overvoltages and/or overcurrents?

Answer. The commission should be granted authority to protect systems from physical attacks because it is the agency charged with overseeing the reliability of the grid, and physical attacks can cause equal or greater destruction than cyber attacks. Direct physical attacks on electric facilities, either through malicious physical assault or natural occurrences can have devastating consequences. A set of well-coordinated direct physical attacks on the grid could jeopardize national security and military readiness and threaten the Nation's social and economic stability. Any crisis created by a physical attack could be compounded by an inability to immediately replace damaged equipment. Lead time for purchase and delivery of the most critical equipment (such as large power transformers) can be up to 2 years because of limited production and the fact that no domestic manufacturer currently provides these devices. The bulk power system is designed to withstand the loss of some critical equipment, but not at the magnitude that could fail because of a physical attack. The commission does not need, however, to displace local or other Federal authorities that have oversight of physical security.

One example of a physical threat is an electromagnetic pulse (EMP) event. In 2001, Congress established a commission to assess the threat from EMP, with particular focus on the nature and magnitude of high-altitude EMP threats to the United States, the vulnerability of U.S. military and civilian infrastructure to an attack, the capability to recover from an attack, and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure, from an attack. In 2004, the commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack. The commission issued a second report in 2008.

An EMP may also be a naturally occurring event caused by solar flares and storms disrupting the Earth's magnetic field. In 1859, a major solar storm occurred, causing auroral displays and significant shifts of the Earth's magnetic fields. As a result, telegraphs were rendered useless and several telegraph stations burned down. The impacts of that storm were muted because very little electronic technology existed at the time. Were the storm to happen today, according to an article in Scientific American, it could "severely damage satellites, disable radio communications, and cause continent-wide electrical black-outs that would require weeks or longer to recover from."

Commission staff has no data on how well the bulk power system is protected against an EMP event, and the existing reliability standards do not address EMP vulnerabilities. Protecting the electric generation, transmission, and distribution systems from severe damage due to an EMP would involve vulnerability assessments at every level of electric infrastructure. In addition, as the 2004 and 2008 commission reports point out, the reliable operation of the electric grid requires other infrastructure systems, such as communications, natural gas pipelines, and transportation, which would also be affected by an EMP attack or event.

Question 8. Does FERC maintain any existing authorities that would allow it to require owners and operators of electric facilities to harden their equipment to mitigate the effects of an electromagnetic pulse?

Answer. Section 215 explicitly addresses reliability and cybersecurity but is not explicit about its applicability to EMP. Moreover, the process under section 215 typically takes years to return a standard and there is no assurance that the standard

will be responsive to the commission's directive or adequately address the threat. As has been described earlier, the commission does not have any direct authority to require owners and operators of electric facilities to harden their equipment to mitigate the effects of an EMP attack.

Question 9. Does FERC maintain any existing authorities that would allow it to require owners and operators of electric facilities to harden their equipment to mitigate the effects of a cyber attack?

Answer. Although the commission could direct NERC to develop additional reliability standards to address the threat of a cyber attack, the process typically takes years to return a standard and there is no assurance that the standard will be responsive to the commission's directive or adequately address the threat. As has been described earlier, the commission does not have any direct authority to require owners and operators of electric facilities to harden their equipment to mitigate the effects of a cyber attack.

In January 2008, the commission exercised its authority to approve cybersecurity standards and approved eight cybersecurity standards in Order No. 706. However, upon approval, the commission found that the standards required significant modifications in order to effectively protect the bulk power system and therefore directed NERC, as the ERO, to make changes to the approved standards. Although the drafting of some of those modifications is currently under way through NERC's standards development process, it is expected to take years before all of the modifications are filed with the commission for review. Currently, the eight cybersecurity standards are in various stages of implementation and are not yet in full effect. For instance, the standards do not require that many utilities be "auditably compliant" until mid-2010.

There is reason for concern about the thoroughness and consistency with which the electric industry is applying the cybersecurity standards. In April 2009, NERC's Chief Information Officer sent a letter to industry (attached) discussing the results of an industry-wide survey of critical assets. According to NERC's findings, only 31 percent of entities identified at least one critical asset, and only 23 percent identified at least one Critical Cyber Asset. The letter also stated that only 29 percent of generation owners or operators reported at least one Critical Asset. The Chief Information Officer questioned these results and stated that NERC "will also carry out more detailed analyses to determine whether it is possible that 73 [percent] of Table 3 and 4 Registered Entities do not possess any assets that, 'if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.'" The currently approved reliability standards allow the regulated entities to self-determine the equipment that is subject to the cybersecurity standards. If the equipment is not identified, no cyber protection is required under the standard.

Question 10. What are the key aspects of any piece of legislation that seeks to secure the electric grid from cyber and physical attack? Which of the four bills currently being considered in Congress best addresses these requirements?

Answer. Any legislation that seeks to secure the electric grid from cyber and physical attack should grant the commission authority, following a determination by the President or a national security agency of a vulnerability or threat that endangers national security, to order such emergency mitigation measures or actions necessary to protect the Nation's critical electric infrastructure. This authority should encompass both physical and cybersecurity, as vulnerabilities and threats to the grid exist in both areas.

Additionally, the commission must have the ability to protect security-sensitive information from public disclosure. The potential for publication of sensitive information regarding cyber and physical threats to the security of the Nation's critical electric infrastructure weakens the commission's ability to respond to cyber threats and endangers compliance by private entities concerned about the sensitivity of information they provide to the commission.

Finally, Congress should consider applying any new legislation to electric infrastructure that is critical to the safety and security of the United States, regardless of whether the electric facilities are excluded from section 215 or included by that section. Currently under section 215, the commission has no jurisdiction over any electric infrastructure in Alaska and Hawaii, and lacks jurisdiction over some transmission, generation, and all distribution facilities in the rest of the United States.

Currently, H.R. 2195 and S. 946 address many, but not all, of these issues adequately.

Question 11. H.R. 2195 would provide FERC with authority to rewrite existing NERC standards if deemed inadequate. How do you envision exercising this authority?

Answer. H.R. 2195 proposes, inter alia, to direct the commission to establish, in consultation with the Secretary of Homeland Security, interim measures that would supplement, replace, or modify cybersecurity standards that the commission, in consultation with the Secretary of Homeland Security and other national security agencies, determines are inadequate to address known cyber vulnerabilities or threats.

I envision that the commission would use this authority only when the President or an outside intelligence agency has found that the security of the Nation is endangered by either a cyber or physical threat or vulnerability to the Nation's power supply. In these limited cases, the commission would be able to quickly develop cybersecurity interim measure that adequately address known vulnerabilities and threats, enact modifications that the commission previously directed the ERO to make, and address security issues that the ERO has not yet reached. The ERO would have the opportunity to develop and propose standards through its standards development process to replace the interim measures.

Question 12. Does the current FERC/NERC standards-setting process (i.e. NERC writes, FERC approves or remands) make sense in a national security context? Does FERC believe that industry-written standards are appropriate to protect assets as critical to national security as the electric system?

Answer. No. The FPA section 215 process is not adequate to protect against cyber- or physical security vulnerabilities and threats that endanger national security. The current standards process is too slow, open, and unpredictable to effectively address threats and vulnerabilities that endanger national security. In addition, the jurisdiction conveyed by section 215 to the commission omits major sections of the Nation's critical electric infrastructure including all facilities in Alaska and Hawaii, all distribution facilities, and some transmission and generation including facilities that serve metropolitan areas such as New York City.

Question 13. How much does compliance with current NERC mandatory standards cost the average utility? How much do you anticipate the costs would rise if FERC were given authority to write "stronger" standards? How does industry recoup the costs of mandatory standards today? Would they be able to recoup costs in the future, and if so, how?

Answer. I do not have specific information regarding the cost to individual utilities of compliance with NERC standards, and in the absence of this information, I am unable to predict the additional cost of compliance, if any, with "stronger" standards.

Typically, the costs of compliance with mandatory standards by entities that qualify as "public utilities" under the FPA are recovered either through filings submitted to the commission pursuant to section 205 of the FPA or filings made to State utility commissions. In a Statement of Policy issued September 14, 2001, the commission provided assurances to regulated entities that the commission "will approve applications to recover prudently incurred costs necessary to further safeguard the reliability and security of our energy supply infrastructure in response to the heightened state of alert." The commission further stated that "[c]ompanies may propose a separate rate recovery mechanism, such as a surcharge to currently existing rates or some other cost recovery method." The commission reiterated this policy in an April 19, 2004 Statement of Policy on matters related to bulk power system reliability.

If Congress believes it appropriate, it could include in legislation a directive to the commission to establish a cost recovery mechanism for the costs associated with compliance with any commission order issued pursuant to emergency authority.

Question 14. Should a regulator like FERC provide resources (funding) to utilities to implement physical and cyber protections?

Answer. Any Federal Government funding of such efforts would be more appropriately assigned to the Department of Homeland Security or the Department of Energy. However, a simpler approach could be to allow the commission to grant cost recovery to the affected entities for any mitigation measures that it orders.

Question 15. Are procedures in place today that would allow FERC to issue immediate orders upon receipt of information that a physical or cyber attack is imminent? What are those procedures, and are they regularly exercised? (For instance, what could be done to protect the grid from an imminent geomagnetic event given 15 minutes of warning?) Could the effects of such an incident actually be mitigated in time?

Answer. No, there are currently no procedures or authorities in place that would allow the commission to issue orders that address imminent cyber or physical attacks. The commission does not have authority to immediately and directly order actions to thwart imminent physical or cyber attacks. As I have mentioned, under the framework established by section 215 of the FPA, the commission approves and enforces mandatory standards that are developed and proposed by a self-regulatory

organization and submitted to the commission. This process is too slow, open, and unpredictable to address imminent threats to the power grid that imperil national security.

If such authority did exist, however, it is possible that the commission could issue an effective order with only 15 minutes warning if an emergency plan that has already been prepared and practiced is in place. For example, according to the EMP Commission, an effective measure to protect large transformers from an EMP event is a resistor connected in the neutral of the transformer. If such a resistor had been installed ahead of time, it is conceivable that it could be switched on within 15 minutes if the utility had enabled remote operation and provided adequate training and practice drills. For a cyber threat, an effective order might be to direct the immediate disconnect of the remote capabilities of targeted facilities if an adequate plan had been developed along with training and practice drills.

Question 16. What involvement does FERC have in Smart Grid development and deployment?

Answer. On July 16, 2009, the commission issued a final Smart Grid Policy Statement. This policy statement sets priorities to guide the electric industry in the development of Smart Grid standards for achieving interoperability and functionality of Smart Grid systems and devices. It also sets out commission policy for the recovery of costs by utilities that act early to adopt Smart Grid technologies. The new policy adopts as a commission priority the early development by industry of Smart Grid standards that: (1) Ensure the cybersecurity of the grid; (2) provide two-way communications among regional market operators, utilities, service providers and consumers; (3) ensure that power system operators have equipment that allows them to operate reliably by monitoring their own systems as well as neighboring systems that affect them; and (4) coordinate the integration into the power system of emerging technologies such as demand response resources, electricity storage facilities, and electric transportation systems. Additionally, commission staff routinely participates in various National Institute of Standards and Technology efforts concerning Smart Grid standards, as well as coordinates with the Department of Energy on its Smart Grid efforts.

Question 17. Does FERC believe that the Energy ISAC is effective in producing timely and relevant analysis and warnings for the industry? If not, what measures can be undertaken to improve this capability?

Answer. The ES–ISAC is effective when transmitting system status information and information regarding operational issues that can affect other areas or utilities. While this provides some threat information on technical issues (such as viruses and computer worms) and certain physical threats (such as surveillance issues and copper theft threats), it is very limited. However, this system was not designed and is not operated in order to address vulnerabilities and threats that endanger national security. As an example, although ES–ISAC acts as a forum to share information regarding security-related events that are occurring across the bulk-power system, this forum cannot preemptively identify the vulnerabilities and threats and does not develop effective mitigations to address the issues it reports.

Question 18. Do you believe that the Spare Transformer Program has been successful, and that there are enough spare transformers that could be put in place to ensure operation of the gird in the event of a large-scale cyber or EMP event?

Answer. As the commission stated when it issued a declaratory order about the program, the Spare Transformer Program initiated by the Edison Electric Institute is a good first step. The program is limited, however, because it does not cover all voltage classes or step-up transformers from generating stations, and many utilities do not participate. For these and other reasons, the program does not have adequate spares to ensure continued operation of the power grid after a targeted cyber or large-scale EMP event.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR MS. PATRICIA A. HOFFMAN, ACTING ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, DEPARTMENT OF ENERGY

Question 1. What is the current role of the Federal Government in defending against nation-state or terrorist cyber or physical attacks against electric facilities? Should the security of the electric grid rely on voluntary private sector measures? What should the role of the Federal Government be?

Answer. Response was not received at the time of publication.

Question 2. Does an early detection and warning capability for cyber and physical threats exist for the electric industry today? Is this an appropriate role for the Federal Government? What are the technical and political challenges in creating such a system?

Answer. Response was not received at the time of publication.

Question 3. Who within DOE is charged with protection of the electric grid from electromagnetic pulse? Who within DOE is charged with protection of the electric grid from cyber attack?

Answer. Response was not received at the time of publication.

Question 4. What limitations does the term and definition of "bulk power system" have on the security of the electric grid at large? Assuming we can protect the "bulk power system" from attack, will that be adequate to protect the U.S. electric system? Are all cities protected? Are facilities in Alaska and Hawaii protected? Are all generation, transmission, and distribution systems protected?

Answer. Response was not received at the time of publication.

Question 5. Can the electric grid be significantly disrupted through attacks on assets that are not regulated by FERC (i.e. assets that do not belong to "bulk power system")?

Answer. Response was not received at the time of publication.

Question 6. Does DOE maintain any existing authorities that would allow it to require owners and operators of electric facilities to harden their equipment to mitigate the effects of an electromagnetic pulse?

Answer. Response was not received at the time of publication.

Question 7. Does DOE maintain any existing authorities that would allow it to require owners and operators of electric facilities to harden their equipment to mitigate the effects of a cyber attack?

Answer. Response was not received at the time of publication.

Question 8. Does the current FERC/NERC standards-setting process (i.e. NERC writes, FERC approves or remands) make sense in a national security context? Does DOE believe that industry-written standards are appropriate to protect assets as critical to national security as the electric system?

Answer. Response was not received at the time of publication.

Question 9. The Office of Electricity Delivery and Energy Reliability received $4.5 billion in the American Recovery and Reinvestment Act, of which $3.5 billion is for grants for Smart Grid development. How do you intend on disbursing this grant money? In reviewing applications for monies, how will DOE determine if appropriate physical and cyber protections are in place? Will you award grants to applicants for the purpose of protecting their systems against physical and cyber attacks?

Answer. Response was not received at the time of publication.

Question 10. Does DOE have a program that would allow for private or publicly-owned utilities to receive Federal grant monies for hardening their equipment against an intentional or unintentional electromagnetic pulse? If not, why not? Should such a program be created, and, if so, what would appropriate parameters look like?

Answer. Response was not received at the time of publication.

Question 11. Does DOE have a program that would allow for private or publicly-owned utilities to receive Federal grant monies for hardening their equipment against an intentional cyber attack? If not, why not? Should such a program be created, and, if so, what would appropriate parameters look like?

Answer. Response was not received at the time of publication.

Question 12. When will DOE update its control systems roadmap?

Answer. Response was not received at the time of publication.

Question 13. Has DOE done any analysis on the security of the electric grid from cyber or physical attack? If so, how secure and resilient does DOE believe the grid is today?

Answer. Response was not received at the time of publication.

Question 14. Does DOE currently have any authority to perform cyber or physical vulnerability assessments on private or publicly-owned electric grid assets?

Answer. Response was not received at the time of publication.

Question 15. Are procedures in place today that would allow DOE to issue immediate orders upon receipt of information that a physical or cyber attack is imminent? What are those procedures, and are they regularly exercised? (For instance, what could be done to protect the grid from an imminent geomagnetic event given 15 minutes of warning?) Could the effects of such an incident actually be mitigated in time?

Answer. Response was not received at the time of publication.

Question 16. Does DOE believe that the Energy ISAC is effective in producing timely and relevant analysis and warnings for the industry? If not, what measures can be undertaken to improve this capability?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRWOMAN YVETTE D. CLARKE OF NEW YORK FOR SEÁN P. MCGURK, DIRECTOR, CONTROL SYSTEMS SECURITY PROGRAM, NATIONAL CYBERSECURITY DIVISION, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Question 1. What is the role of DHS in securing the electric grid, and how do you carry out that mission? What programs and policies exist? How are you resourced?

Answer. Response was not received at the time of publication.

Question 2. What are the largest threats to the electric grid, and what is DHS doing to mitigate those threats?

Answer. Response was not received at the time of publication.

Question 3. What authorities does DHS have to address cyber and physical threats to the electric grid?

Answer. Response was not received at the time of publication.

Question 4. Who within DHS is charged with protection of the electric grid from electromagnetic pulse? Who within DHS is charged with protection of the electric grid from cyber attack?

Answer. Response was not received at the time of publication.

Question 5. Out of the critical infrastructure and key resource sectors, what is the criticality of the electric grid?

Answer. Response was not received at the time of publication.

Question 6. Has DHS done any analysis on the security of the electric grid from cyber or physical attack? If so, how secure and resilient does DHS believe the grid is today?

Answer. Response was not received at the time of publication.

Question 7. Does DHS currently have any authority to perform cyber or physical vulnerability assessments on private or publicly-owned electric grid assets?

Answer. Response was not received at the time of publication.

Question 8. What is the current role of the Federal Government in defending against nation-state or terrorist cyber or physical attacks against electric facilities? Should the security of the electric grid rely on voluntary private sector measures? What should the role of the Federal Government be?

Answer. Response was not received at the time of publication.

Question 9. Does an early detection and warning capability for cyber and physical threats exist for the electric industry today? Is this an appropriate role for the Federal Government? What are the technical and political challenges in creating such a system?

Answer. Response was not received at the time of publication.

Question 10. Does DHS believe there are shortcomings in FERC authority to regulate physical and cybersecurity practices throughout the electric grid?

Answer. Response was not received at the time of publication.

Question 11. What recommendations has DHS ever made to DOE or FERC regarding electric grid protections, and have those recommendations been followed?

Answer. Response was not received at the time of publication.

Question 12. Does DHS have a program that would allow for private or publicly-owned utilities to receive Federal grant monies for hardening their equipment against an intentional or unintentional electromagnetic pulse? If not, why not? Should such a program be created, and, if so, what would appropriate parameters look like?

Answer. Response was not received at the time of publication.

Question 13. Does DHS have a program that would allow for private or publicly-owned utilities to receive Federal grant monies for hardening their equipment against an intentional cyber attack? If not, why not? Should such a program be created, and, if so, what would appropriate parameters look like?

Answer. Response was not received at the time of publication.

Question 14. Does the current FERC/NERC standards-setting process (i.e. NERC writes, FERC approves or remands) make sense in a national security context? Does DHS believe that industry-written security standards are appropriate to protect assets as critical to national security as the electric system?

Answer. Response was not received at the time of publication.

Question 15. Does DHS support the grant of authority under HR 2195, which would provide DHS with authority to assess cyber vulnerabilities or threats to critical infrastructure, including critical electric infrastructure and advanced metering infrastructure, on an on-going basis and produce reports, including recommendations, on a periodic basis?

Answer. Response was not received at the time of publication.

Question 16. Are procedures in place today that would allow DHS to issue immediate orders or advisories upon receipt of information that a physical or cyber attack

is imminent? What are those procedures, and are they regularly exercised? (For instance, what could be done to protect the grid from an imminent geomagnetic event given 15 minutes of warning?) Could the effects of such an incident actually be mitigated in time?

Answer. Response was not received at the time of publication.

○