THE EMP THREAT: EXAMINING THE CONSEQUENCES

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

SEPTEMBER 12, 2012

Serial No. 112–115

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

80–856 PDF WASHINGTON : 2013

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
RON BARBER, Arizona

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

DANIEL E. LUNGREN, California, *Chairman*

MICHAEL T. MCCAUL, Texas
TIM WALBERG, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
BILLY LONG, Missouri
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

COLEY C. O'BRIEN, *Staff Director*
ZACHARY D. HARRIS, *Subcommittee Clerk*
CHRIS SCHEPIS, *Minority Senior Professional Staff Member*

CONTENTS

Page

FOR THE RECORD

APPENDIX

THE EMP THREAT: EXAMINING THE CONSEQUENCES

Wednesday, September 12, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:11 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, Long, Clarke, Richardson, and Richmond.

Mr. LUNGREN. The Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. This subcommittee is meeting today to examine the electromagnetic pulse threat.

I will now recognize myself for an opening statement.

The Washington, DC area was recently impacted by a deadly, fast-moving storm, called a derecho—a word I had never heard of before until I found myself in the midst of it—which is one of the most destructive and deadly thunderstorm systems in North American history. It resulted in 22 deaths, widespread damage, and millions of power outages from the Midwest to the Middle Atlantic States.

This derecho provided a glimpse of the kind of destruction—just a glimpse of the kind of destruction that would result from an electromagnetic pulse (EMP) attack. Falling trees and the loss of electric power caused death and destruction from Chicago to Virginia. Fortunately, this power outage was short-term, which limited the human and economic consequences.

An EMP is a burst of electromagnetic radiation typically generated by a high-altitude nuclear explosion or a non-nuclear device. Nuclear weapon EMPs are most effective when detonated high in the altitude above the intended target. Depending on the yield of the weapon and the height of the explosion, nuclear EMPs can destroy large portions of the U.S. power and communications infrastructure, we are informed.

Geomagnetic radiation generated by a naturally occurring solar storm can also damage the same infrastructure. An EMP attack would destroy the electronics and digital circuitry in the area of impact, thereby denying electric power to our homes, businesses, and military.

Our country is dependent on electricity to power our health, financial, transportation, and business systems. If our power system was ever lost for an extended period, according to Dr. William Graham, the chairman of the EMP Commission, it would have catastrophic and lethal consequences for our citizens and the economy. It would also potentially degrade our military defenses.

America's digital dependence grows every year and we rejoice in that. But the fact of the matter is that along with that dependence comes our EMP vulnerability. What I mean by that is America has gotten used to the digital world. It powers and is implicated in so much of our everyday life, that if it were in fact attacked in a serious way, it would result in some cases, unforeseen circumstances. What I mean by that is most people don't think about them.

Computer simulations carried out in March 2010 by Oak Ridge National Laboratory demonstrated that an electromagnetic pulse from a nuclear device detonated at high altitude or a powerful solar storm could destroy or permanently damage major sections of our National power grid. According to this Oak Ridge study, the collapse of our power system could impact 130 million Americans, could require 4 to 10 years to fully recover, and could impose economic costs between $1 trillion and $2 trillion.

The National electric grid has almost no backup capability in the event of a power collapse from electromagnetic pulses. According to FERC testimony presented this morning, existing bulk power reliability standards don't even address EMP vulnerabilities. In addition, with most of the Nation's power system under private ownership, who view an EMP event as unlikely or so we are told, there is been little preparation for a long-term power collapse.

Although the impact of an EMP event has been examined, studied, and debated, I am fearful that little progress seems to have been made in mitigating the EMP threat. Although the United States has conducted numerous exercises to test our readiness against natural events such as hurricanes, we have never conducted an exercise to help us prepare for the severe consequences of a National power outage from an EMP event.

I am informed that the Defense Department takes this seriously and, therefore, has taken steps to protect many of their critical infrastructure from an EMP event. Either they are wasting a lot of money because it is not a serious event—we should stop them from doing it and save us billions of dollars—or it is a serious threat to our National defense capabilities, and we ought to look in the same way in terms of our domestic capabilities. That is, what sustains our standard of living, but in some ways, a way of life for the American public.

I don't want to be an alarmist on this. I want to be a realist on this. That is why we have asked a number of people to testify here today, so that we can get our hands around this, at least a little better than we have to this point.

In today's hearing, we will examine the consequences of an EMP attack, and examine whether we are adequately protecting our power system and other critical infrastructure from this growing vulnerability. My thought is that the more information, the greater awareness the American people have and that we as leaders have,

the better we will be prepared to deal with this, as long as we understand what the true consequences are.

Okay, and so at this point in time, I would recognize my colleague from California for a statement representing her side of the aisle.

[The statement of Chairman Lungren follows:]

STATEMENT OF CHAIRMAN DANIEL E. LUNGREN

SEPTEMBER 12, 2012

The Washington DC area was recently impacted by a deadly fast-moving storm called a derecho which was one of the most destructive and deadly thunderstorm systems in North American history. It resulted in 22 deaths, widespread damage and millions of power outages from the Midwest to the Middle Atlantic States. This derecho provided a glimpse of the kind of destruction that would result from an electromagnetic pulse (EMP) attack. Falling trees and the loss of electric power caused death and destruction from Chicago to Virginia. Fortunately, this power outage was short-term, which limited the human and economic consequences.

An EMP is a burst of electromagnetic radiation typically generated by a high-altitude nuclear explosion or a non-nuclear device. Nuclear weapon EMPs are most effective when detonated high in the altitude above the intended target. Depending on the yield of the weapon and the height of the explosion, nuclear EMPs can destroy large portions of the U.S. power and communications infrastructure. Geomagnetic radiation generated by a naturally occurring solar storm can also damage this same infrastructure.

An EMP attack would destroy the electronics and digital circuitry in the area of impact, denying electric power to our homes, businesses, and military. Our country is dependent on electricity to power our health, financial, transportation, and business systems. If our power system was ever lost for an extended period, according to Dr. William Graham the chairman of the EMP Commission, it would have catastrophic and lethal consequences for our citizens and the economy. It would also degrade our military defenses. America's digital dependence grows every year and along with that dependence, our EMP vulnerability.

Computer simulations carried out in March 2010 by Oak Ridge National Laboratories demonstrated that an electromagnetic pulse from a nuclear device detonated at high attitude or a powerful solar storm could destroy or permanently damage major sections of our National power grid. According to this Oak Ridge Study, the collapse of our power system could impact 130 million Americans, require 4 to 10 years to fully recover and impose economic costs of $1 to $2 trillion.

The National electric grid has almost no backup capability in the event of a power collapse from electromagnetic pulses. According to FERC testimony presented this morning, existing bulk power reliability standards don't even address EMP vulnerabilities. In addition, with most of the Nation's power system under private ownership, who view an EMP event as unlikely, there has been little preparation for a long-term power collapse. Although the impact of an EMP event has been examined, studied, and debated, little progress seems to have been made in mitigating the EMP threat. Although the United States has conducted numerous exercises to test our readiness against natural events such as hurricanes, we have never conducted an exercise to help us prepare for the severe consequences of a National power outage from an EMP event.

Today's hearing will examine the consequences of an EMP attack and whether we're adequately protecting our power system and other critical infrastructure from this growing vulnerability.

I now recognize the Ranking Member, the gentle lady from New York, Ms. Clarke, for her opening statement.

Ms. RICHARDSON. Good morning, Mr. Chairman, and those before us.

Before I start my prepared comments, I would like to acknowledge the unfortunate passing of Ambassador Stevens of Libya and also the several other Foreign Service personnel members who we lost. It is times like these on both sides of the aisle where it really doesn't matter that there is an aisle. We are all here to serve this country and we are very grateful for our Foreign Service personnel

who advocate and, in many instances, implement the policies that we have brought forward. So I first would like to do that on behalf of all of us.

Mr. Chairman Lungren and Ranking Member Clarke, it is very good and I concur with the Chairman of convening this hearing today on the threat of electromagnetic pulse (EMP) that the potential impacts that it could have on our critical infrastructure, which we witnessed, unfortunately, several months ago.

I look forward to this hearing from our esteemed panel of witnesses, including our colleague Congressman Trent Franks.

I also welcome back Chris Beck to this hearing before our subcommittee. It has been a pleasure working with you on this subcommittee, and I look forward to your testimony.

An electronic magnetic pulse can be caused by solar activity, nuclear explosions, lightning, or other sources. The energy from any electromagnetic pulse can damage or destroy electronics, such as cell phones, car computers, and computer networks. We have found that we depend upon cell phones in times of emergencies. It was quite alarming that through this latest storm that we had, the tremendous impact that it had on cell phones. We found them not to be immune and to be the sole source of our means of communication.

Our electric grid is also vulnerable to electromagnetic pulse. The EMP that knocks out our electric grid would have a catastrophic consequence that could result in lives lost, as well as having a devastating impact on our economy.

While an EMP attack on our electric grid is a high-impact, low-frequency event, we need to be cognizant of its consequences. We can and should take precautions to make our electronics and our grid more resilient to an EMP incident.

The Department of Homeland Security has not identified EMP as a high-risk threat, and thus has not included it in its 15 all-hazards National planning scenarios. I am interested to hear from all of our witnesses today whether planning and preparing for an EMP attack is appropriate.

I thank the Chairman and Representative Clarke for holding this hearing today. I hope that we can learn forward how we might best protect our critical infrastructure against natural and terrorist threats.

Finally, I would like to say, Mr. Chairman, I would like to ask unanimous consent that the opening statement of the full committee Ranking Member Mr. Thompson be submitted for the record.

Mr. LUNGREN. Without objection.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

SEPTEMBER 12, 2012

Thank you, Mr. Chairman for holding this hearing on electromagnetic pulse threats. I want to welcome our colleague, Mr. Franks, who will testify about his bill, H.R. 668, the SHIELD Act, which has been referred to the Energy and Commerce Committee, and the Budget Committee.

I also want to welcome all of our witnesses, but especially Dr. Chris Beck, a former staffer of this committee.

Scientists tell us that a geomagnetic solar storm capable of affecting parts of the U.S. electrical grid is an event with a low probability of occurrence. However, if such a thing were to occur, it could have a serious impact on our electrical transmission system.

Our witnesses today will be able to shed some light on the probability of such an event, and the likelihood and severity of the effects on the electric grid and other critical infrastructure.

But in this time of increasingly tight budgets, we must depend on risk analysis to guide us in making the tough decisions about our priorities.

We know the electric grid is vulnerable to disruption. I am very interested in the testimony today, to hear about how the Department of Homeland Security assesses the risk of geomagnetic storms and other EMP threats.

I am pleased that the North American Electric Reliability Corporation has submitted a statement for the record. They are the folks on the ground dealing with how the electric industry prepares for grid vulnerabilities, and it is important that we listen carefully to their findings.

Thank you again Mr. Chairman, and I yield back.

Ms. RICHARDSON. Thank you. The next one, I will hold. Thank you, sir. I yield back.

Mr. LUNGREN. I thank the gentlelady.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Clarke follows:]

STATEMENT OF RANKING MEMBER YVETTE D. CLARKE

SEPTEMBER 12, 2012

Good morning and thank you Mr. Chairman for holding this hearing on our efforts to assess the EMP threat.

I too, also want to welcome our colleague, Mr. Franks, to the subcommittee. He has helped write the road map for addressing the EMP threat, and I am glad he is here to discuss his bill.

I also want to welcome our other witnesses today, and especially Dr. Beck, who formerly was the staff director for this subcommittee and is an expert on this matter. Welcome back Chris. I look forward to all the testimony.

I believe it is important that we find the building blocks for a partnership that will bring improvements to the security and reliability of one of our most important critical infrastructures, the electric grid.

This hearing will help give this topic the visibility it deserves. We all know the grid plays a fundamental role in our lives, our economy, and way of life. We simply cannot afford to lose broad sections of the grid for days, or weeks.

It is our very reliance on this infrastructure that makes it important to anticipate the worst, and there are many scenarios that we should concerned about.

We are still learning about the significant threat that could come in the form of a natural or manmade Electromagnetic Pulse, and we have more to learn about the effects of an EMP and geomagnetic disturbances to the grid as well.

Over the past few years, I have followed with interest Secure Grid exercises that The National Defense University has held at Fort McNair. These series of tabletop exercises on U.S. electrical grid security have focused on the effects of a major geomagnetic storm on the Nation's electrical infrastructure.

With the 12-year peak in solar activity approaching in 2012–2013, there is considerable upturn in interest from Government agencies, including the White House and Congress, in understanding the potential impacts if a severe geomagnetic disturbance event should occur.

Although this is a low-probability event, the consequences of an extended and widespread power loss across portions of the country would constitute a serious National emergency.

To me, one of the largest barriers to Government agency disaster response is cross-agency coordination and roles of authority—crucial elements made more difficult when discussing the privately-owned National electrical grid.

Ultimately, the Secure Grid exercises and other policy discussions work to identify preparedness gaps in plans to manage the challenges associated with extended power outages, and add urgency to existing efforts to identify technology solutions to protect the U.S. grid.

Hearings such as this serve to highlight areas where the United States and its Allies are analyzing the risks that a severe geomagnetic disturbance would present, and help us look for international approaches to effectively react to these risks.

While severe solar storms that create geomagnetic disturbances cannot be prevented, there are tools and opportunities to mitigate and protect the grid from the risks of such an event.

My colleagues on the Homeland Security Committee and I have spent nearly 3 years identifying and reviewing the security protections that are in place to mitigate the effects 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 extensive discussions and review with the private sector, which owns, operates, and secures the grid. The private sector develops its own security standards and also oversees compliance with these standards. In short, the private sector has the responsibility for securing the grid from electromagnetic events and cyber attacks.

I am very pleased to see the statement for the record submitted by the North American Electric Reliability Corporation. These are the folks who are closest to the electric grid, and they manage an almost impossibly complex flow of energy, not to just our 330-plus million people, but also the flow of energy across our borders . . . every day.

Finally, the U.S. Congress has also acted. In June 2010, the GRID Act passed the House of Representatives unanimously. Unfortunately, it stalled in the Senate and did not become law.

The bill would have granted the Federal Energy Regulatory Commission expanded authorities to oversee electromagnetic and cyber protections.

This Congress, Mr. Franks has introduced a version of the bill, now called the SHIELD Act, which is similar to the GRID Act but focuses only on the electromagnetic threat component without the cybersecurity component.

I am a co-sponsor of that bill, and it is our hope that during the next Congress we will get the bill through both Houses and to the President's desk.

With that, Mr. Chairman, I yield back.

Mr. LUNGREN. Before I introduce our first witness, I have written statements from the North American Electric Reliability Corporation and private citizen, Mr. Nicholas Leggett. I ask unanimous consent that these two statements may be made a part of the record.

Without objection, so ordered.

[The information follows:]

STATEMENT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SEPTEMBER 12, 2012

The mission of the North American Electric Reliability Corporation (NERC) is to ensure the reliability of the bulk power system of North America and promote reliability, excellence, and accountability in the electric utility industry. In 2007, NERC was designated the Electric Reliability Organization (ERO) by the Federal Energy Regulatory Commission (FERC) in accordance with Section 215 of the Federal Power Act (FPA), enacted by the Energy Policy Act of 2005. To ensure the reliability of the bulk power system, NERC relies on the combined expertise of the North American electric power industry. NERC works collaboratively with industry and Government experts to address issues impacting the bulk power system, including the effects of geomagnetic disturbances. NERC is pleased to provide written comments as requested by the committee to discuss the differences between electromagnetic pulses and geomagnetic disturbances, and provide an update on current activities underway to address geomagnetic disturbances.

ELECTROMAGNETIC PULSES VS. GEOMAGNETIC DISTURBANCES

Geomagnetic disturbances (GMDs) are part of a class of risks called High-Impact, Low-Frequency (HILF) events. These events are characterized by their potential to impose very large adverse impacts on the electric power system (and other infrastructures in some cases), their infrequent nature, and hence, the industry's limited experience mitigating them. This group of risks includes major disasters such as earthquakes, tsunamis, and pandemics. The group also includes man-made phe-

nomena such as electromagnetic pulses (EMPs) caused by high-altitude nuclear blasts.

EMP attacks are often studied alongside, and confused with, GMDs. One reason is that a component of an EMP, the E3 wave, is similar to a GMD in its effects; however, the E3 wave has a larger magnitude and shorter duration than a GMD, and it occurs after the grid has already been exposed to the other more intense components of an EMP, the E1 and E2 waves.[1] As with GMD, the E3 component can induce currents that couple to transmission lines and drive high-voltage transformers to saturation, potentially disrupting or damaging equipment of the electric power delivery system. There are significant differences between EMP and GMD in both the nature of the threat, the science behind their impacts, and the scale and form of potential solutions.

EMPs result from nuclear blasts that represent intentional acts of war, something first and foremost in the domain of National defense and security. For that reason, the Electricity Subsector Coordinating Council (ESCC) concluded that NERC should focus its efforts on the risk and underlying science behind the naturally-occurring phenomenon of GMD.

OVERVIEW—GEOMAGNETIC DISTURBANCES

Solar magnetic pulses emanate from the sun, causing GMDs on Earth. According to space scientists, solar coronal holes and coronal mass ejections are the two main categories of solar activity that drive solar magnetic disturbances on Earth. Coronal mass ejections create a large mass of charged solar energetic particles that escape from the sun's halo (corona), traveling to Earth in 14 to 96 hours. These high-energy particles consist of charged electrons, along with coronal and solar wind ions.

GMDs are produced when a large coronal mass ejection occurs and is directed at Earth. The interaction between the particle cloud and the earth's magnetic field can cause geomagnetically-induced currents to arise on the power system. The intensity of the effects on the power system depends on a number of factors such as the polarity of the magnetic structures created by the charged particle cloud, geomagnetic latitude of the impacted system, directionality of the disturbance, and geology (electrical conductivity of the ground), as well as power system characteristics such as system configuration and power system impedances.

Geomagnetically-induced currents can be measured directly using monitors attached to the neutral connections of power transformers. The measurements from these monitors, along with alerts and warnings issued by the National Oceanographic and Atmospheric Administration (NOAA) Space Weather Prediction Center or the Canadian Space Weather Forecast Centre, can provide the key information that a GMD event is imminent or in progress, and can support or trigger preplanned operational decisions and actions.

NERC AND GMD

In November 2009, NERC and the U.S. Department of Energy (DOE) held a 2-day workshop on HILF event risk to the North American Bulk Power System. The proceedings of this workshop and recommendations were documented in a jointly released report in 2010,[2] which outlined a plan to address these risks to the bulk power system, including proposals for action and options to respond to GMDs.

Following the release of the NERC and DOE June 2010 assessment, the ESCC, chaired by NERC President and CEO Gerry Cauley, developed the Strategic Roadmap to address HILF events through an organized combination of industry-led task forces and initiatives, including the formation of a NERC GMD Task Force. FERC held a technical conference on GMD in February 2011, and NERC held a workshop in April 2011 to develop strategies and plans to address this risk. NERC released a NERC Alert[3] to the industry on GMDs in May 2011, providing bulk power system owners and operators with immediate operating and planning actions that could be taken to mitigate the impact of a large geomagnetic storm.

NERC issued a Special Reliability Assessment Interim Report on GMDs (Interim Report)[4] in February 2012. The report highlights the potential for voltage collapse and the damage or loss of a limited number of vulnerable transformers across the North American bulk power system. Previous examples of the impact of GMDs, such

---

[1] Radasky, W. A., "High-altitude EMP (HEMP) Environments and Effects," NBC Report, Spring/Summer 2002, pp. 24–29.

[2] *http://www.nerc.com/files/HILF.pdf.*

[3] *http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01__GMD-__FINAL.pdf.*

[4] *http://www.nerc.com/files/2012GMD.pdf.*

as a 1989 event which led to the fast collapse of the Hydro Québec system, showed these effects. The 1989 event left more than 6 million people without power for 9 hours, demonstrating that severe solar storms represent a serious risk that can challenge the reliability of the bulk power system.

IMPLEMENTING THE TASK FORCE RECOMMENDATIONS AND NEXT STEPS

In May of 2012, NERC filed comments[5] with the FERC addressing the recommendations outlined in the Interim Report. NERC is currently implementing a Phase 2 workplan[6] for the reconvened NERC GMD Task Force that outlines the specific tasks necessary to support these recommendations.

NERC is coordinating its efforts on GMD with agencies and other stakeholder groups in the United States and Canada such as DOE, NOAA, SpaceWeather Canada, the U.S. Geological Survey (USGS), Natural Resources Canada (NRCan), the U.S. National Aeronautics and Space Administration (NASA), the Canadian Space Agency, the Electric Power Research Institute (EPRI), the Institute for Electrical and Electronic Engineers (IEEE), the North American Transmission Forum, and other industry and scientific organizations. These efforts are focused on two key areas: (1) Assessing the vulnerability of the North American transformer fleet, using power system modeling with space weather simulation and transformer thermal characteristics; and (2) surveying the industry for best practices in operations to respond to GMDs and updating the NERC Industry Alert. In tandem with these efforts, and in support of other HILF events, NERC has released a revamped Spare Equipment Database to support the sharing of equipment amongst entities in the face of a catastrophic event.

The potential for voltage collapse and the loss of even a limited number of transformers as a result of a GMD is a serious issue that should be addressed to minimize the effects on bulk power system reliability. NERC, through industry groups and the membership of the NERC GMD Task Force, is working to provide power system planners and operators with the necessary information to develop better design criteria to withstand GMDs, the tools to identify problems that may result from GMDs, improved operating procedures to protect reliability in response to GMDs event, and mitigating approaches to address impacts of GMDs. The approaches and need for action may differ depending on the geomagnetic latitude, geology, as well as transformer design and health.

To supplement the work of the NERC GMD Task Force, NERC, EPRI, DOE, and 12 industry organizations have funded a collaborative research and development project focused on developing and enhancing tools to better prepare and manage effects from strong GMDs. Open-source software to calculate geomagnetically-induced current has been developed, and several commercial software vendors are incorporating GMD studies into their power flow packages, so that commonly-used off-the-shelf tools will soon be available for industry planners to study the impact of GMD on their systems. Additionally, the recent release of publically available "1-in-100-year" wave-forms by NASA will facilitate industry benchmarking and establish common frames of reference for comparative analysis.

The primary goals of the NERC GMD Task Force in its continuing work are to:

- Provide industry subject-matter expertise and volunteer industry participation as appropriate in the development of tools and practices to study and mitigate the effects of GMDs;
- Motivate, review, and verify (where applicable) the work products of NERC and other industry and scientific organizations in support of power system and transformer vulnerability assessment, improved operational practices, and information exchange;
- Augment and finalize the Interim Report on GMD; and
- Set an industry path forward towards addressing identified vulnerabilities.

The four key activities to support these goals are:

1. Vulnerability assessment through system analysis, to enhance system design, operating procedures, and mitigation techniques;
2. Training of planners and operators;
3. Spare equipment inventory management; and
4. Development of improved transformer specifications to withstand geomagnetically-induced current (GIC).

---

[5] *http://elibrary.ferc.gov/idmws/common/OpenNat.asp?fileID=12989318.*

[6] *http://www.nerc.com/docs/pc/gmdtf/GMD__Phase__2__Project__Plan__APPROVED.pdf.*

1. VULNERABILITY ASSESSMENT THROUGH SYSTEM ANALYSIS, TO ENHANCE SYSTEM DESIGN, OPERATING PROCEDURES, AND MITIGATION TECHNIQUES

The conclusions of the 2012 Interim Report on GMDs will be validated through detailed vulnerability assessment of the North American grid, undertaken by industry experts with the support of NERC GMD Task Force members, with final results being published in 2013. This joint effort will specifically examine transformer vulnerability and will take into consideration the two primary risks to reliability from GMDs: Reactive power loss and transformer hot spot heating. These two phenomena involve two very different time constants: Seconds for reactive power loss and potential voltage collapse, compared to several minutes for transformer heating.

NERC has supported the development of publicly-available simulation software to support this vulnerability assessment. Commercial software vendors are now leveraging this work to incorporate GMD studies into off-the-shelf tools. Transformer reactive power and thermal models are being validated to focus attention on the appropriate characteristics of the system. This information will be used to complete the high-level vulnerability assessment which can be used to further industry discussion on mitigation strategies. To complete the vulnerability assessment, NERC is working with the private sector and with Governmental agencies. For example, the NERC GMD Task Force is working with:

- Transformer vendors, to determine the thermal characteristics of hot spot heating due to geomagnetic-induced currents to identify the risk associated with specific transformer types;
- U.S. Geological Survey and Natural Resources Canada, to improve the ground impedance maps of North America, which will improve modeling of the electric fields that cause geomagnetically-induced currents;
- Interconnection modeling groups, to improve power system models so the effects of GMDs on and across grids can be simulated;
- NASA and the Canadian Space Agency, to develop a credible basis for GMD scenario development, which can differ based on geology and geomagnetic latitude, as well as develop the theoretical maximum GMD; and
- The North American Transmission Forum, to support review of confidential information on bulk power system and equipment performance, as well as, to support the vulnerability assessment.

To support these activities, over the next few months NERC will pursue an industry voluntary data request on the existing transformer fleet to gather the important transformer characteristics with respect to the risks to reliability. The data collected through this request would remain confidential and would be subject to NERC's Rules of Procedures regarding data confidentiality. If necessary, NERC can make a mandatory request for information under Section 1600 of its Rules of Procedure.

Further, in the next few months, the NERC GMD Task Force will review and update the existing NERC Alert on GMDs, to ensure that the guidance given reflects the most recent information.

2. Training of planners and operators

NERC will continue to educate industry on GMDs, work with industry to refine operator tools and procedures, and have industry consider actions such as preemptively increasing reserves, enabling forced cooling, or taking equipment out of service in advance of a GMD. As part of this transfer of knowledge, it will be vital that open-source models are developed to facilitate industry learning, study, and action. Further, NERC will also add GMD training as part of its existing Operator Certification program.

3. Spare equipment inventory management

The industry continues to demonstrate its commitment to reliability in the response to HILF events. One example is the development of programs to share spare equipment in the event of a severe event. NERC's Spare Equipment Database has been upgraded with specific focus on spare transformers. The Spare Equipment Database is a voluntary program whereby owners of long lead-time transformers would share information about their spare equipment to facilitate potential equipment sharing.

4. Development of improved transformer specifications to withstand GIC

As a result of NERC GMD Task Force activities, the IEEE Transformers committee has begun development on a guide on transformer and step response specifications to meet the service conditions related to a GMD, as well as, the magnitude and stress cycle due to geomagnetically-induced current that transformers should be designed to withstand. This project was initiated at the spring 2012 meeting of the IEEE Transformers Committee, and NERC will continue to collaborate with the

IEEE on the progress of this effort and provide technical expertise as warranted to its conclusion.

Over the next 12 months, the NERC GMD Task Force will continue working with experts from across the science and engineering spectrum to develop the tools and training necessary for the industry to incorporate GMD study and mitigation as regular planning and operating practice. Just as they prepare for earthquakes, hurricanes, and snowstorms, preparations for GMDs should be a part of the electric industry's on-going efforts in the future.

IMPORTANT ROLE FOR THE GOVERNMENT

From an operational perspective, more useful GMD forecasting is needed to support operator action. NOAA and SpaceWeather Canada need to enhance warning time frames and granularity of forecasts so industry can take the right action, in the most affected parts of North America. To ensure that the agencies can provide timely and detailed forecasts, it will be crucial that their efforts in satellite development and replacement, event simulation and prediction, and communications methods to the industry be maintained and enhanced.

CONCLUSION

Work is underway to address the recommendations for industry in the NERC Special Reliability Assessment Interim Report on GMDs. NERC and its stakeholders have made measureable progress toward mitigating the potential reliability impacts of GMDs, by characterizing the reliability issues and risk, gathering industry experts to focus on short- and long-term solutions, identifying spare equipment data for collection, assessing bulk power system resiliency through improved modeling, and alerting industry to potential actions they can take to fortify their systems from the risks posed.

NERC is addressing GMD in an open forum with a transparent process, leveraging the expertise of utility members, the scientific community, and equipment manufacturers, to guide the development of the necessary tools and training that will enable the industry to determine appropriate responses for its unique but interconnected systems. Substantial work remains to further the understanding of the impacts from GMDs, to continue improving the scientific methods used in its study, to demonstrate solutions, and to support the development as well as implementation of mitigation measures in a cost-effective manner.

STATEMENT OF NICKOLAUS E. LEGGETT, N3NL, ANALYST, AMATEUR RADIO OPERATOR, INVENTOR, U.S. CITIZEN

SEPTEMBER 12, 2012

My name is Nickolaus E. Leggett. I am an analyst, amateur radio operator, commercial radio operator, and an inventor who is resident in Reston, Virginia. I have been a Federally-licensed amateur radio operator since the 1960s. My amateur radio call sign is N3NL. I am a credentialed electronics technician (ISCET and iNARTE) and I am an inventor with three United States Patents—U.S. Patents 3,280,929, 3,280,930, and 6,771,935.

EXECUTIVE SUMMARY

My testimony discusses the need to develop protections from the effects of electromagnetic pulse (EMP) and solar geomagnetic storms. The first step is to get Governmental agencies to hold public hearings on EMP and suitable protections.

THE NATURE OF ELECTROMAGNETIC PULSE (EMP)

Electromagnetic pulse (EMP) is a serious threat to the continued existence of the United States as a major military, economic, and social power. Indeed, EMP is a major threat to the continued existence of the United States in any form.

High-altitude Electromagnetic Pulse (HEMP) is the generation of a very intense pulse of radio waves using a nuclear weapon or device exploded in space near the Earth. The radiation from the nuclear bomb excites and agitates the Earth's ionosphere which generates a large zone of intense radio waves that can disable electronic equipment and communications equipment throughout the Nation. Several years ago, the Congress commissioned a detailed study of EMP that can be accessed on-line. Refer to Note 1 at the end of this document.

CONSEQUENCES OF ELECTROMAGNETIC PULSE ATTACKS

A HEMP attack consisting of a single high-yield nuclear weapon exploded a couple of hundred miles above the United States would disable electronics and communications through most of the Nation. Most of our Nation's electronic infrastructure uses solid-state electronics and microprocessors that are quite vulnerable to electromagnetic pulse.

The failure of much of our electronics infrastructure would cause serious problems in supplying food, water, electric power, and communications to our population. In addition, the functions of business, government, and law enforcement would be greatly impaired. Panic, rioting, and the failure of law and order would probably occur.

LACK OF ACTION BY THE FEDERAL COMMUNICATIONS COMMISSION

I have devoted many years of my life to bringing the EMP threat to the attention of the Federal Communications Commission (FCC). Donald J. Schellhardt and I have submitted two formal petitions to the FCC calling for a Notice of Inquiry (NOI) and a Notice of Proposed Rule Making (NPRM) on EMP. Refer to Note 4. In addition, we have filed other formal comments with the Commission on this subject. The FCC has declined to take any positive action on EMP.

I am rather puzzled that the FCC refuses to act to protect our communications infrastructure from EMP. The subject is certainly interesting and it would be desirable to avoid the great damage that would result from any EMP attack. There is ample evidence that EMP is a real and serious threat to the Nation. Certainly, if an EMP attack did occur, the Nation would not be friendly towards the decision makers who refused to protect against EMP attacks and their consequences.

HOSTILE NATIONS

We can all easily imagine several nations that would be quite happy if the United States were to collapse in response to an EMP attack. In their view, EMP would be a rather convenient method for deleting a major competitor. While launching a missile with a warhead from a ship is not an easy task, it is certainly easier than other methods of eliminating the United States. Also, the structure of the United States may become so shattered by an attack that other nations could actually colonize parts of the former United States.

PROPOSED CONGRESSIONAL ACTIONS

The Congress should request or require the FCC to hold rulemaking hearings on electromagnetic pulse and effective methods to protect communications equipment from it. Probably some form of shielding should be required to protect critical communications equipment. Similarly, Congress could require the Federal Energy Regulatory Commission (FERC) to hold hearings on protecting the electric power industry and other energy industries from EMP effects. Similarly, the Federal Aviation Administration (FAA) should have hearings on EMP impacts on air navigation technology and on the operation of aircraft engines.

Also, the Congress can consider legislation that would require that critical infrastructure be shielded against EMP. In developing this legislation, the Congress can consult with the International Electrotechnical Commission (IEC) that has developed detailed standards on protection of infrastructure from EMP.

SOLAR GEOMAGNETIC STORMS

Congress also needs to examine the related natural phenomenon of solar geomagnetic storms. This natural phenomenon has a different physics from EMP but it is related. An intense solar storm can have a similar comprehensive effect that would result in the failure of the electric energy grid and other aspects of the infrastructure. Refer to Note 2. Federal agencies should be required to have hearings on solar geomagnetic storms.

AMATEUR RADIO

Amateur radio can perform local and long-distance communications during and after these chaotic events. Congress should establish legislation that would allow amateur radio operators to establish minimum-sized amateur radio antennas despite opposition of homeowner associations, condominium managements, and rental landlords.

OUR DUTY

It is in the Nation's interest that we all work to develop and apply effective protections against EMP attacks. Mr. Schellhardt and I have spent many years on this subject. Now Congress needs to move ahead constructively and deal with EMP threats.

APPENDIX A—REFERENCES ON SOLAR GEOMAGNETIC STORMS AND ELECTROMAGNETIC PULSE

Note 1

The text of the Congressional Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack is available at the web site: *www.empcommission.org*.

This document confirms the serious impact of an EMP attack on the infrastructure of the United States.

Note 2

Severe Space Weather Events—Understanding Societal and Economic Impacts—A Workshop Report, National Academy of Sciences, National Academies Press, Publication Year 2008, PAPERBACK, ISBN–10:0–309–12769–6, ISBN–13:978–0–309–12769–1.

This document can be accessed on-line at the URL: *http://www.nap.edu/catalog.php?record__id=12507*.

Note 3

H. Robert Schroeder, "Electromagnetic Pulse and Its Implications for EmComm", QST magazine, November 2009, pages 38 through 41. [The term EmComm refers to emergency communication.]

Note 4

Petitions to the Federal Communications Commission by Donald J. Schellhardt and Nickolaus E. Leggett:

Docket RM–5528, Request to Consider Requirements for Shielding and Bypassing Civilian Communications Systems from Electromagnetic Pulse (EMP) Effects.

Docket RM–10330, Amendment of the Commission's Rules to Shield Electronics Equipment Against Acts of War or Terrorism Involving Hostile Use of Electromagnetic Pulse (EMP).

Note 5

Daniel N. Baker and James L. Green, "The Perfect Solar Superstorm", Sky & Telescope, February 2011, Vol. 121 No. 2, Pages 28–34.

Note 6

Publications Dealing with the Protection of Civil Equipment and Systems from the Effects of HEMP and HPEM—Issued by the International Electrotechnical Commission (IEC) SC 77C.

Note 7

Mark Clayton, "Is US Ready for a 'Solar Tsunami'? "The Christian Science Monitor, June 27, 2011, Page 20.

Note 8

H.R. 668, Secure High-voltage Infrastructure for Electricity from Lethal Damage Act (SHIELD Act). This bill was introduced on February 11, 2011. This bill addresses the subjects of solar geomagnetic storms and electromagnetic pulse (EMP) impacting the electric power industry.

Mr. LUNGREN. We are pleased to have several panels of distinguished witnesses before us today. The sole witness of our first panel is Congressman Trent Franks. He represents Arizona's second Congressional district, serves on the Armed Services Committee and the Judiciary Committee, where he currently chairs the Constitutional Law Subcommittee. In addition, Congressman Franks serves as the co-chair of the Congressional EMP Caucus, and has studied this issue for several years.

The Chairman now recognizes Congressman Franks for his statement. As a witness, you know our routine here—5 minutes and your full written statement will be included in the record.

STATEMENT OF HON. TRENT FRANKS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ARIZONA

Mr. FRANKS. Well, thank you, Mr. Chairman. Good morning to you, sir. Good morning to Representative Clarke and the other Members of the committee. I am especially grateful to be here before you all.

Mr. Chairman, I would suggest to you that I am critically grateful to you for your knowledge and for your commitment to this issue. Your opening statement leaves little to add, but I will do my best.

The reality of the potential devastating effects of sufficiently intense electromagnetic pulse on the electronic systems and sources of many of our critical defense and National security components is well-established, Mr. Chairman.

As a Nation, we have spent billions of dollars over the years hardening our nuclear triad, our missile defense capabilities, and numerous other critical elements of our National security apparatus against the effects of electromagnetic pulse, particularly the type that might be generated by a high-altitude nuclear warhead detonation over our country by one of America's enemies.

However, our civilian grid, which the Defense Department relies upon for nearly 99 percent of its electricity needs, is completely vulnerable to the same kind of danger. This constitutes an invitation, in my opinion, on the part of certain enemies of the United States to use the asymmetric capability of EMP against us. There is now evidence that such strategies are being considered by certain of those enemies.

We recently witnessed, as you said, Mr. Chairman, the chaos that attends a prolonged power outage when the derecho storm impacted the District of Columbia and the surrounding area. Our sick and elderly suffered without air conditioning. Grocery stores were unable to keep food fresh. Gas lines grew. Thankfully, the derecho had only a regional and limited impact.

In 2004 and 2008, the EMP Commission testified before the Armed Services Committee, of which I am a member, that the U.S. society and economy are so critically dependent upon the availability of electricity that a significant collapse of our grid precipitated by a major natural or manmade EMP event could result in catastrophic civilian casualties. This conclusion is echoed by separate reports recently compiled by the DOD, DHS, DOE, NAS, along with various other agencies and independent researchers.

Now I am heartened, Mr. Chairman, by the efforts of DHS to address the vulnerabilities EMP poses to our grid, including the recovery transformer and resilient electric grid projects. However, while these projects are well-intentioned and a major positive step in the right direction, they do not go far enough to adequately protect our grid and our Nation against a catastrophic, continental-wide EMP event.

Our first priority should always be National security. To that end, I have introduced H.R. 668, the Shield Act, which among other

things, requires automated hardware-based solutions, rather than relying upon procedural safety measures alone to protect our Nation's major transformers from a cascading, destructive effect catalyzed by a major EMP event.

According to solar weather experts, there is only a 20- to 30-minute warning from the time we can actually predict a solar storm may affect us significantly to the time that it actually does. This is not enough time to implement procedures that will adequately protect the grid. Furthermore, these predictions are only accurate one out of three times. This places a crushing dilemma on industry who must decide whether or not to heed the warning with the knowledge that a wrong decision, either way, could result in the loss of thousands or even perhaps millions of lives and massive legal ramifications beyond expression.

Additionally, while there are those certainly who believe that the likelihood of terrorists or rogue nations obtaining nuclear weapons and using them in an EMP attack is remote, the recent events of the Arab Spring, which our intelligence apparatus did not foresee, show us that regimes can change very quickly. Iran's increasingly obvious efforts to gain nuclear weapons should serve as a grave and urgent warning to all of us.

Thankfully, Mr. Chairman and Members, there is a moment in the life of every problem, when it is big enough to be seen by reasonable people and still small enough to be solved or addressed. You and I live in that moment when there still may be time for the free world to address and mitigate the vulnerability that naturally occurring or weaponized EMP represents to the mechanisms of our civilization.

Your actions today to protect America may gain you no fame or fanfare in the annals of history. However, it may happen in your lifetime that natural, manmade, or other types of EMP may have an event so large and have an effect so small that no one but a few will recognize that was averted. For the sake of our children and future generations, I pray it happens exactly that way.

I thank you, Mr. Chairman. God bless you all for hearing this. I welcome Ms. Clarke. Thank you, sir.

[The statement of Mr. Franks follows:]

PREPARED STATEMENT OF HONORABLE TRENT FRANKS

Good morning Chairman Lungren, Ranking Member Clarke, and the rest of my fellow Members on the committee. I believe the subject of this hearing is one of profound implication and importance to Western civilization, and consequently I hope the Members will feel inclined to read my written testimony—and I thank you for allowing me to testify here today.

In our technological advancement, we have now captured the electron and transported its utility into nearly every business, home, and industrial endeavor throughout the civilized world. In so doing, we have advanced our standard of living and productivity beyond dreams. But we have also grown profoundly dependent upon electricity and its many accoutrements. In keeping with one of humanity's most reliable hallmarks, we now find among our greatest strengths an unsettling vulnerability . . . EMP . . . Electromagnetic Pulse.

Catalyzed by a major solar storm, a high-altitude nuclear blast, or a non-nuclear, device-induced Intentional Electromagnetic Interference, this invisible force of ionized particles has the capability to overwhelm and destroy our present electrical power grids and electrical equipment, including electronic communication networks, radio equipment, integrated circuits, and computers.

The reality of the potentially devastating effects of sufficiently intense electromagnetic pulse on the electronic systems/sources of many of our critical defense and

National security components is well-established, and beyond dispute. We as a Nation have spent billions of dollars over the years hardening our nuclear triad, our missile-defense capabilities, and numerous other critical elements of our National security apparatus against the effects of electromagnetic pulse, particularly the type of electromagnetic pulse that might be generated against us by an enemy. However, our civilian grid, which the Defense Department relies upon for nearly 99% of its electricity needs, is completely vulnerable to the same kind of danger. This constitutes an invitation on the part of certain enemies of the United States to use the asymmetric capability of an EMP weapon against us, and there is now evidence that such strategy is being considered by certain of those enemies.

The effects of geomagnetic storms and electromagnetic pulses on electric infrastructure are well-documented, with nearly every space weather and EMP expert recognizing the dramatic disruptions and cataclysmic collapses these pulses can bring to electric grids. We all recently witnessed the chaos that ensues a prolonged power outage when the derecho storm impacted the District of Columbia. Sick and elderly suffered without air conditioning, grocery stores labored to keep food fresh, and gas lines grew. Thankfully, the derecho was only regional in its impact and limited in its effects.

In 2004 and 2008 the EMP Commission testified before The Armed Services Committee, of which I am a member, that the U.S. society and economy are so critically dependent upon the availability of electricity that a significant collapse of the grid, precipitated by a major natural or man-made EMP event, could result in catastrophic civilian casualties. This conclusion is echoed by separate reports recently compiled by the DOD, DHS, DOE, NAS, along with various other Government agencies and independent researchers. All came to very similar conclusions. The sobering reality is that this vulnerability, if left unaddressed, could have grave, societal-altering consequences.

I am heartened by the efforts of DHS to address the vulnerabilities EMP poses to our grid, including the Recovery Transformer and Resilient Electric Grid Projects. However, while these projects are well-intentioned and a positive step forward, they do not go far enough to adequately protect our grid and our Nation against a catastrophic, continental-wide EMP event.

Like many of you, I believe Federal regulation should be very limited. Our first National security priority in this instance is to protect our major transformers from cascading destruction. To that end, I have introduced the SHIELD Act which, among other things, requires automated hardware-based solutions rather than procedural safety measures alone. And the SHIELD Act does not contain cybersecurity provisions, leaving the conflicting approaches to that extremely important issue, among members of the Senate in particular, to be debated in a separate bill.

Automated hardware is particularly important when one considers the shortcomings of procedural safety measures alone in response to an EMP event. According to solar weather experts, there is only 20–30 minutes' warning from the time we predict a solar storm may affect us to the time it actually does. This is simply not enough time to implement procedures that will adequately protect the grid. Furthermore, these predictions are only accurate one out of three times. This places a crushing dilemma on industry, who must decide whether or not to heed the warning with the knowledge that a wrong decision either way could result in the loss of thousands or even millions of lives and massive legal ramifications beyond expression.

Mr. Chairman, the phenomenon of natural and man-made electromagnetic pulse is not a new one.

In 1859, English Astronomer Richard Carrington discovered the cause of natural EMP when he identified and chronicled a major geomagnetic solar storm which brilliantly intensified the Northern lights and caused the telegraph system, the only major electrical system that existed on earth at that time, to go down across the planet. The National Academy of Sciences predicts this effect, to a lesser or greater degree, will recur globally approximately once every 100 years.

In 1962, the United States discovered that a high-altitude nuclear blast could generate a more localized electromagnetic pulse of the same intensity as the Carrington effect. In an upper atmospheric nuclear test called Starfish Prime, an EMP occurred and electric lines were fused and radios and street lights stopped working in Hawaii nearly 900 miles away. The residual effects also disabled nearly all major satellites systems.

Because of new understandings of how EMP interacts with the Earth's electromagnetic field, and that it is intensified over large land mass, we now believe that if a warhead with a nuclear yield of just 100 kilotons detonated at an altitude of 400 kilometers over America's heartland, the resulting damage to our electric grid and infrastructure would be catastrophic across most of the continental United

States. Such a result would be devastating to our electricity, transportation, water and food supply, medical care, financial networks, telecommunication and broadcasting systems and our infrastructure in general. Under such a scenario, both military and productive capability would be devastated. The immediate and eventual impact, directly and indirectly, on the human population, especially in major cities, is unthinkable.

It should be remembered that EMP was first considered as a military weapon during the "Cold War" as a means of paralyzing U.S. retaliatory forces.

America's EMP commission began their 70-page executive summary describing a one- or two-missile EMP attack as one of the few threats which look as if it could defeat the U.S. military.

Dr. William Graham, the chairman of the EMP Commission, testified before the U.S. House Armed Services Committee, and stated:

"EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences.

" . . . A determined adversary can achieve an EMP attack capability without having a high level of sophistication. For example, an adversary would not have to have long-range ballistic missiles to conduct an EMP attack against the United States. Such an attack could be launched from a freighter off the U.S. coast using a short- or medium-range missile to loft a nuclear warhead to high altitude. Terrorists sponsored by a rogue state could potentially execute such an attack without revealing their identity."

Dr. Graham has said that a major catastrophic EMP attack on the United States could cause an estimated 70–90 percent of the our Nation's population to become unsustainable.

It is impossible for me to even wrap my mind around that figure.

But for terrorists, this is their ultimate goal, and I believe EMP is their ultimate asymmetric weapon. In 1988, Osama bin Laden called it a religious duty for al-Qaeda to acquire nuclear weapons. U.S. Admiral Mike Mullen, the chairman of the Joint Chiefs of Staff, has stated: "My worst nightmare is terrorists with nuclear weapons. Not only do I know they are trying to get them, but I know they will use them."

This is indeed the greatest danger of all. If a rogue state like Iran steps over the nuclear threshold, rogue regimes and terrorists the world over will have access to these monstrous weapons.

We do well to remember that Iran, the world's leading sponsor of international terrorism, has practiced launching a mobile ballistic missile from a vessel in the Caspian Sea. Iran has also tested high-altitude explosions of the Shahab–III, a test mode consistent with an EMP attack, and described the tests as successful. We have also discovered an Iranian military journal that included an article recommending such a strategy. The article noted that if major Western nations do not learn to defend themselves against EMP attacks, they will be destroyed.

Mahmoud Ahmadinejad again made it clear where he stands on Israel when he declared, "[Israel] is about to die and will soon be erased from the geographical scene."

Jewish author, Primo Levi, was once asked what he had learned from the Holocaust. He replied, "When a man with a gun says he's going to kill you—believe him."

At this moment, Iranian President Mahmoud Ahmadinejad, a man who, in the same breath, both denies the Holocaust ever occurred, and then threatens to make it happen again, is arrogantly seeking a gun with which he vows to wipe the state of Israel off the map.

He has also said: "The time for the fall of the satanic power of the United States has come and the countdown to the annihilation of the emperor of power and wealth has started." He has said point-blank, "The wave of the Islamist revolution will soon reach the entire world."

What a happy cheerful, fellow . . .

Unfortunately, he talks like a man who knows something the rest of us don't.

It is not enough, to casually dismiss his fanatical rhetoric. When analyzing the nature of any threat, we must always seriously assess two things: A potential enemy's intent and his corresponding capacity to carry out any such intent.

Mahmoud Ahmadinejad and his regime have stated very clearly their intent to see Israel wiped off the face of the earth and America and the West brought to their knees. Nuclear warheads could give them the capacity to effectively proceed in that endeavor; and to ignore the incontrovertible fact that Iran is rapidly progressing toward a nuclear weapons capability, is to resign ourselves and our children to live and walk in the shadow of nuclear terrorism.

Mr. Chairman and Members, these things should not surprise us. We are now 65 years into the nuclear age, and the ominous intersection of jihadist terrorism and nuclear proliferation has been inexorably and relentlessly rolling toward America and the free world for decades. But, when we add the dimension of asymmetric electromagnetic pulse attacks to that equation, we face a menace that may represent the gravest short-term threat to the peace and security of the human family in the world today.

Certainly there are those who believe that the likelihood of terrorists or rogue states obtaining nuclear weapons and using them in an EMP attack is remote. It may be a reasonable conclusion for the moment. But the recent events of the Arab Spring, which our intelligence apparatus did not foresee, show us that regimes can change very quickly. Is a regime change in Pakistan possible? Will there be blowback from our involvement in Libya? What about the current crisis in Syria? Will North Korea ever supply or sell it nuclear technology or warheads to terrorists? Will Iran develop or obtain nuclear weapons? Iran's increasingly obvious efforts to gain nuclear weapons should serve as a grave and urgent warning to all of us.

If terrorists or rogue states do acquire nuclear weapons, hardening our electric grid would become a desperate priority for our Nation. However, that process will take several years, while a regime change takes only weeks and a missile launch only minutes. The fact that we are now 100% vulnerable means we should start securing our electric infrastructure now. Indeed, by reducing our vulnerability we may reduce the likelihood that terrorists or rogue states would attempt such an attack.

We should always remember that 7 decades ago, another murderous ideology arose in the world. The dark shadow of the Nazi swastika fell first upon the Jewish people of Germany. And because the world did not heed the warnings of men like Winston Churchill and respond to that evil in time, it began to spread across Europe until it lit the fires of World War II's hell on earth which saw atomic bombs fall upon cities and over 50 million people dead worldwide.

History has repeatedly shown humanity to be susceptible to malignant dangers that approach inaudibly and nestle among us with innocuous countenance until a day of sudden calamity finds us empty-handed, broken-hearted, and without excuse.

Thankfully, Mr. Chairman and Members, there is a moment in the life of nearly every problem when it is big enough to be seen by reasonable people and still small enough to be solved. You and I live in that moment when there still may be time for the free world to address and mitigate the vulnerability that naturally occurring or weaponized EMP represents to the mechanisms of our civilization.

The challenge to ultimately and fully protect our peoples and nations from all of the various perils of natural or man-made electromagnetic pulse will be long and lingering. But the time to protect our Nation from the most devastating scenario is now; the threat is real, and the implications are sobering.

America's Brink Lindsey said it it this way: "Here is the grim truth: We are only one act of madness away from a social cataclysm unlike anything our country has ever known. After a handful of such acts, who knows what kind of civilizational breakdown might be in store?"

Mr. Chairman and Members of the committee, the first purpose of any government or its leaders is to protect the lives and security of its innocent citizens. The failure of this responsibility renders all others meaningless.

Your actions today to protect America may gain you no fame or fanfare in the annals of history. However, it may happen in your lifetime that a natural or man-made EMP event so big has an effect so small that no one but a few will recognize the disaster that was averted. For the sake of our children and future generations, I pray it happens exactly that way.

Thank you and God bless all of you.

Mr. LUNGREN. Thank you very much, Congressman Franks. I appreciate the leadership that you have shown in this particular area.

There are some that have suggested that EMP attack or an EMP event, if naturally caused, is not that serious—that there is sort of an alarmist tone to statements to the public that this is an issue about which they should be concerned. How do you respond to that?

Mr. FRANKS. Well, first, in the sincerest way that I can express to you, I pray they are correct. I hope that there is just some overreaction on the part of all of us. But I will say to you, if that is

true, then your seminal point made earlier that the military is spending a great deal of unnecessary money hardening our military apparatus should be considered carefully.

There is no question about the reality of the effects of EMP if there is a sufficient surge. We have got a great deal of research in that regard and to ignore that would be to ignore some of the major reports not only by the EMP Commission, but the Department of Defense. There are somewhere between six and nine major reports now in Government—and I will certainly refer you to the experts that will follow me that testify clearly to the danger.

The challenge before us is to ascertain exactly what that danger is. We suggest to you that we don't know fully what it is. But something that has the potential to have this kind of catastrophic effect should be considered carefully.

Mr. LUNGREN. Where is the failure? Is the failure with the Congress? Is the failure with the Executive branch? Is the failure with critical infrastructure owners? If this is as serious as you suggest, as some of these reports suggest, the lack of attention to it is something that bewilders me.

I mean you have been involved in a lot of issues on the Armed Services Committee and so forth, and I am trying to figure out what is it that is lacking on this issue that does not garner the attention of the American people? In other words, is there a lack of consensus about the threat? I mean is there a serious question that—from your standpoint—is there a serious question about whether this is a serious issue?

Mr. FRANKS. No, I think, Mr. Chairman, that is probably the most important question that we have to ask. I would only suggest to you that when the EMP Commission came to the Armed Services Committee in 2004, I had been aware of EMP. My background is engineering. I had been aware of it, but I thought it was like something that could be catastrophic, but the chances of it happening were so remote. I just didn't see that happening.

The testimony was that other nations—there were five nations at the time that were developing this as an offensive capability. Certainly, the Soviet Union had a major EMP component in their nuclear strategy.

So there is a dichotomy here that I don't exactly understand in the military, among our National security experts, there is clear consensus of the danger this represents. However, when you go over into the civilian areas, it seemed like there is a general, sort of a lackadaisical, kind of a——

Mr. LUNGREN. Let me ask you about that, because I have found most people who are involved in critical infrastructure in the private sector are serious-minded folks. They do recognize the value of their assets. In most cases, when I am dealing with them on issues, I find them to be forward-thinking and to actually try and protect those assets. They articulate that in a way so that they can justify certain capital investments to their shareholders or their ratepayers.

Well, let me ask you this: Do you find the attention to the protection of their assets that you believe to be necessary, and if not, why as the owners and protectors of those assets, is this not taken more seriously?

Mr. FRANKS. I think that is a good question. It has been something that has bewildered me to a degree. It seemed just a few years ago, as this became more well known that there was a more serious—or at least a more recognizable response. It seemed like in the recent just past last year, there has been sort of a pushback in parts of industry.

My concern is if they have credible, scientific bases for being unconcerned or not addressing it as vigorously as some of us think that it should be, then I would adjure them to bring that testimony and that evidence to the rest of us. Because I can suggest to you that I haven't seen it.

It may be that there is some concern on the part of major manufacturers of these large components, transformers and others, that are somewhat out of professional pride. That they either don't want to recognize the danger or somehow they feel like that there would be some requirement of reengineering of some of these major components if they did.

But I would suggest that the potential liability here is off the charts. The fix here—and this would probably be one of the more important points to point out—the fix here is fairly simple, at least in terms of protecting our electric-producing grid—not all the elements that are connected to it. That is a huge issue. But at least to be able to keep the lights on—electricity coming—that is a fairly easy fix. I think this country needs to look at it.

Mr. LUNGREN. Thank you very much.

I recognize the Ranking Member Ms. Clarke for 5 minutes.

Ms. CLARKE. Let me thank you, Mr. Chairman.

Thank you, Mr. Franks, for your testimony before our subcommittee today. I know how passionate you are about this. We share that passion. You are helping to write the road map for addressing the EMP threat speaks to your commitment.

I wanted to also welcome Dr. Beck, who as a former staffer, a staff director for this subcommittee and has also developed an expertise on this matter. So I want to welcome you back, Dr. Beck.

I believe it is important that we find the building blocks for the partnership of which Councilman, excuse me, Congressman Franks has articulated this morning. We must bring improvements to the security and reliability of one of our most important critical infrastructures, our electric grid.

I understand that our very reliance on the infrastructure that makes it important to anticipate the worst. There are many scenarios that we should be concerned about. We are still learning about the significant threat that could come in the form of a natural or manmade electromagnetic pulse and have more to learn about the effects of the EMP and geomagnetic disturbances to the grid as well.

Over the past few years, I have followed with interest, Mr. Chairman, the secure grid exercises that the National Defense University has held at Fort McNair. These series of tabletop exercises in the U.S. electric grid security have focused on the effects of a major geomagnetic storm on the Nation's electrical infrastructure. With the 12-year peak in solar activity approaching in 2012–2013, there is considerable upturn in interest from Government agencies,

including the White House and Congress in understanding the potential impacts if a geomagnetic disturbance event should occur.

Although this is a low-probability event, the consequences of an extended and widespread power loss across portions of the country would constitute a serious National emergency. To me, one of the largest barriers to Government agency disaster response is cross-agency coordination, the role of authority—crucial elements made more difficult when discussing privately-owned National electric grid. Ultimately, the secure grid exercises and other policy discussions work to identify preparedness gaps in plans to manage the challenges associated with extended power outages and add urgency to existing efforts to identify technology solutions to protect the U.S. grid.

This hearing serves to highlight areas where the United States and its allies are analyzing the risk that a severe geomagnetic disturbance would present, and help us look for international approaches to effectively react to those risks. While severe solar storms that create geomagnetic disturbances cannot be prevented, there are tools and opportunities to mitigate and protect the grid from such risks of such an event.

My colleagues on the Homeland Security Committee and I have spent nearly 3 years identifying and reviewing security protections that are in place to mitigate the effects 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 extensive discussions and review with the private sector, which owns, operates, and secures the grid. The private sector develops its own security standards and also oversees compliance with these standards. In short, the private sector has the responsibility, as has been stated by Congressman Franks, for securing the grid from electromagnetic events and cyber attacks.

I am very pleased to see the statement for the record submitted by the North American Reliability Corporation. These are the folks who are the closest to the electric grid and they manage an almost impossibly complex flow of energy, not just our 330-plus million people, but also the flow of energy across our borders every day.

Finally, the U.S. Congress has acted. In June 2010, the Grid Act passed the House of Representatives unanimously. Unfortunately, it stalled in the Senate and did not become law. The bill would have granted the Federal Energy Regulatory Commission expanded authorities to oversee electromagnetic and cyber protections.

This Congress, Congressman Franks, has introduced the version of the bill now called the Shield Act, which is similar to the Grid Act, but focuses only on the electromagnetic threat component, without the cybersecurity component. I am a cosponsor of the bill. It is our hope that during the next Congress, we will get this bill through both houses and to the President's desk.

So I just wanted to put that on the record. Thank you, again, Congressman Franks, for your vigilance. I think this is a very crucial concern. As we look at the modernity of our civil society, we must be concerned about unintended consequences from what may be solar, geomagnetic, or intentional threat to our electric grid.

I yield back, Mr. Chairman.

Mr. FRANKS. Mr. Chairman, if I could just respond to—Ms. Clarke has demonstrated tremendous commitment in this area and has done some amazing things. I appreciate her work so much.

I would just leave the committee with this thought. As we have challenged those who don't think or are not significantly convinced that this is a threat, weigh on one hand the money that we spend in the military to defend against this threat and all of the reports that are ubiquitous throughout our Government. On the other hand, let us ask the industry to show us why this is not a threat.

We, as a human family, have been historically, you know, clear back in the days of London, when 90 percent of London burned, we knew about fire then, but somehow we just kind of didn't respond to it until something critically significant happened.

So I would encourage the committee, just get the facts. Because if it is not a problem, then we can all go home. It is——

Mr. LUNGREN. Mr. Long, do you have any questions for our witness?

Mr. LONG. Thank you, Mr. Chairman.

Congressman Franks, the solar flare you spoke about earlier—you said solar flares—if I remember what you said right—sometimes you will have 20–30 minutes' notice before solar flare with an accuracy rating of one out of three times, I think you said.

Mr. FRANKS. Go ahead, please.

Mr. LONG. Go ahead.

Mr. FRANKS. Uh, let me try to expand that a little bit. We have satellites that give us some indication much sooner than that, about 24 hours in advance sometimes that there is a major geo—like a CME, which is a chrome mass ejection or it is an effective solar flare—that creates a geomagnetic disturbance, which is inevitable. It happens about every 100–105 years, sometimes even more frequently. But the major ones are called the Carrington Effect, which was named after a gentleman that discovered or essentially documented the first major clear demonstration of that type of solar storm.

We have in this society about 24 hours to say, okay, we have one coming. But we don't know if it is going to be severe enough to do any damage until about 30 minutes out. Now the problem is, even then, when we say, okay, we have 30 minutes and this looks like one that could really be serious. It looks like our earth polarity—is just right. All of that, as it were, the stars are lining up and this could be really bad. But even then, only one out of three times is that correct.

So as an operator, do you shut down the grid to protect it and take a chance on risking human life, or do you leave it up and take a chance on it being damaged and risk even more human life?

Mr. LONG. My question was the 20- to 30-minute warning, what could be done in that 20–30 minutes. You say shutting it down, I suppose. But what if we had 20–30 days or 20–30 months for that warning? Let us pretend we had 20–30 months. What steps can be taken to mitigate this? Are there things that can be done?

You gotta keep in mind that most of these—a lot of the infrastructure is privately held, so has there been studies to show what will mitigate this? Are there things—back on the farm, every house

had a lightning rod on it to mitigate the lightning to keep it from burning the house down. Are there things to mitigate this if we had the sufficient amount of time?

Mr. FRANKS. You know, you point out probably the perfect example and that is lightning—that lightning is a type of EMP—it is E2. The lightning rods redirected the force or the rush of electric energy into the ground, where it wouldn't damage anything. There are what we call nuclear phase blockers that can go before these major transformers that would interrupt the electric flow. If there was a surge, that it would happen instantaneously. If there was a surge, it would keep these transformers from burning themselves up. That is one way to mitigate it.

Mr. LONG. When you say can go before it, what do you mean?

Mr. FRANKS. These neutral face blockers are, prior to any charge going into the transformer, coming out of it——

Mr. LONG. So this is hardware that is actually hard laid.

Mr. FRANKS. That is correct.

Mr. LONG. Okay, that is what I——

Mr. FRANKS. That means if there is no electromagnetic pulse, then no one has to shut something down just in case. But if there is, then it automatically says no, we are going to interrupt the flow to that transformer so that it won't add to its load that would ultimately cause it to burn up. If it does, those transformers are difficult to replace.

The challenge, of course, as far as having sufficient warning, is that we would have to be able to predict when there is a major solar flare—major coronal mass ejection. We haven't really found the science to do that yet. So even——

Mr. LONG. Well, if you had it installed ahead of time, you wouldn't need to predict, right?

Mr. FRANKS. Correct. Correct. But I am saying right now, if you base it on procedures alone, where you tell the operators there is a big one coming. Shut down manually. At best, they are going to have 24 hours general warning. Again, more often, a 30-minute warning is just not enough time.

Mr. LONG. Is the effect the same whether it is an act of God, whether it is a solar flare or solar storm that you called the other one.

Mr. FRANKS. Well, the act of God as it were——

Mr. LONG. Well, yes, but my question is, is it the act of God, solar storm, solar flare—is the ramification the same as a man-made act, such as the high-altitude electromagnetic pulse that a nuclear device set off at 100 kilometers above the earth would?

Mr. FRANKS. It is a little bit technical, but I will answer your question. The solar storm or the geomagnetic disturbance is primarily E3. It is a slower and it is more damaging to transformers and the heavy equipment and things of that nature. Whereas, it doesn't have the E1 and E2.

Whereas, the lightning—I mean, excuse me—the nuclear-generated electromagnetic pulse, where a nuclear warhead creates a gamma ray emission which interacts with the atmosphere and creates a rush of ionized particles toward the earth, it happens to create all three—E1, E2, and E3. So it can damage electrical components of, you know, small transistors, scatter control systems—

these very delicate systems that are sort of the hallmark of our, you know, our electronic advancement in this society.

So the answer—the effect is, with a nuclear generated EMP, the effect is—covers a lot more electronic components. But with the geomagnetic——

Mr. LONG. Is the fix the same?

Mr. FRANKS. What is that?

Mr. LONG. Is the fix the same? You said earlier that the fix is simple. Is the fix the same on either——

Mr. FRANKS. Yes, if the components that are destroyed—the fix is the same, but the GMD affects mostly——

Mr. LONG. I am talking about the prevention fix, I guess, not—maybe I misunderstood what you meant by fix.

Mr. FRANKS. Yes, the only thing that the Shield Act—well, I won't say the only thing—but the primary thing that the Shield Act addresses is to make sure that our major transformers are 750 KV corridor are not destroyed, which means that we would be in a catastrophic civilizational challenge where we wouldn't have electricity and wouldn't be able to perhaps restore it for months or even years. That is the worst-case scenario. The Shield is designed to prevent that.

Some of these ancillary damages on cell phones, radios, things like that, it is difficult to mitigate against that in a short-term fix. We have to harden as we go. But my contention is if we take those components as we rebuild them and replace them and harden them against EMP, which we can do that. It adds about 10 percent to the cost of doing that. Then we can eventually get past this vulnerability. But the main big vulnerability that we have right now is the potential damage to our major transformers that could be caused by either a high-altitude electromagnetic pulse or GMD.

Mr. LUNGREN. Time.

Mr. LONG. But that is preventable. I am way past my time. I yield back.

Mr. LUNGREN. Well, if you are way past your time, how can you yield back?

[Laughter.]

Mr. LUNGREN. The gentlelady from California is recognized for approximately 5 minutes.

Ms. RICHARDSON. Thank you, Mr. Chairman. I have no questions for the Congressman. Thank you for your testimony.

Mr. LUNGREN. Mr. Richmond.

Mr. RICHMOND. I don't have many, but the thing that I guess just draws my attention is the Congressman's conversation about the solar storm. I know that it is termed a 1-in-100-year event. But I am from New Orleans, where we get 1-in-100-year events. So I would like to be——

Just your feeling in your opinion, as someone who has really taken the lead on this—I mean, how prepared are we for that 1-in-100-year event right now? What things can we do quickly or what do we need to put in place so that we start developing either criteria, building codes, or codes for or standards for the utility companies to make sure that we don't have the potential to have people out of power for years?

Mr. FRANKS. Well, let me try if I could to address the worst-case scenario, which I consider openly to be remote. But it is possible. It is that 100-year event you talk about.

On the military side, in terms of our National security, being able to fight back, as it were, our major military apparatus is hardened effectively and we are prepared. The problem is on the civilian side, we are almost completely unprepared. It is just an incredible antithesis here. Our military is critically dependent upon the civilian grid for its electricity needs—about 99 percent—and is, according to military sources, their own military mission becomes compromised without that source of electricity.

So our focus needs to—you know, our missile defense systems are able actually to fight through a major EMP environment. It can have major electromagnetic pulse energy everywhere and they are able to fight through it, because they understand that that is exactly the type of environment they would be in, in terms of a nuclear war.

But the civilian grid right now remains unprotected. In the conferences that Ms. Yvette Clarke and I have attended on occasion, the Defense Department has testified that they are in a sort of a no-win situation, because they depend on the electric grid, but they have no control over how it should be protected. I am fine with that.

The Shield Act allows the private sector to come up with the best solution; and if that is good enough, great. I am the last one that wants to regulate any industry, but I am the first one that wants to pay attention to our National security. If we have standards that says we must mitigate or protect against this, which we can do at minimal costs—the neutral face blockers that I had mentioned to the other gentlemen actually allow the grid to be run at a higher capacity, which more than pays for what is a relatively minimal cost. I mean, it is in the noise of the cost of our daily generation costs.

So the bottom line is, we are not prepared in our civilian grid. We are very prepared to be able to continue to fight a war. But I wonder at some point if we have a significant enough impact, how much, you know, are we really protecting the country.

Finally, I would just say that, you know, the worst-case scenario is so bad that rather than preparing for it, we must prevent it from ever occurring.

Thank you. I yield back.

Mr. LUNGREN. The gentleman yields back. Thank you, Congressman Franks, for your testimony and for your leadership on this issue. We appreciate it very much.

Mr. FRANKS. Thank you. Thank all of you.

Mr. LUNGREN. They have it written for me to say, Panel 1 is dismissed. You are Panel 1.

Mr. FRANKS. All right. Thank you, sir. Thank you all very much.

Mr. LUNGREN. Thank you. Now, I would ask the clerks to prepare for our second panel.

We have a very distinguished second panel. I thank you all for being here.

Mr. Joseph McClelland is the director of the Office of Electric Reliability at the Federal Energy Regulatory Commission, a position

to which he was first appointed in September 2007. Mr. McClelland came to the Commission with more than 20 years of experience in the electric utility industry, holds a Bachelor of Science degree in electrical engineering from Penn State.

Mr. Brandon Wales is the director of the Homeland Infrastructure Threat and Risk Analysis Center at the Department of Homeland Security. In this role, he leads a robust all-hazards analytic resource for public and private-sector partners, covering the full array of risks and challenges facing the infrastructure community. Prior to joining the Department, Mr. Wales served as the principle National security advisor to the United States Senator Jon Kyl and was a senior associate at the Washington-based foreign policy and National security think tank.

Mr. Michael Aimone is director of Business Enterprise Integration on Intergovernmental Personnel Assignment—Personal Assignment in the Office of the Secretary of Defense's Installations and Environment Directorate. That is a long term. We will just say you are an expert. How is that?

Mr. Aimone oversees the efforts by the deputy under secretary to modernize and integrate real property, energy, and environmental business information technology systems for the Department of Defense. Mr. Aimone serves as the U.S. Air Force and in the U.S. Air Force and the U.S. Air Force Reserves for nearly 30 years, and is widely known as one of the country's industry leaders on energy, security, and sustainable operations.

We thank you for all being here. Your written submissions are made a part of the record. We would ask you to attempt to summarize your testimony within 5 minutes after which time we will have the panel subjected to questions by our Members of the subcommittee. So if you would go in the order in which I have introduced you.

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

Mr. MCCLELLAND. Good morning, Mr. Chairman, Ranking Member, and Members of the subcommittee. Thank you for the privilege to appear before you today to discuss the security of the power grid. My name is Joe McClelland. I am the director of the Office of Electric Reliability at the Federal Energy Regulatory Commission. I am here today as a Commission staff witness. 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 bulk power system. This authority is in section 215 of the Federal Power Act. It is important to note that FERC's jurisdiction and reliability authority under section 15 is limited to, "the bulk power system," as defined in the FPA, which excludes Alaska and Hawaii, as well as the local distribution systems. Under this section 215 authority, FERC cannot author or modify reliability standards. We must depend upon an electrical reliability organization or ERO to perform this task. The Commission selected the North American Electric Reliability

Corporation, or NERC, as the ERO. The ERO develops and proposes reliability standards or modifications for the Commission's review, which it can then either remand or approve.

If the commissioner approves the proposed reliability standard, it becomes mandatory enforceable in the United States, applying to the users, owners, and operators of the bulk power system. If the Commission remands a proposed standard, it is sent back to the ERO for further consideration.

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 grids stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as tree trimming and equipment maintenance practices. Widespread disruption of electric service can quickly undermine the United States Government, its military, and the economy, as well as endanger the health and safety of millions of its 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.

While the Commission is considering actions that it can take under its current authority, this authority may not be sufficient in cases where mandatory action is needed to protect the United States from physical threats that endanger our Nation's security.

One example of a physical threat is an electromagnetic pulse, or EMP, event. EMP events can be generated from either a naturally occurring or manmade causes. In 2001, Congress established a commission to assess the threat from EMP. In 2004, and again in 2008, the Commission issued its reports. Among the findings in the reports, was 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 order to better understand and quantify the effect of EMP on the power grid, FERC staff, the Department of Energy, and the Department of Homeland Security sponsored a study by the Oak Ridge National Laboratory and their subcontractor Metatech in 2010. The results of this study support the general conclusion of prior studies that EMP events pose substantial risk to equipment and operation of the Nation's power grid, and under extreme conditions, could result in major long-term electrical outages.

In fact, solar magnetic disturbances are inevitable, with only the timing and magnitude subject to variability. The study assessed the 1921 solar storm, which has been termed a 1-in-100-year event and applied it to today's power grid. The study concluded that such a storm could damage or destroy in excess of 300 bulk power system transformers, interrupting service to 130 million people, with some outages lasting for a period of years.

In February 2012, the North American Electric Reliability Corporation released its interim report, "Effects of Geomagnetic Disturbances on the Bulk Power System." In it, they concluded that

the most likely worst-case scenario system impact from a severe geomagnetic disturbance is voltage instability and voltage collapse, with limited equipment damage and recovery times measured in hours or days.

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

The Commission is considering the comments filed after the conference and what actions it can take under its current authority to address National security threats to the reliability of our power system from EMP. Although the Commission's current authority allows it to require submission to the ERO of proposed standards to address the EMP threat to the United States, it does not allow the Commission the ability to author the standards, thereby limiting its effectiveness. These types of threats pose an increasing risk to the power grid that serves our Nation. The Commission is therefore considering actions that it can take under its current authority.

Any new legislation should address several key concerns, including allowing the Federal Government to take action before a cyber or physical National security incident has occurred, ensuring appropriate confidentiality of sensitive information developed under new authority, and allowing cost recovery for entities that mitigate vulnerabilities and threats.

Thank you, again, for the opportunity to testify today. I would be happy to answer any questions that you might have.

[The prepared statement of Mr. McClelland follows:]

PREPARED STATEMENT OF JOSEPH MCCLELLAND

SEPTEMBER 12, 2012

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

The Commission is committed to protecting the reliability of the Nation's bulk electric system. The Commission is considering actions that it can take under its current authority to address National security threats to the reliability of our transmission and power system from electromagnetic pulses. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our Government and economy and helps ensure the health and welfare of our citizens. I will describe how limitations in Federal authority may not fully protect the grid against security threats due to electromagnetic pulse and summarize the Commission's oversight of the electric grid under section 215 of the Federal Power Act.

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 modifica-

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

THE NERC PROCESS

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

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

The procedures used by NERC are appropriate for developing and approving routine reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process can be a strength of the process. However, it can be an impediment when measures or actions need to be taken to address threats to National security quickly, effectively, and in a manner that protects against the disclosure of security-sensitive information. The current procedures used under section 215 for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent 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 to develop a new or modified Reliability Standard using an expedited reliability standard development process 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 expedited process. In the mean time, the bulk power system would be left vulnerable to a known National security threat. Moreover, existing procedures, including the expedited action procedure, could widely publicize both the vulnerability and the proposed solution, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

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

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

PHYSICAL SECURITY AND OTHER THREATS TO RELIABILITY

The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks. While the Commission is considering actions that it can take under its current authority, this authority may not be sufficient in cases where quick mandatory action is needed to protect the United States from the EMP threat or other National security threats to the reliability of our transmission and power system. The Federal Government should have no less ability to act to protect against potential damage from physical threats to the grid than from cyber attacks.

One example of a physical threat is an electromagnetic pulse (EMP) event. EMP events can be generated from either naturally-occurring or man-made causes. In the case of the former, solar magnetic disturbances periodically disrupt the earth's magnetic field which in turn, can generate large induced ground currents on the electric grid. This effect, also termed the "E3" component of an EMP, can simultaneously damage or destroy bulk power system transformers over a large geographic area. Regarding man-made events, EMP can also be generated by weapons. Equipment and plans are readily available that have the capability to generate high-energy bursts, termed "E1", that can damage or destroy electronics such as those found in control and communication systems on the power grid. These devices can be portable and effective, facilitating simultaneous coordinated attacks, and can be reused, allowing use against multiple targets. The most comprehensive man-made EMP threat is from a high-altitude nuclear explosion. It would affect an area defined by the "line-of-sight" from the point of detonation. The higher the detonation the larger the area affected, and the more powerful the explosion the stronger the EMP emitted. The first component of the resulting pulse E1 occurs within a fraction of a second and can destroy control and communication electronics. The second component is termed "E2" and is similar to lightning, which is well-known and mitigated by industry. Toward the end of an EMP event, the third element, E3, occurs. This causes the same effect as solar magnetic disturbances. It can damage or destroy power transformers connected to long transmission lines and cause voltage problems and instability on the electric grid, which can lead to wide-area blackouts. It is important to note that effective mitigation against solar magnetic disturbances and non-nuclear EMP weaponry provides effective mitigation against a high-altitude nuclear explosion.

In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure. In 2004, the EMP commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.[2] The reports concluded that both electrical equipment and control systems can be damaged by EMP. The reports also pointed out how the interdependencies among the various infrastructures could become vulnerabilities after an EMP. In particular, they point to the electrical infrastructure's need of the communication and natural gas infrastructures.

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

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

In February 2012, NERC released its Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System. In it, NERC concluded that the most likely worst-case system impact from a severe geomagnetic disturbance is voltage instability and voltage collapse with limited equipment damage.

On April 30, 2012, the Commission held a technical conference to discuss issues related to reliability of the bulk power system as affected by geomagnetic disturbances. The conference explored the risks and impacts from geomagnetically-induced currents to transformers and other equipment on the bulk power system, as well as options for addressing or mitigating the risks and impacts. The Commission is considering the comments filed after that conference and what actions it can take under its current authority to address National security threats to the reliability of our transmission and power system from electromagnetic pulses.

The existing reliability standards do not address EMP vulnerabilities. Protecting the electric generation, transmission, and distribution systems from severe damage

---

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

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

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

due to an EMP-related event would involve vulnerability assessments at every level of electric infrastructure.

CONCLUSION

Although the Commission's current authority allows it to require the submission by the ERO of proposed standards to address the EMP threat to the United States, it does not allow the Commission the ability to author the standard, thereby limiting its effectiveness. The Commission is considering actions that it can take under its current authority. This authority, however, does not allow it to author standards or to require quick action to protect the United States from the EMP threat or other National security threats to the reliability of our transmission and power system. Any new legislation should address several key concerns, including allowing the Federal Government to take action before a cyber or physical National security incident has occurred, ensuring appropriate confidentiality of sensitive information submitted, developed, or issued under new authority, and allowing cost recovery for costs entities incur to mitigate vulnerabilities and threats.

These types of threats pose an increasing risk to the power grid that serves our Nation, which undergirds our Government and economy and helps ensure the health and welfare of our citizens. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

Mr. LUNGREN. Thank you very much for your testimony.

Mr. Wales.

STATEMENT OF BRANDON WALES, DIRECTOR, HOMELAND INFRASTRUCTURE THREAT AND RISK ANALYSIS CONTER, DEPARTMENT OF HOMELAND SECURITY

Mr. WALES. Thank you, Chairman Lungren, Ranking Member Clarke, and distinguished Members of the committee for inviting me to address the threat posed by electromagnetic pulse, or EMP, to our Nation's critical infrastructure, and the Department of Homeland Security's preparations to respond to and recover from EMP attacks.

As you mentioned, I am the director of the DHS Homeland Infrastructure Threat and Risk Analysis Center, known as HITRAC, which is charged with analyzing risks to the Nation's critical infrastructure from threats and hazards, both natural and man-made, recognizing EMP as a growing threat to the Nation's digital and physical infrastructures and the growing vulnerability of today's microelectronics to that threat. I appreciate the opportunity to discuss this issue.

As you know, an EMP is the burst of electromagnetic radiation created when a nuclear weapon is detonated or when a non-nuclear EMP weapon is used. Naturally-occurring solar weather can generate an effect similar to one component of EMP. The consequences of an EMP range from temporary system disruptions to permanent physical damage and critical service outages.

Overall, EMP in its various forms can cause widespread disruption and serious damage to electronic devices and networks, including those upon which many critical infrastructures rely, such as communication systems, information technology equipment, and supervisory control and data acquisition, commonly known as SCADA modules. SCADA modules are used in infrastructure, such as electric grids, water supplies, and pipelines. The disruption to SCADA systems that could result from EMP range from SCADA control errors to actual equipment destruction. Secondary effects of EMP may harm people through induced fires, electric shocks, and disruption of the transportation and critical support systems, such

as those at hospitals or sites like nuclear power plants and chemical facilities.

EMP places all critical infrastructure sectors at risk. Those sectors that rely heavily on communications technology, information technology, the electric grid, or that uses SCADA system, are particularly vulnerable. The complex interconnectivity among critical infrastructure sectors means that an EMP incident that affects a single sector will likely affect other sectors, potentially resulting in cascading failures. The interdependent nature of all 18 critical infrastructure sectors complicates the impact of the event and recovery from it.

The Department is working collaboratively, both internally and with external stakeholders, to reduce the risk from EMP and solar weather. For example, the Federal Emergency Management Agency have exercised scenarios involving EMP and solar weather and are developing plans to help address these evolving threats. FEMA is also working with States and industry to reduce the risk from EMP, notably by deploying new capabilities as part of the integrated public alert and warning system to help keep the public informed and alerted during a major EMP event.

The National Protection and Program Directorate's Office of Cybersecurity and Communications has also worked to model and assess EMP effects, and to conduct research and propose solutions to understand and mitigate EMP risks. NPPD's Office of Infrastructure Protection also plays a role in the Department's work on EMP. For example, our office conducted a study in 2010 on EMP's potential impact on extra-high voltage transformers and recommended options for hardening these systems from EMP attacks.

The Science and Technology Directorate has led much of the Department's research in the EMP area. Its recovery transformer project is intended to increase the resilience of the power grid through the development of a prototype extra-high voltage transformer that, unlike traditional transformers, will be able to be quickly delivered to a site, reducing potential recovery time by 75 percent.

S&T is also working to increase the resilience of the power grid through their resilient electric grid project. This project is designed to develop an inherently fault-current-limiting high temperature super-conducting cable, which can help the electric utilities manage fault currents that can cause cascading blackouts and permanent damage to electrical equipment.

The Commission to assess the threat to the United States from EMP attack recommended in its final report that DHS play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences. The Department takes that recommendation seriously. We have pursued a deeper understanding of the threat and its potential impacts and effective mitigation strategies, and a greater level of public awareness and readiness through various communication channels. But as we all know, there is more work to be done.

Thank you for holding this important hearing. I would be happy to respond to any questions.

[The prepared statement of Mr. Wales follows:]

PREPARED STATEMENT OF BRANDON WALES

SEPTEMBER 12, 2012

Thank you, Chairman Lungren, Ranking Member Clarke, and distinguished Members of the committee. It is a pleasure to appear before you today to discuss the nature of the threat posed by electromagnetic pulse (EMP) to our Nation and its critical infrastructure, including its cyber, communications, and electric-grid assets, as well as to discuss the Department of Homeland Security's (DHS) preparations to respond to and recover from potential EMP attacks.

Over the past several decades, the threat to digital and physical infrastructures has grown. For example, today's power grid and information networks are much more vulnerable to EMP than those of a few decades ago.[1] The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack recommended in its final report that DHS "play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences."[2] The Department takes that recommendation seriously and welcomes in cooperation with other Government agencies increasing understanding of this critical topic.

BACKGROUND

An EMP is the burst of electromagnetic radiation created when a nuclear weapon is detonated or when a non-nuclear EMP weapon is used. Naturally-occurring solar weather can generate effects similar to one component of an EMP. EMPs can be high-frequency, similar to a flash of lightning or a spark of static electricity, or low-frequency, similar to an aurora-induced phenomenon.[3] An EMP can spike in less than a nanosecond or can continue longer than 24 hours, depending on its source. The consequences of an EMP range from permanent physical damage to temporary system disruptions and can result in fires, electric shocks to people and equipment, and critical service outages. There are four general classes of EMP.

High-altitude EMP (HEMP) results from a nuclear detonation typically occurring 15 or more miles above the Earth's surface. The extent of HEMP effects depends on several factors, including the altitude of the detonation, the weapon yield and design, and the electromagnetic shielding, or "hardening," of assets. One high-altitude burst could blanket the entire continental United States and could cause widespread power outages and communications disruptions and possible damage to the electricity grid for weeks or longer.[4] HEMP threat vectors can originate from a missile, such as a sea-launched ballistic missile; a satellite asset; or a relatively low-cost balloon-borne vehicle. A concern is the growing number of nation-states that in the past have sponsored terrorism and are now developing capabilities that could be used in a HEMP attack.

Source Region EMP (SREMP) is a burst of energy similar to HEMP but differs in that it is created when a nuclear weapon detonates at lower altitudes within the atmosphere. SREMP can occur when a detonation occurs on or near the ground, as would likely be the case of a terrorist nuclear device attack. A SREMP's electromagnetic field is much more limited in range than that from HEMP; it would only affect a delimited geographic area. SREMP can induce very high currents on power

[1] Since the 1980s, our power grid control systems and information infrastructures have been growing in their reliance on the Ethernet and computers, which are much more vulnerable to E1 EMP than previous control and communications systems designs. Likewise, the power grid today is much more vulnerable to (E3 EMP) and solar storms than the grid of the 1970s and 80s due to the increasing network size and evolution to higher operating voltages.

[2] "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures," April 2008, page 181. This report presents the results of the Commission's assessment of the effects of a high-altitude EMP attack on our critical National infrastructures and provides recommendations for their mitigation.

[3] Aurora-induced phenomena refer to effects like geomagnetically-induced currents in the power grid that are caused by solar storms which are associated with increased aurora activity. Although there are many different phenomena associated with solar storms, one of the most important is the geomagnetically-induced quasi-dc current flow that can damage our power transmission networks.

[4] "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures," April 2008, page vi, "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." See also: Glasstone, S., P.J. Dolan, "The Effects of Nuclear Weapons," Chapter XI on EMP, U.S. Dept. of Energy, 1977.

cables or metallic communications lines near the fireball, and it can send extreme spikes of energy great distances from the blast zone along these metal lines, potentially causing fires where these lines meet other infrastructures. In addition, the SREMP travels through the air and can damage or disrupt equipment connected to Ethernet cables, telephone lines, and power cords out to 70 miles or more. Electronic systems not connected to power cords or communications lines, such as a cell phone, are generally resistant to SREMP but become useless if the infrastructure that supports them is non-functional. While SREMP is not the primary reason a terrorist would detonate a nuclear weapon, it is important to note that all ground-based detonations create SREMP of sufficient magnitude to cause infrastructure disruptions, including an improvised nuclear device, a crude nuclear device that could be built from the components of a stolen weapon or from using nuclear materials. Given the possible impacts of SREMP, such as secondary fires and the disruptions of power, communications, and other critical infrastructures, it is an important consideration in our Department's planning to mitigate and respond to this type of attack.

Unlike HEMP and SREMP, which primarily disrupt Earth-based infrastructures, System Generated EMP (SGEMP) is a threat to space-based assets, such as satellites or a space station. SGEMPs originate from a nuclear weapon detonation above the atmosphere that sends out damaging X-rays that strike space systems. Both SGEMP and HEMP are similar, in that they both originate from a high-altitude burst. The Department's chief concern with SGEMP and other related high-altitude nuclear effects is that satellite or other space systems that support critical communications and navigation services, as well as essential intelligence functions, can be immediately disrupted. SGEMP and other related effects could also harm systems supporting any astronaut in space.

The fourth type of EMP is Non-Nuclear EMP, or NNEP. This type of EMP can be created by Radio Frequency Weapons (RFWs), devices designed to produce sufficient electromagnetic energy to burn out or disrupt electronic components, systems, and networks. RFWs can either be electrically-driven, where they create narrowband or wideband microwaves, or they can be explosively driven, where an explosive is used to compress a magnetic field to generate the pulse. Multiple nations have used RFWs since the 1960s to disable or jam security, communications, and navigation systems; induce fires; and disrupt financial infrastructures. Devices that can be used as RFWs have unintentionally caused aircraft crashes and near crashes, pipeline explosions, gas spills, computer damage, vehicle malfunctions, weapons explosions, and public water system malfunctions.[5] The Department believes that much of the mitigation and planning we are doing for other types of EMP will help reduce our threat to NNEP.

SOLAR WEATHER

Solar Weather is created as a result of massive explosions on the sun that may shoot radiation towards the Earth. These effects can reach the Earth in as little as 8 minutes with Solar Flare X-rays or over 14 hours later with a Coronal Mass Ejection (CME) plasma hurricane. An extreme CME is the Department's biggest Solar Weather concern. It could create low-frequency EMP similar to a megaton-class nuclear HEMP detonation over the United States, which could disrupt or damage the power grid, undersea cables, and other critical infrastructures. The United States experiences many solar weather events each year, but major storms that could significantly impact today's infrastructures are not common but have previously occurred in 1921 and 1859 and possibly in several other years prior to the establishment of the modern power grid. The U.S. Department of Energy and utility owners and operators have been focusing on potential threats and steps that utilities can take to reduce possible impacts.[6] Work is underway in cooperation with a number of Federal agencies including the: National Aeronautics and Space Administration (NASA), Nation Oceanic and Atmospheric Administration (NOAA), United States Geological Survey, Department of Energy, Department of Defense, and DHS with industry support and participation to ensure this threat is understood.

---

[5] Robert L. Schweitzer, LTG (ret) USA, "Radio Frequency Weapons: The Emerging Threat and Policy Implications," Eagan, McAllister Associates, October 1998; see also: Overview of Evolving and Enduring Threats to Information Systems, National Communications System, August 2012.

[6] In the last 200 years, only the 1859 and 1921 solar superstorms are believed by experts to have exceeded the 4,000 nanoTesla/minute level over the United States. If one of these storms were to occur today, many experts believe they would likely damage key elements of the power grid and could cause very long-term power outages over much of the United States.

POTENTIAL IMPACTS TO CRITICAL INFRASTRUCTURE

Overall, EMP in its various forms can cause widespread disruption and serious damage to electronic devices and networks, including those upon which many critical infrastructures rely, such as communication systems, information technology equipment, and supervisory control and data acquisition (SCADA) modules. SCADA modules are used in infrastructure such as electric grids, water supplies, and pipelines. The disruptions to SCADA systems that could result from EMP range from SCADA control errors to actual SCADA equipment destruction. Secondary effects of EMP may harm people through induced fires, electric shocks, and disruptions of transportation and critical support systems, such as those at hospitals or sites like nuclear power plants and chemical facilities.

EMP places all critical infrastructure sectors at risk. Those sectors that rely heavily on communications technology, information technology, the electric grid, or that use a SCADA system are particularly vulnerable. The complex interconnectivity among critical infrastructure sectors means that EMP incidents that affect a single sector will likely affect other sectors—potentially resulting in cascading failures. The interdependent nature of all 18 critical infrastructure sectors complicates the impact of the event and recovery from it.

DHS'S EFFORTS TO STUDY, MITIGATE, AND RESPOND TO EMP ATTACKS

The Department, acting through the Federal Emergency Management Agency (FEMA), the National Protection and Programs Directorate (NPPD) and the Science and Technology Directorate (S&T), has worked extensively to help recognize EMP as a threat to the Nation. Specifically, the Department is working collaboratively, both internally and with external stakeholders, in various arenas to reduce risk. For example, DHS has exercised scenarios involving both EMP and solar weather and is developing plans to help address these evolving threats. Likewise, FEMA and other Government agencies are working with States and industry. For example, FEMA is deploying new capabilities as part of the Integrated Public Alert and Warning System, such as the protected Emergency Alert System Primary Entry Point AM and FM radio stations that would be used by the President and key leadership to help keep the public informed and alerted during a major EMP event.[7] Both NASA and NOAA are improving and testing their Space Weather warning systems. Many of the Federal Government's missions rely on satellite imagery, communications satellites, and GPS for their execution. The potential impact of solar storms on satellites led Secretary Napolitano to issue the DHS Space Policy on February 3, 2011, which committed the Department to working with both private and public-sector partners on increasing the resilience of mission essential functions.

Two offices within NPPD are at the forefront of understanding and working to identify how EMP can impact the homeland security enterprise. First, the Office of Cybersecurity and Communications (CS&C) has worked extensively to model and assess EMP effects and conduct research and propose solutions to understand and mitigate EMP risks. As a result, CS&C has produced many assessments of the risks and mitigation options related to EMP. In particular, significant progress has been made in the last few years in modeling and understanding the risks of SREMP associated with an improvised nuclear device.

NPPD's Office of Infrastructure Protection (IP) also plays a significant role in the Department's work on EMP. IP conducted a study in 2010 on EMP's potential impact on extra high-voltage (EHV) transformers for the Western United States' electrical grid. The study included findings about EMP from both artificial and naturally-occurring incidents and recommended options for hardening EHV transformers from EMP.

S&T has led much of the Department's research in the EMP area and is conducting important work through the Recovery Transformer (RecX) Project to increase the resiliency of the EHV transmission power grid, through the use of more mobile and modular transformers. EHV transformers are very large, extremely difficult to transport, and until 2009 primarily manufactured overseas, complicating rapid recovery and restoration efforts. This effort has developed a prototype EHV transformer that can quickly be deployed to a site, via a series of trailers and semitrucks, and then installed, assembled, and energized rapidly. The prototype RecX was demonstrated and installed in the grid at a host utility and is currently undergoing a 1-year observational period to verify its performance.

[7] To date, 17 National-level Emergency Alert System radio stations have been protected against EMP. Within the next year, another 20 National-level EAS radio stations are planned to have EMP protection installed.

Another Departmental effort to increase the resiliency of the power grid is the S&T Resilient Electric Grid Project. S&T has developed a power-surge limiting, high-temperature, superconducting cable for electric grid resiliency that enables distribution-level substations to interconnect and share power and assets, while helping electric utilities manage power surges arising from a variety of causes that can cause cascading blackouts and permanent damage to electrical equipment. The interconnection of substations increases the resiliency of the grid by creating multiple paths for power flow. Superconducting cables also provide additional benefits such as allowing more power to flow through a smaller cable with lower transmission losses. The cable will be installed for testing and evaluation in Yonkers, NY, in 2014. Several approaches to improving the resiliency of the electrical grid are underway both in the United States and abroad that hold promise to reduce the vulnerability of extra large transformers and reduce the threat to the electricity grid.

CONCLUSION

DHS has pursued a deeper understanding of the EMP threat as well as its potential impacts, effective mitigation strategies, and a greater level of public awareness and readiness in cooperation with other Federal agencies and private equipment and system owners and operators through various communications channels. However, more work is needed to understand the risk posed by EMP and solar weather to all sectors, through direct and cascading impacts. I commend the committee for its interest in this key issue and look forward to your questions.

Mr. LUNGREN. Thank you very much, Mr. Wales.
Mr. Aimone.

STATEMENT OF MICHAEL A. AIMONE, DIRECTOR, BUSINESS ENTERPRISE INTEGRATION OFFICE OF THE DEPUTY UNDER SECRETARY OF DEFENSE FOR INSTALLATIONS AND ENVIRONMENT, OFFICE OF UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS, DEPARTMENT OF DEFENSE

Mr. AIMONE. Thank you, Chairman Lungren, Ranking Member Clarke, and distinguished Members of the subcommittee.

I was asked specifically to address the question of how the Department of Defense would operate during a significant outage of the commercial electrical grid. Although today's hearing is focused on the prospect of the EMP event, such an event is only just one scenario of a grid outage. DOD, as it has been stated before me, is in fact heavily dependent upon the electrical commercial grid.

The Department has two closely-coordinated sets of activities that focus on the need to maintain critical mission activities in the event of a commercial outage. One set of these activities, led by our Department's Office of Homeland Defense, is part of the Department's explicit Mission Assurance Strategy. The other set of activities focused in the Office of the Under Secretary for Installations and Environment falls underneath the Facilities Energy Strategy. These two strategies are tied together.

With regards to the Mission Assurance Strategy, the Department has long had a major focus on mitigating risks to high-priority DOD facilities and infrastructure and the critical global missions they support. To that end, DOD recently adopted the Mission Assurance Strategy to focus on enduring operational continuity in an all-hazards threats environment.

This strategy entails a two-track approach. Track I includes in-house mitigation activities, those efforts that the Department can execute largely in-house. Track II of our Mission Assurance Strategy tackles the many challenges to DOD mission execution and re-

quires external collaboration with our partners in the Department of Energy, Homeland Security, and industry.

With regards to the facility's energy strategy, the Department's fixed installations are traditionally served by—as largely as platforms for training and deployment of forces. But in recent years, they have begun to provide direct support to combat operations, such as unmanned aerial vehicles flown in Afghanistan from fixed installations here in the United States.

Our fixed installations also serve as staging platforms for humanitarian and Homeland Defense missions. These installations are largely dependent on the commercial power grid that is vulnerable to disruptions due to aging infrastructure, weather-related events, and potential kinetic and cyber attack.

Currently, the Department ensures that it can continue its mission-critical activities on base, in the event of a grid outage through its fleet of on-site power generation equipment. This equipment is connected to essential mission systems. In addition, each installation has standby generators in storage for repositioning as required.

As further backup to these on-site generation equipment, DOD maintains a strategic stockpile of electrical power generators and support equipment that is kept in operational readiness. For example, during Hurricane Katrina, the Air Force transported more than 2 megawatts of specialized diesel generators from Florida, where they were stored, to the Keesler Air Force base in Mississippi to support base recovery.

Although the Department will continue to maintain its fleet of on-site and mobile backup generators, we are also moving aggressively to adopt the next generation micro-grids. Advanced micro-grids combined with on-site energy generation and energy storage offer a more robust and cost-effective approach to ensuring installation energy security than the current solution of just maintaining a fleet of backup generators.

Advanced micro-grids are a triple play. First, they will facilitate and incorporate renewable and other on-site energy generation. Second, they will reduce installation energy costs on a day-to-day basis by allowing for load balancing and demand response. Third, and more importantly, the combination of on-site energy and storage, together with the micro-grid's ability to manage local energy supply and demand will allow an installation to shed the non-essential loads and maintain critical mission loads if the grid should go down.

The Department's Installation Energy Test bid is funding 10 demonstrations of micro-grids and storage technologies to evaluate benefits and risks of alternative approaches and configurations. The test bid is working with multiple vendors so that to allow that DOD captures the benefits of competition.

That ends my prepared remarks. Thank you for holding this important hearing.

[The prepared statement of Mr. Aimone follows:]

PREPARED STATEMENT OF MICHAEL A. AIMONE

SEPTEMBER 12, 2012

Chairman Lungren and distinguished Members of the subcommittee. Thank you for the opportunity to testify. I was asked to address the question of how the Department of Defense (DoD) would operate during a significant outage of the commercial electric power grid.

Although today's hearing is focused on the prospect of an electromagnetic pulse (EMP) event, such an event is only one scenario for a grid outage. DoD is heavily dependent on the commercial electric power grid. The Department has two closely coordinated sets of activities that focus on the need to maintain critical mission activities in the event of a commercial grid outage. One set of activities, led by DoD's office of homeland defense, is part of the Department's explicit "mission assurance strategy." The other set of activities, focused on the Department's fixed installations and led by its Installations and Environment office, falls under DoD's "facility energy strategy."

MISSION ASSURANCE STRATEGY

The Department has long had a major focus on mitigating risks to high-priority DoD facilities and infrastructure and the critical global missions they support. Toward that end, DoD recently adopted an explicit Mission Assurance Strategy, which is focused on ensuring operational continuity in an all-hazard threat environment.

This strategy entails a two-track approach. Track I includes "in-house" mitigation efforts—activities that the Department can execute largely on its own. A key element is DoD's Defense Critical Industry Program (DCIP)—an integrated risk management program designed to secure critical assets, infrastructure, and key resources for our Nation. DoD and the Department of Homeland Security (DHS) work closely together as part of DCIP. Under Track I of the Mission Assurance Strategy, DCIP will continue to update the list of DoD's most critical assets and target them for special mitigation efforts through DoD's budget and other internal processes.

Track II of our Mission Assurance Strategy tackles the many challenges to DoD mission execution that require external collaboration with partners such as the Department of Energy (DOE), DHS, and industry. Given that DoD mission execution relies heavily upon the energy surety of the communities surrounding our installations, Defense Industrial Base facilities spread across entire regions, and on private sector infrastructure that will collapse without electricity, this two-track approach can help meet the challenges to DoD mission assurance that lie far beyond our military bases.

DOD'S FACILITY ENERGY STRATEGY

DoD's facility energy strategy is also focused heavily on grid security in the name of mission assurance. Although the Department's fixed installations traditionally served largely as a platform for training and deployment of forces, in recent years they have begun to provide direct support for combat operations, such as unmanned aerial vehicles (UAVs) flown in Afghanistan from fixed installations here in the United States. Our fixed installations also serve as staging platforms for humanitarian and homeland defense missions. These installations are largely dependent on a commercial power grid that is vulnerable to disruption due to aging infrastructure, weather-related events, and potential kinetic, cyber attack. In 2008, the Defense Science Board warned that DoD's reliance on a fragile power grid to deliver electricity to its bases places critical missions at risk.[1]

STANDBY POWER GENERATION

Currently, DoD ensures that it can continue mission-critical activities on base largely through its fleet of on-site power generation equipment. This equipment is connected to essential mission systems and automatically operates in the event of a commercial grid outage. In addition, each installation has standby generators in storage for repositioning as required. Facility power production specialists ensure that the generators are primed and ready to work, and that they are maintained

[1] "More Fight—Less Fuel," Report of the Defense Science Board Task Force on DoD Energy Strategy, February 2008. Facility energy is also important because of its high cost. With more than 300,000 buildings and 2.2 billion square feet of building space, DoD has a footprint three times that of Walmart and six times that of the General Services Administration. Our corresponding energy bill is $4 billion annually—roughly 10 percent of what DoD spends to operate and maintain its installation infrastructure.

and fueled during an emergency. With careful maintenance these generators can bridge the gap for even a lengthy outage. As further back up to this installed equipment, DoD maintains a strategic stockpile of electrical power generators and support equipment that is kept in operational readiness. For example, during Hurricane Katrina, the Air Force transported more than 2 megawatts of specialized diesel generators from Florida, where they were stored, to Keesler Air Force Base in Mississippi, to support base recovery.

NEXT GENERATION MICROGRIDS

Although the Department will continue to maintain its fleet of on-site and mobile backup generators, we are moving aggressively to adopt next-generation microgrids. Advanced microgrids, combined with on-site energy generation (e.g., solar or geothermal) and energy storage, offer a more robust and cost-effective approach to ensuring installation energy security than the current solution (backup generators). Although microgrid systems are in use today, they are relatively unsophisticated, with limited ability to integrate renewable and other distributed energy sources, little or no energy storage capability, uncontrolled load demands, and "dumb" distribution that is subject to excessive energy losses. By contrast, we envision advanced (or "smart") microgrids as local power networks that can utilize distributed energy, manage local energy supply and demand, and operate seamlessly both in parallel to the grid and in "island" mode.

Advanced microgrids are a "triple play" for DoD's installations: First, they will facilitate the incorporation of renewable and other on-site energy generation. Second, they will reduce installation energy costs on a day-to-day basis by allowing for load balancing and demand response—i.e., the ability to curtail load or increase on-site generation in response to a request from the grid operator. Third, and most importantly, the combination of on-site energy and storage, together with the microgrid's ability to manage local energy supply and demand, will allow an installation to shed non-essential loads and maintain mission-critical loads if and when the grid goes down.

DoD's Installation Energy Test Bed, run out of the Department's Installations and Environment office, is funding ten demonstrations of microgrid and storage technologies to evaluate the benefits and risks of alternative approaches and configurations. The Test Bed is working with multiple vendors so as to allow DoD to capture the benefits of competition. Demonstrations are underway at Twentynine Palms, CA (General Electric's advanced microgrid system); Fort Bliss, TX (Lockheed Martin); Joint Base McGuire-Dix-Lakehurst, NJ (United Technologies); Fort Sill, OK (Eaton); and several other installations.

Mr. LUNGREN. Thank you very much. I appreciate the testimony of all our panelists. You have added to our record in very substantial ways and we appreciate that.

I will recognize myself to begin with the questioning now.

Mr. McClelland and Mr. Wales, in the area of dam safety and in the area of protection against flooding, we have means by which we assess whether a dam is at protection level of 1-in-100-year flood, 1-in-200-year flood. My area, the Folsom Dam was 1-in-90-year flood. We are doing modifications to bring it up to 1-in-200-year flood, which is an improvement, but would still leave us behind where New Orleans was before Katrina hit.

But there is an assessment by which you can make those determinations. Do we have a way of determining, with critical infrastructure of the electric grid, whether they are protected against the 1-in-100 possibility, the 1-in-200 possibility? Is there a way of gauging that sort of thing? If there is, is there a general assessment of where our electric grid is in terms of protecting against this 1-in-100 possibility of electromagnetic pulse?

Mr. MCCLELLAND. I can start with that. There are operational procedures in specific parts of the country and monitors in place. For instance, in PJM, in the eastern interconnection, if ground current levels reach 10 amps, they start to mitigate. They start to redispatch the units and move power around, so they reduce load on

some of the transformers. But as far as automatic mitigation efforts, there are very few.

If an entity puts in a series capacitor, it will block a ground-induced current, so it will mitigate any effects from a solar magnetic disturbance. It is not done particularly for GMD. It is done for economic reasons to reduce the losses on the transmission line and increase the throughput, particularly in the western interconnection. The far and away, both the electronics aspects and the large power equipment, is largely unmitigated from a hardware standpoint.

I think that is particularly important when you consider some of the past events. In 1989, there was a geomagnetic disturbance, a solar flare. The whole province of Quebec, 5 million people, was out of power in 90 seconds. There was little any operator could have done. In fact, there was nothing practically an operator could have done to prevent that grid from collapsing.

The information we have from Zurich is that—and we are trying to confirm this with our friends in Quebec—is that that outage alone cost $2 billion.

Mr. LUNGREN. You say there is nothing that could be done. Do you mean with current equipment as it was displayed at that time? Or are there that could have been done in retrospect?

Mr. MCCLELLAND. Oh, yes. There are things that could have been done. But from an operational standpoint, it happened too fast for an operator sitting at a terminal to really realize what was occurring. After that event, though, Quebec did protect themselves from geomagnetic disturbance and electromagnetic pulse. They did put series capacitors in to protect their system. So they have mitigated themselves against this issue.

Mr. LUNGREN. Mr. Wales, Congressman Franks suggested that the costs associated with taking some of these measures to protect our electric grid in the light of the potential damage would be reasonable. Does that make sense to you?

Mr. WALES. I would actually defer some of this question to my colleague from FERC. But I would say two things. One is, working with the private sector, they are going to look at both cost; they are also going to look at the potential impact on operations. I think the electric sector is a fairly conservative industry. They have a responsibility for ensuring a very high degree of reliability in electric power grids. So anytime we turn on the lights, it is 99-plus times, it is working. In order to maintain that, they are fairly conservative about new advances in new technology, what gets inserted in the grid without sufficient testing and other procedures.

Over time, I think we are definitely seeing improvements, more series capacitors inside of networks to mitigate the risk of geomagnetic disturbances, exploring new technologies that could be brought to bear to allow a more resilient grid.

There is certainly more that the industry can do. I think one last point on the cost is, this is an industry that when they want to raise costs, have to get permission from numerous utility commissions—utility boards around the country. So when they have to pass on potential costs, even ones that may seem minor, they have to go request permission from individual utility commissions, one at a time. That does have a potential impact on their ability to

move quickly, raise rates, in order to deploy new and advanced technologies.

Mr. LUNGREN. I would say that costs are difficult to pass on if, in fact, the information is not there for people to understand the worthiness of the cost commitment. Let me just ask you Mr.—and by the way, when you use the word conservative, I am not offended.

[Laughter.]

Mr. LUNGREN. Mr. McClelland, in terms of the costs, Congressman Franks suggested that the costs are not out of proportion to the damage to be prevented. Is that, in your mind, accurate?

Mr. MCCLELLAND. Yes. Just to give you a quick example, if we go to the Quebec outage again, the cost to society for a relatively short outage to 5 million people—I believe the outage was about 9 hours long—was about $2 billion, estimated by Zurich. Mitigation devices that would absolutely block the geomagnetic disturbance effects, so you wouldn't have to worry if it is a 1-in-100-year event or a 1-in-60,000-year event, the Fukushima-Daiichi, the conservative cost is about $500,000 per transformer. If you extrapolate that into $2 billion cost for relatively modest losses, I mean, you could mitigate 4,000 transformers, which is far and away in excess of anything that would need to be done in Quebec.

The Oak Ridge report, on the other extreme, when it estimated severe effect, was $1 trillion to $2 trillion. That is with equipment damage. So that one event, even if there is no loss of equipment whatsoever, one even could more than pay for the cost of mitigation.

Mr. LUNGREN. Thank you very much.

The Ranking Member is recognized.

Ms. CLARKE. Thank you, Mr. Chairman. Conservatism does has its place.

My first question is to Mr. Wales. I wanted to just get from you what your best risk analysis is telling us about the probability of a severe geomagnetic disturbance or an EMP that would cause widespread damage to the electric grid.

Mr. WALES. You know, I think the Department would classify both of those events as ones that are low likelihood. In the case of a solar storm, we are sure that there are solar storms that will hit the United States again in the future. Whether that is in 1 year or in 10,000 years, we don't know.

The potential when you are evaluating the potential impacts of those types of events, in particular the challenge of addressing what Chairman Lungren mentioned earlier in terms of against the 1-in-100-year flood, looking at geomagnetic storms is not just a 1-in-100-year event, it is what direction is that solar storm—north, south, east, west? What is the intensity of that storm, duration, et cetera? So all of those factors will come into play when evaluating the potential impacts. So in some cases, if it goes in one direction, the western interconnect doesn't have severe outages. If it goes in another direction, it may have a severe outage.

I would also say that some of the information associated with the likelihood of an EMP being used would have to be done in a closed hearing. But on the whole, we would continue to assess these as low-likelihood events. That is not to say that the nature of the im-

pacts associated with them don't require action, which is why the Department is taking those measures where it can. But again, trying to balance those against all the risks that critical infrastructure, including the power grid face every day, requires both interaction with the private sector to build their capacity and ensure that they have the right information available to them as they are deciding on their own, how to use their scarce resources for security enhancements and to build resilience into these systems.

Ms. CLARKE. So would you say low likelihood is the equivalent of a once-in-10-year event, once-in-100-year event, once-in-500-year event? You know, how do we kind of gauge that categorization of it?

Mr. WALES. I think, in general, in the solar storm context, it is a little bit easier to determine since there is more frequency in which to do analysis on. Those severe solar storms have historically been termed a 1-in-100-year event. That is generally considered to be a low-likelihood scenario, particularly when that 1-in-100-year event may only hit a one piece of the country, may hit—or a larger one—we don't really know.

I think there is need to do more study for exactly how a solar event could impact the infrastructure. While it is likely that there will be significant disruption, the key variable is whether there will be severe equipment damage that will require long lead times to replace. Without that kind of information, it is unclear what type of mitigation may be best and be able to assess in more detail what the likely consequences and how quickly we can recover.

Ms. CLARKE. Mr. McClelland, as I understand, there are two risks that result from the introduction of a ground-induced current from a geomagnetic disturbance to the bulk power system. No. 1, damage to the bulk power system assets, like transformers. No. 2, loss of reactive power support, which could lead to voltage instability. How does the Commission oversee that operators of the grid address these risks in a responsible and comprehensive way?

Mr. MCCLELLAND. I think you have hit on, sort of, the key differentiation between all the prior bodies of study and the NERC report. The prior bodies of study have said that there would be a significant opportunity for widespread destruction of transformers. The NERC report, however, took exception and said that the reactive power requirements of the transformers under these conditions would increase significantly, causing the grid to collapse before there was any significant damage. The two are very related.

So the Commission called a technical conference to sort out the details. What we did find was an absolute certainty was that no one really knows. There was no correlation studies done on the reactive power supply or on the relays and controls themselves, so with absolute certainty, no one can say that the grid would collapse.

In fact, there have been events in 2003 in South Africa, there was a low-level GIC current. It was too small to cause reactive power requirements to increase on the transformers and yet it destroyed 12 large bulk power system transformers. It took years for the South Africans to recover.

So we know with certainty that is not going to be the case. We know in Quebec, although the grid collapsed very quickly, there

were still transformers lost at St. John's Bay. So I think that the issue, the consensus we did achieve was that grid collapse is absolutely unacceptable in any event, whether it causes a lot of transformers to be damaged or whether it just causes a few transformers. The protection scenario, fortunately, is the same.

So if the GIC is mitigated, either dampened or blocked—if you dampen, you have to pick to what level. If you block, it costs the same and you have got certainty associated with it. You won't have to worry about either the reactive power consumption or the destruction of the transformers. It is mitigated.

Mr. LUNGREN. Thank you.

Mr. Long.

Mr. LONG. Thank you, Chairman.

Mr. Wales, you talked about a study, I think, in an accompanying report earlier. Was that a HITRAC study? Or——

Mr. WALES. Yes.

Mr. LONG. Okay. What would the cost be to implement that proposal that came out of the HITRAC study and accompanying report?

Mr. WALES. We did not work with industry to assess the explicit costs. Some of those recommendations, however, were similar to those that were found in the EMP Commission's report. I will refer you to that, but in the EMP Commission and most of the recommendations in the electric power grid section came to a couple of billion dollars for a Nation-wide implementation.

Mr. LONG. It would be what?

Mr. WALES. A couple of billion dollars for Nation-wide implementation of all of their recommendations related to the electric power system.

Mr. LONG. A couple of billion dollars Nation-wide?

Mr. WALES. Yes.

Mr. LONG. Mr. McClelland, didn't you say that the one event up in Canada cost how much?

Mr. MCCLELLAND. Two billion dollars. Estimated at $2 billion by Zurich.

Mr. LONG. So you are telling me, Mr. Wales, that for $2 billion we could implement what we need to do to mitigate this.

Mr. WALES. It may be higher than $2 billion. It may be closer to $4 billion or $5 billion. Some of their costs were per unit, so figuring out exactly how many of those units you would employ, where you want to have that level of EMP protection. But based upon, again, the EMP Commission's report contained these cost estimates.

Mr. LONG. The what now?

Mr. WALES. The Commission to assess the threat to EMP to the United States—that Commission—that is where those cost estimates came from.

Mr. LONG. It still doesn't jive to me. So, I mean, if we are asked to do something as a Congress in these austere times, it would sure be handy if we had some kind of a—and, I mean, just on the surface, thinking that an event in Canada cost $2 billion in Quebec. Was that where it was?

Mr. WALES. Yes.

Mr. LONG. To think we could go and do everything—put in all the safeguards we need to for $2 billion or $4 billion or $6 billion, that doesn't jive with me. So if we are trying to make decisions here and serious discussion, I think that if you all could come back with some figures of some type that had a little justification to them, it would help us try and help you.

Mr. Wales, by virtue of how our economy is structured, most electric and other critical infrastructure is privately owned. So No. 1, I think we would have to get the figure first, but how do you overcome the challenge of convincing private industry to make that type of capital investment. Again, we don't know what the capital investment is yet, but to protect the electric grid.

Mr. WALES. Historically, DHS has—given the fact that it does not have regulatory authority to compel action within the private sector for most critical infrastructure sectors—has determined that the best way for us to advance the overall mission is to work collaboratively with the industry, provide them with the information that they need to better assess how they can increase their protection and enhance their resilience. Using that type of information, hopefully, and owners and operators will make the capital investments that are best situated given the potential risk that they may face.

For example, power operators in the southern part of the country are less at risk than the northern part of the country to geomagnetic storms. They may take a somewhat different perspective when it comes to investments to harden their systems against solar or events. But forming—partnerships, working with the industry and relevant other Government agencies, like Department of Energy, Department of Defense, FERC, to ensure that all available information is on the table. Any knowledge gained through the studies that we do, the research and development that is done in places like S&T and in the private sector are shared and the knowledge base is expanded.

Mr. LONG. Okay. Again, I would like to—you know, with all the reporting and the study and everything, if we had some numbers that we could—you know, they say, figures lie and liars figure, so if we had some decent figures to work with, it would sure help. Thanks for being here.

I am proud to report that I have 30 seconds to yield back.

[Laughter.]

Mr. LUNGREN. I thank the gentleman. So I will use those 30 seconds.

Mr. Aimone, I feel sorry for you not having any questions directed to you, so I feel compelled to ask you about the micro-grids that you were talking about. You referred to that as one of the Defense Department's approaches to dealing with the potential of a loss of energy supply to fix facilities. How do you define micro-grids and how far along are you in the development of them?

Mr. AIMONE. Thank you very much for the question.

What we are hoping to do with our micro-grid demonstrations—and we have one going on today at Twentynine Palms, a U.S. Marine Corps installation in California, as well as an installation in Texas at Fort Bliss, and several other of these micro-grid demonstrations—are bringing together, if you will, the ability to take

the renewable energy resources that are variable in nature—the sun is out. These renewable energy sources can provide energy, tie these to the electrical loads on the base and operate, if you will, the power system of the base as a small electrical grid, separate from the Nation's grid, should that happen to be.

In fact, what we really want to do is be able to use the best of the economics of the National grid when it is available and the micro-grid can take a look at economics associated with power production on base and purchasing electrical power off base with regards to the demands that are available that are occurring on the installation moment-by-moment and balance those electrically, such that demand and supply are achieved as a local grid.

Mr. LUNGREN. I am not an expert on this, so forgive me. But in speaking with some of the operators of electrical systems in California, they have told me how renewable energy sources are the most difficult to balance because of the variability—sun, wind, et cetera. So maybe I just don't understand the technology there, but it seemed to me if you are creating a micro-grid that is reliant on the variabilities of the renewable resources—wind, solar—that is a difficult technical challenge and how long a fix is that?

Mr. AIMONE. Combine our renewable sources that would bring energy onto the installation from on-base sources with our demands would be the appropriate energy storage devices. We have demonstrations of battery technology that would, if you will, gap the difference between what is available from renewable energy and the demands required. Also would allow for the on-base generation that exists to be able to be ramped up to meet the needs if the storage system is being exhausted, yet the renewable sources aren't available.

So this is a combination of demand on-base generation and storage.

Mr. LUNGREN. I appreciate all that, and I appreciate what you are doing on that. But does the fact still remain that our fixed installations within the continental United States still rely primarily on energy produced from our regular electric grid?

Mr. AIMONE. That is a true statement. With one caveat, if I may, and that caveat is those critical mission loads have those standby generators that I was speaking to that have the capability of operating in times of grid outage, such that they could make sure that those important mission loads can be achieved. For example——

Mr. LUNGREN. So long as the grid outage isn't beyond the capability of your on-installation energy production.

Mr. AIMONE. That is a true statement. So testing these generators to make sure that they can meet the needs of the loads during a simulated outage, the understanding of how much fuel is required, and when the fuel needs to be provided to those particular generators so that you always have a constant supply of fuel. The inherent generator itself, if it is well-maintained and operated correctly within the parameters of that generator, will meet that load for as long as you have fuel to it.

So we practice how do we get fuel to those generators in the time of an emergency, even if we have to go off-base and find appropriate fuel from other locations.

Mr. LUNGREN. Thank you very much.

Mr. Long, do you have any more questions?

All right, I want to thank this panel. You have been very, very helpful. This is an issue that is timely and timeless and we appreciate your assistance. Thank you very much.

The sole witness of our final panel today is Dr. Chris Beck, the president of the Electric Infrastructure Security Council. Dr. Beck is a policy expert in several homeland security-related areas, including critical infrastructure protection, cybersecurity, science and technology development, WMD prevention and protection, and emerging threat, identification, and mitigation. Dr. Beck holds a Ph.D. in physics from Tufts University, a B.S. in physics from Montana State University. Immediately prior to his service at EIS, Dr. Beck served as the minority staff director of this very subcommittee. We appreciate your return.

As you know the rules as well as anybody, your written testimony will be entered into the record and we would ask you to try and summarize your testimony in 5 minutes and then we will ask questions.

STATEMENT OF CHRIS BECK, PRESIDENT, ELECTRIC INFRASTRUCTURE SECURITY COUNCIL

Mr. BECK. Well, thank you, Chairman Lungren. Thank you, Ranking Member Clarke. Thank you, Mr. Long. It is good to be back before the committee. It is a little disorienting to be on this side of the witness table, but I will do the best I can.

As you mentioned, I started looking at these issues while a member of this committee, and it was because of the seriousness of this issue that I moved to the Electric Infrastructure Security Council to focus on this issue full-time. So I very much appreciate this committee holding this hearing and giving this issue your attention.

The Electric Infrastructure Security Council's mission is to work in partnership with Government and corporate stakeholders to host National and international education, planning, and communication initiatives to help coordinate infrastructure protection against electromagnetic threats.

We are happy and proud to co-host the Electric Infrastructure Security Summit series, the annual international government NGO summits on infrastructure security. The third annual summit took place on May 14 and 15 this year in the United Kingdom's houses of parliament in London. Ranking Member Clarke was one of the U.S. bipartisan co-chairs of this event, along with Representative Trent Franks, who you heard from earlier.

The summit was a gathering of senior government representatives, scientists, and industry executives from 21 countries. The conclusions and recommendations that we discussed should be of great interest to this committee. I have provided the full summary report and my testimony is a quick summary of that.

We have covered a lot of the ground, so I don't think I need to describe the problem, the severity, or the lack of specificity of the timing of these events. The key questions we asked at the Electric—at the summit were, "Should we respond to these threats?" "If so, what is the path forward?" "Who should be involved?" "And how broad should our response be?"

"Should we respond" was a resounding, "yes." There is certainly enough evidence known and enough identified vulnerability that the delegates felt it is time to move forward.

"What is the path to move forward?" A much more difficult question. We arrived at a couple of things. One is to define and apply interconnect-wide standards and protection plans and to pursue two paths to implementation. One, is validate and implement specific cost-effective protection measures. Two, is to prioritize scope and timing of protective measures by expanded hardware and interconnect-wide modeling prioritization and data collection.

"Who should be involved?" The sense of the summit participants is the broader the community, the better the result that we are going to get. So while this issue initially was, as Mr. Wales said, identified by the EMP Commission and it was initially looked at as a government question, we need participation from government, from commercial power suppliers, insurance companies, other stakeholders that can each contribute in their own area of expertise.

"How broad should our scope be?" We have discussed both naturally-occurring instances of geomagnetic disturbances and malicious EMP, and the consensus again was that both need to be addressed.

I am happy to go into any of these points in greater detail as we move forward. I would like to note that there appear to be no significant technical or financial barriers to mitigating this threat. The technologies needed are well understood and the cost based on both government estimates and recent corporate experience is quite low. Going back to questions raised by Mr. Long. So I think that cost-effective measures are available.

This concludes my prepared testimony. I look forward to answering any questions.

[The statement of Mr. Beck follows:]

PREPARED STATEMENT OF CHRIS BECK

SEPTEMBER 12, 2012

Good morning Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee. Thank you for holding this hearing on what I consider to be one of the greatest threats to our National and homeland security. As many of you know, before I became EIS Council's President, I worked for this committee, focusing on Critical Infrastructure Protection and Science and Technology issues. It was through that work that I first became aware of the threats facing our critical electric infrastructures, and I found the issue to be so important that I felt compelled to focus on it exclusively.

The Electric Infrastructure Security Council's mission is to work in partnership with Government and corporate stakeholders to host National and international education, planning, and communication initiatives to help coordinate infrastructure protection against electromagnetic threats (e-threats). E-threats include naturally-occurring geomagnetic disturbances (GMD), high-altitude electromagnetic pulses (HEMP) from nuclear weapons, and non-nuclear EMP from intentional electromagnetic interference (IEMI) devices.

EIS Council is also proud to co-host the Electric Infrastructure Security Summit Series, the annual international government/NGO summits on infrastructure security. The third annual summit took place on May 14 and 15 this year, in the United Kingdom's Houses of Parliament in London. Ranking Member Clarke was one of the U.S. bipartisan co-chairs of that event, along with Rep. Trent Franks. This summit was a gathering of senior government representatives, scientists, and industry executives from 21 countries. The conclusions and recommendations that we discussed

should be of great interest to this committee. The full report has been provided to the committee as an addendum to my testimony, and I include the summary here.

SUMMARY OF MAJOR THEMES AND RECOMMENDATIONS

Defining the Issue

The Problem.—Developed nations are vulnerable to serious National power grid damage from e-threats, both natural and malicious.

The Severity.—The impact will range from, at minimum, a serious financial and economic crisis to, at maximum, a catastrophe that would threaten societal continuity.

The Timing.—For severe space weather, the most recent events occurred 90 and 150 years ago, but the precise timing of the next such occurrence, as with all extreme natural disasters, is unknown. For malicious EMP, either local (non-nuclear) or sub-continental (nuclear), a strike could be induced by on-going vulnerability coupled with rapidly changing geopolitical realities.

The Key Questions

1. Should we respond to e-threats? Should we accept the status quo, and minimize near-term costs by accepting growing vulnerability, or begin reducing vulnerability?
2. If we respond, what is the path? How should we address interconnect-wide interdependence, and how should we proceed with implementation?
3. If we respond, who should be involved? Who should take responsibility to define the path, and implement it?
4. How broad should our response be? Should both GMD and EMP be included?

The Response: Consensus Recommendations

1. Should we respond? A common theme of the summit deliberations, broadly accepted in all presentations and discussions, was that the risks associated with severe e-threats are serious, and it is time to begin taking positive actions to protect critical infrastructures.

2. What is the path? The broad consensus of summit presenters and other delegates was that we need to establish interconnect-wide standards and plans. For implementation, we should begin working aggressively to validate and implement specific protection measures, while also pursuing expanded modeling, priority assessment, and planning. More specifically:

a. Define and apply interconnect-wide standards and protection plans.—We should define and apply applicable interconnect-wide e-threat protection standards, through regulatory or other means, and develop implementation plans that include prioritized protection for critical assets.

b. Pursue two paths to implementation.—

1. Validate and implement specific, cost effective protection measures.

We should thoroughly evaluate protective measures to validate that they support the e-threat standards, including both procedural and hardware-based measures (e.g., transformer or other hardware design upgrades, current blockers, series capacitance and power substation IEMI protection).

If expectations for high effectiveness and low-cost hardware-based protection can be tested and demonstrated, this will become a core approach to mitigation, beginning with development of interconnect-wide protection planning.

2. Prioritize scope and timing of protective measures by expanded hardware and interconnect-wide modeling, prioritization, and data collection.

We should also pursue a path of data collection, hardware vulnerability modeling and grid impact modeling, and define critical, high-value asset protection priorities. This process will guide and prioritize cost-effective implementation measures. It will be even more vital in those cases where more expensive measures are needed.

3. Who should be involved? The sense of summit presenters and delegates was that assembling and implementing a plan for e-threat protection will require the broadest possible participation among government agencies, commercial power suppliers, insurance companies and other stakeholders, each contributing in its own domain of authority and expertise. A common theme of all the discussions: The need to work toward international partnerships in developing these plans.

4. Addressing EMP and IEMI: How broad should our scope be? These recommendations, it became clear, will be essential for both aspects of e-threats, both natural—Severe Space Weather, and malicious—IEMI and EMP. In fact, another common theme at the summit was that, in focusing on space weather, there has been insufficient attention given to the needs for protection against malicious EMP and IEMI threats. In this regard, all the security-related speakers were quite clear: Security forces cannot perform their National security and protection mission with-

out the partnership of commercial power suppliers, who will need to "expand their resilience into a new hazard environment." The hope that the government could handle either the natural or malicious threat domain on its own was rejected, with the clearest articulation of this reality coming from speakers who represented the responsible government departments and agencies.

This summary of summit consensus-based themes and recommendations reflects many detailed comments made in the presentations and discussions during summit events. I would welcome the opportunity to discuss any of these points in greater detail.

I should note that there appear to be no significant technical or financial barriers to mitigating this threat—the technologies needed are well understood, and the cost—based on both government estimates and recent corporate experience—is quite low, even in comparison with just existing logistics and maintenance budgets for affected equipment. Rather, the primary needs seem to be for education to increase awareness and willingness to address the problem, and for coordination to address the complex government and corporate administrative structures of even the most critical infrastructures.

This concludes my prepared testimony, and I'd be happy to answer any questions.

Mr. LUNGREN. Thank you very much, Dr. Beck. Again, good to have you back here.

Mr. BECK. Thank you.

Mr. LUNGREN. Maybe I will follow along on Congressman Long's earlier statements. There have been some generalized statements about how there is no significant financial barrier—so I guess the question I would ask is this, if there is no significant technical or financial barriers to mitigating this threat, what is the difficulty?

I am not trying to cast aspersions on the industry at all. I think the industry is, by and large, is one of the primary providers of the standard of living we have today and the way of life we have today. The consistency and reliability of the systems is actually remarkable when you think about it. It goes to the question—you turn the light switch on. It only comes to your attention if it doesn't go on when you turn that light switch.

We take it for granted. That is the way we live. That is what we rely on. That is our expectation. Something so essential to our needs would seem to require heightened attention. If it is as apparent as many have suggested and the studies have concluded that we have significant vulnerabilities, either natural or man-made, the question would be, why aren't we taking these steps?

My partial is—and I would ask yours—that we haven't raised the awareness to the level that the public would accept rate increases that would allow for the capitalization of the technical fixes that are necessary. So that is one of the obligations that I think we have.

But we have talked in general terms about how we have got technical fixes and how we have technical fixes within our fiscal grasp, I guess I would say. Can you put some meat on the bones on that? Can you give us some idea from the work that was done at these conferences to suggest the ballpark that Mr. Long asked about? Or is there some other gauge that you can give us that would show the appropriateness of applying these fixes to the current system?

Mr. BECK. Yes, I think I can do that. Going back to the original question is: What is the disconnect or why don't we know about this? I think part of it is just a question of human nature. It is that there are—when you have certain events that don't happen very

often and they are things that we don't see, then we fail to plan for those.

When we designed the grid and built it over the last 100 years, there wasn't the consistent level of disruption from solar storms. In other words, lower-level solar storms do happen all the time. Any time the aurora borealis that you see it—that is, in effect, a geomagnetic disturbance. So there are low-level events all the time. So the grid was able to deal with those. We haven't see the very high-level events and when the grid wasn't designed for that purpose, there is a certain inertia both mental and physical that comes in with saying we designed the grid. I know how this works. We have optimized it. We are happy with its performance. Trying to move beyond that sometimes is difficult.

Going to the question of costs—and you mentioned capitalization, which I think is important. So taking the EMP Commission report estimate of about a billion dollars for mitigation for transformers that both Mr. Wales and Mr. McClelland talked about. You take that the step further and say, well, the transformer is a 30- to 50-year asset. They have a long lifetime, as opposed to other components on the grid, electronics and stuff that are replaced much more frequently.

So if you have a 30-year asset and a billion dollars, you are talking about $33 million or so a year. That breaks down to, you know, a few cents per citizen that we would have to pay. So your job and your two concerns, especially on this panel, are providing for security and protection of the public; but also you have a fiscal responsibility that you don't want to stick the citizens with an enormous bill that doesn't make sense. But when you run some of those numbers, especially when you are talking about the transformers and the fact that those assets last for a long time, you can spread those costs out and make them nearly insignificant to the ratepayer or the taxpayer.

Mr. LUNGREN. Those are your words. I can never say that there is an insignificant cost to taxpayers, but I understand the point that you make.

The gentlelady from New York is recognized.

Ms. CLARKE. Thank you very much, Mr. Chairman. Let me first say, Mr. Chairman, or ask if we could ask for unanimous consent that the EIS summit three London report, a summary of the third Electric Infrastructure Security summit held this summer in London be placed in the record.

Mr. LUNGREN. Without objection.*

Ms. CLARKE. I think its findings and conclusions will benefit the record of this hearing.

Dr. Beck, in your recent London conference, there were representatives from business and industry, in addition to governments. Can you describe the conversations and discussions about how the insurance industry is viewing EMP—excuse me—and the geomagnetic disturbances in the electric industry?

Mr. BECK. Yes. This was one of the significant new or differences—thankful one—between the prior conferences that we

*The information has been retained in committee files and is available at *http://www.eissummit.com/images/upload/conf/media/EISS%20III%20London%20Report.pdf.*

have had. So this was our third summit. The first summit in London was pretty much a government-only event and the second one—and you know this very well, Ms. Clarke—we had some expanded participation. We had a half-day where we had industry roundtables and we talked to the electric grid operators.

But Lloyd's of London, for example, 2010, did a report on space weather. So they had been reading the same reports, and so we had a panel at the summit and you can see a lot of the highlights of that in the report that you just referenced. So the interest is there that Lloyd's insures not just the assets directly, but we talked about earlier, the economic disruption overall of a power outage.

Joe McClelland talked about the $2 billion estimate for the Quebec outage. In the 2003 northeast blackout, not a GMD event, but still instructive because it was a power outage of 1–3 days, depending on where you were in that blackout zone. The after-action report was about $14 billion in societal costs.

So when an insurance company, whether they are insuring an electric grid operator and his assets or a major power consumer that is manufacturing or any other major player that has insurance, when effects like geomagnetic disturbance impact electric grid and the continuous supply of electricity, especially for high-precision manufacturing that really rely on that, there are insurance effects. So the insurance companies looked at this. They said, we think that we need to take a deeper dive.

You know, they didn't come back with any conclusions. We know what GMD costs. We are ready to have a GMD insurance package. They are not there yet, but I would recommend to the members and staff that the Lloyd's report would help to give some of those—put the meat on the bones, as Mr. Lungren put it.

Ms. CLARKE. Is the council proposing international standards for EMP and the geomagnetic disturbance mitigation? Who would oversee such an effort?

Mr. BECK. The council acts as a host to the discussion, so we are summarizing the discussions and recommendations. So I wouldn't say that we are proposing international standards, but those were called for by many of the members there.

So a lot of the, you know, the sophisticated electric grids are located in North America and Europe, northern Europe. So that was the bulk of the participants there and so the grids there have some interconnection. I mean, the grid doesn't just end, you know, at the border of France, and a brand new grid in Spain. There is some crosstalk there, like we have across State lines here. So there is interest there to say, well, we are all, you know, we all have a connection, just like we all have a connection here in the United States to each other.

So a standard or goal to be set for reliability and operation under a geomagnetic disturbance or protection modalities for EMP—the individual operators recognize that a standard that they could look to would be very helpful. Because otherwise, they, you know, look at, well, what does the threat mean and I will do my best. I will give my best engineering judgment to apply that to my section of the grid. But in an interconnected system, you know, you always have the question of, well, what if I do something and the guy next

to me does nothing? Is that worth the investment? Because I am still vulnerable and I don't have any control over that grid next to me.

So that was the point where international standards—or in the United States, National standards, or I guess it is a bit broader, because we include Canada and parts of Mexico here—but those types of standards so that everyone has some common goal and common understanding of the issue. Everyone suggested that that was very important.

Mr. LUNGREN. Thank you very much. I guess Mr. Long has gone.

So I thank you for your testimony, Mr. Beck. Once again, thank you for your participation on this committee in your major staff positions. Congratulations on the Council's work.

I thank you and all the other witnesses for the valuable testimony and the Members for their questions. The Members of the committee may have some additional questions, as you know, for you and the other witnesses. We will ask you to respond to these in writing. The hearing record will be held open for 10 days. The subcommittee stands adjourned.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM RANKING MEMBER YVETTE D. CLARKE FOR JOSEPH MCCLELLAND

Question 1. Are there any areas—in infrastructure, programs, or research—that seem urgently in need of attention regarding a Geomagnetic Disturbance threat?

If you could affect one change in current arrangements for managing the risks of severe space weather and geomagnetic disturbance events, what would that be?

In other words, what development in the current system of space weather risk management would yield the greatest benefit with the least cost?

Answer. Yesterday, the Commission issued a proposal to address the impacts of GMD on the electric grid. This proposal stems from the technical conference held by the Commission on April 30 of this year, which explored the risks and impacts from geomagnetically-induced currents to transformers and other equipment on the bulk power system, as well as options for addressing or mitigating the risks and impacts.

In the proposed rule discussed above, the Commission proposes to direct the North American Electric Reliability Corporation (NERC) to submit for approval Reliability Standards that address the impact of geomagnetic disturbances (GMD) on the reliable operation of the Bulk-Power System. The Commission proposes to do this in two stages. In the first stage, the Commission proposes to direct NERC to file, within 90 days of the effective date of a final rule in this proceeding, one or more Reliability Standards that require owners and operators of the Bulk-Power System to develop and implement operational procedures to mitigate the effects of GMDs consistent with the reliable operation of the Bulk-Power System. In the second stage, the Commission proposes to direct NERC to file, within 6 months of the effective date of a final rule in this proceeding, one or more Reliability Standards that require owners and operators of the Bulk-Power System to conduct initial and on-going assessments of the potential impact of GMDs on Bulk-Power System equipment and the Bulk-Power System as a whole. Based on those assessments, the Reliability Standards would require owners and operators to develop and implement a plan so that instability, uncontrolled separation, or cascading failures of the Bulk-Power System, caused by damage to critical or vulnerable Bulk-Power System equipment, or otherwise, will not occur as a result of a GMD. This plan cannot be limited to operational procedures or enhanced training alone, but should, subject to the needs indentified in the assessments, contain strategies for protecting against the potential impact of GMDs based on factors such as the age, condition, technical specifications, or location of specific equipment. These strategies could include automatically blocking geomagnetically-induced currents from entering the Bulk-Power System, instituting specification requirements for new equipment, inventory management, and isolating certain equipment that is not cost-effective to retrofit. This second stage would be implemented in phases, focusing first on the most critical Bulk-Power System assets.

Current GMD forecasting methods provide limited time for operators to react once a GMD warning is issued. I am concerned with the short period of time to react to a GMD event and the potential consequences of not reacting fast enough. The Commission's proposed rule would first ensure that appropriate operational procedures to mitigate GMD are in place in a relatively short time frame, then turn to implementation of a plan so that instability, uncontrolled separation, or cascading failures of the Bulk-Power System, caused by damage to critical or vulnerable Bulk-Power System equipment, or otherwise, will not occur as a result of a GMD.

Question 2. What is FERC currently doing to address EMP and Geomagnetic Disturbance threats?

Answer. See question 1.

Question 3. As I understand, there are two risks that result from the introduction of ground-induced currents from a geomagnetic disturbance to the bulk power sys-

tem: (1) Damage to the bulk power system assets, like transformers, and (2) Loss of reactive power support, which could lead to voltage instability.

How does the Commission oversee that operators of the grid address these risks in a responsible and comprehensive way?

Answer. The proposed rule issued yesterday would take short-term and long-term steps to protect the electric grid from a geomagnetic disturbance. The Commission's proposed two-phase approach recognizes this difference by focusing first on the development of Reliability Standards requiring operational procedures in a relatively short time frame. The Commission proposes to give NERC and owners and operators of the Bulk-Power System more time to perform, in the second phase, initial and on-going assessments and, based on those assessments, to develop and implement a plan so that instability, uncontrolled separation, or cascading failures of the Bulk-Power System, caused by damage to critical or vulnerable Bulk-Power System equipment, or otherwise, will not occur as a result of a GMD.

Question 4. NERC has outlined several recommendations in their GMD report—what is the Commission's process or approach to implement or facilitate their recommendations?

Answer. In addition to proposing that NERC develop Reliability Standards that require operational procedures during the first phase, the Commission's proposal also would accept aspects of the "Initial Actions" proposal set forth in NERC's post-Technical Conference comments.

Question 5. Do you think each utility should have spare transformers to be prepared in case of a solar Geomagnetic Disturbance event? Who should pay for these spare transformers and what is the cost?

Answer. There should be some spare transformers for the Bulk-Power System to recover from geomagnetic disturbances as well as from many other risks (e.g., lightning, voltage surges, and fault conditions). However, spare transformers alone are not sufficient to address GMDs. During a GMD, geomagnetically-induced currents flowing through transformers cause those transformers to operate in a manner for which they are not designed (typically described as half-cycle saturation). As question 3 above notes, two results of this abnormal operation are equipment damage and loss of reactive power support. In addition, the affected transformers introduce disruptive harmonics into the power grid. The harmonics can be thought of as "noise" on the power grid. This "noise" can cause switching equipment to misoperate (opening or closing when they should not) and other equipment damage, most notably damage to generators. The risks from loss of reactive power support and from harmonics would not be mitigated by spare transformers. Steps such as preventing half-cycle saturation from occurring would be necessary in order to avoid these risks.

Maintaining spare equipment is a time-tested method of improving electric reliability, and typically is a legitimate cost of providing service. The cost of a spare extra-high voltage (EHV, typically over 300kV) transformer varies depending on many design features, including the operating voltages and the power rating of the transformer. However, a ball-park range would be $10 million to $15 million for a typical three-phase EHV transformer.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN FOR BRANDON WALES

Question 1. What is DHS' 90-day, 1-year, and 5-year plan to address the threat posed by EMP?

Answer. Signed March 30, 2011, Presidential Policy Directive–8 (PPD–8) seeks to strengthen security and resilience through systematic preparation for threats that pose the greatest risk to the Nation. As a part of PPD–8 implementation and from a Whole Community approach, the Federal Emergency Management Agency (FEMA) is leading the development of a National Planning System (NPS) that integrates planning across all levels of Government and with the private and non-profit sectors around key capabilities to address all-hazard threats. This work will result in a set of focused planning documents that support the effective delivery of core capabilities across the Whole Community to address all-hazards, including those posed by Electromagnetic Pulses (EMP) due to space weather or nuclear incidents.

As a component of PPD–8, the Federal Interagency Operational Plan (FIOP)-Response is an all-hazards plan that describes how the Federal Government supports State, local, Tribal, territorial, and insular area efforts to save lives, protect property and the environment, and meet basic human needs following an emergency or disaster, such as EMP impacts. The FIOP-Response delineates Federal response roles and responsibilities; identifies critical tasks, resources, and sourcing requirements necessary to deliver the Response Core Capabilities; and coordinates statutory authorities across governments.

While this plan is based on a no-notice catastrophic incident that spans multiple regions and States, it will also contain incident-specific annexes as required. For example, FEMA has scheduled development of a "Long-Term Power Outage Annex" for fiscal year 2014. The FIOP-Response will also be updated 18 months after initial signature with quadrennial re-writes thereafter.

Question 2. The Department of Homeland Security does not include the threat of EMP attack in its 15 National Disaster scenarios. Why not?

How is DHS protecting the homeland against EMP? Is it enough?

Answer. Under Presidential Policy Directive–8 (PPD–8), the 15 National Planning Scenarios were replaced by a new National Preparedness System based on the Strategic National Risk Assessment which identified incidents that posed the greatest threat to the Nation. Electromagnetic radiation from space weather was included as a National-level event that could test the Nation's preparednesss. PPD–8 includes five integrated National planning frameworks and interagency operational plans. As stated under the response to Question No. 1, the Federal Interagency Operational Plan (FIOP)-Response is a component of PPD–8. The FIOP-Response is an all-hazards plan that describes how the Federal Government supports State, local, Tribal, territorial, and insular area efforts to save lives, protect property and the environment, and meet basic human needs following an emergency or disaster, such as those with EMP threats. While this plan is based on a no-notice catastrophic incident that spans multiple regions and States, it will also contain incident-specific annexes as required. For example, FEMA has scheduled development of a "Long-Term Power Outage Annex" for fiscal year 2014. The FIOP-Response will also be updated 18 months after initial signature with quadrennial re-writes thereafter.

Question 3. By virtue of how our economy is structured, most electric and other critical infrastructure is privately owned. How do you overcome the challenge of convincing private industry to make the capital investments required to secure the electric grid?

Answer. The Department of Homeland Security (DHS) works with industry in a number of ways to promote appropriate security investments. The National Infrastructure Simulation and Analysis Center (NISAC) prepares and shares analyses of critical infrastructure, including their interdependencies, vulnerabilities, consequences, and other complexities, under the direction of the Office of Infrastructure Protection's Infrastructure Analysis and Strategy Division.

Additionally, DHS coordinates unclassified and classified briefings and workshops for industry and works to analyze their vulnerabilities and demonstrate potential impacts and costs if those vulnerabilities are left unaddressed. To facilitate discussions of this type, DHS administers the Critical Infrastructure Private Sector Clearance Program (PSCP). The PSCP sponsors clearances for private-sector partners that are responsible for critical infrastructure protection but would not otherwise be eligible for a clearance. Through these activities, private-sector partners become better positioned to make more informed security investments.

Question 4. How much do you or does your agency rely upon data from NOAA's ACE satellite for warnings about naturally-occurring EMPs?

Question 5. Are you aware that this satellite is well past its expected lifetime, and already operating at a severely diminished capacity?

Answer. The Federal Emergency Management Agency (FEMA) relies on space weather information and warnings from NOAA's Space Weather Prediction Center (SWPC), which uses data from the ACE satellite. FEMA benefits from the SWPC's real-time monitoring and forecasting of solar and geophysical events, which could impact satellites, power grids, communications, navigations, and other systems. FEMA is aware of the ACE satellite's current state and the fiscal year 2014 mission planned to replace it.

Question 6. Are you aware of NOAA's plans and time line to replace the failing ACE spacecraft with the refurbished DSCOVR spacecraft?

And, the naturally-occurring EMP warning needs of your agency?

Answer. The Federal Emergency Management Agency (FEMA) is aware of NOAA's plans and time line to replace the ACE spacecraft with DSCOVR. FEMA liaisons regularly communicate with the National Weather Service and, more specifically, the Space Weather Prediction Center (SWPC). FEMA relies on SWPC's real-time monitoring and forecasting of solar and geophysical events, which could impact satellites, power grids, communications, navigations, and other systems. NOAA and the SWPC have communicated to FEMA the ACE satellite's vulnerabilities and their plans to address it.

Question 7. How would your agency's ability to meet its mission requirements be effected if ACE were to completely fail before DSCOVR is operationally on-orbit?

Answer. Failure of the ACE satellite would only impact the Federal Emergency Management Agency's (FEMA) actual operations if such failure led to delays in crit-

ical information or warnings. To respond to a space weather event, FEMA would implement its response plans in accordance with the Stafford Act and the National Response Framework. Delays in space weather-related information or warnings could theoretically delay implementation of preventative or early response actions.

QUESTIONS FROM RANKING MEMBER YVETTE D. CLARKE FOR BRANDON WALES

Question 1a. I understand that your office includes analysts from the Office of Infrastructure Protection and the Office of Intelligence and Analysis.

Could you outline for us how HITRAC creates actionable risk-informed analysis for EMP or geomagnetic disturbance threats?

Question 1b. In other words, what kind of input information, in generally do you use in the risk analysis of geomagnetic disturbances or EMP threats?

Question 1c. To whom would you report this analysis for action on EMP-specific threats?

Answer. There are several reports that analyze the threat posed by electromagnetic pulse (EMP) and geomagnetic disturbances. The 2011 and 2012 National Risk Profiles identify what sectors are most at-risk from geomagnetic disturbances and what systems are in place to warn of an impending space weather event. A 2010 HITRAC study performed by the National Infrastructure Simulation and Analysis Center analyzed the impact of EMP on extra high-voltage power transformers. Additionally, a 2010 National-Level Exercise looking at the effects of an improvised nuclear device touched upon the impacts of an EMP from a nuclear attack. At this time, the Department of Homeland Security has not performed a comprehensive study analyzing how different inputs would change how critical infrastructure is affected.

Question 2. I see that within Infrastructure Protection, risk analysis, modeling, simulation/analysis and incident planning and response are bundled together as part of an overall package for Critical Infrastructure and Key Resources protection.

Are EMP and geomagnetic disturbance considered a discreet separate threat or are they combined in an all-hazards analysis approach?

Answer. Electromagnetic pulse (EMP) and geomagnetic disturbance are considered discreet and separate threats. The 2011 and 2012 National Risk Profiles have separate Space Weather sections. A National Infrastructure Simulation and Analysis Center report highlighted threats from EMP and geomagnetic disturbance and considered them to be separate from other hazards. Also, studies analyzing the impacts from the detonation of a nuclear device include analysis on the effects from the resulting EMP.

Question 3. I understand that within DHS, under the National Infrastructure Protection Plan, the Office of Infrastructure Protection oversees three key elements of the Risk Management Frameworks:

i. Identification of critical infrastructure assets and systems;
ii. Risk assessment based on event consequences, facility or system vulnerabilities, and known or probable threats; and
iii. Prioritization of CIKR protection activities based on risk.

How is the U.S. grid identified or described in this framework (or is it identified), what are the risk assessment levels, and what prioritization is listed for EMPs and geomagnetic disturbances threats to the grid?

Answer. Electric power is identified as a subsector of the energy sector and includes power plants and the electric grid. Infrastructure, including the electric grid, is not prioritized based on electromagnetic pulse or geomagnetic disturbances, but rather is based on the National Critical Infrastructure Prioritization Program (NCIPP) outlined in the National Infrastructure Protection Plan. NCIPP identifies Nationally significant critical assets and systems to enhance decision making related to critical infrastructure protection. Critical infrastructure identified includes those that, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to National well-being and governance capacity.

Question 4. Do you think each utility should have spare transformers to be prepared in case of a solar geomagnetic disturbance event? Who should pay for these spare transformers and what is the cost?

Answer. The Department has not taken a position on whether utilities should have spare transformers and if so who should bear the cost. The Department recognizes that redundancy can add resilience to infrastructure systems. In the event of a major electromagnetic pulse or geomagnetic disturbance, the current quantity of spare transformers could be insufficient if enough transformers were physically damaged. There is no regulatory requirement that utility companies maintain spare transformers, though some currently do at their own expense.

More needs to be learned about the effects of large GMD on major transformers. Stockpiling spares would be costly and not easy to do generically since transformer needs vary and their massive weight make them difficult to move.

The DHS Science & Technology Directorate has worked with industry to jointly develop a prototype extra high-voltage (EHV) transformer that is easier to transport and quicker to energize than conventional EHV transformers to enable rapid recovery from such events. Known as the Recovery Transformer (RecX), a pilot demonstration was successfully conducted in March 2012 in which the RecX was transported, installed, and energized in less than 1 week. The RecX is currently operational in the grid for a 1-year monitoring period. DHS S&T and RecX project partners are working on transition plans for RecX with various stakeholders, including Federal partners & private industry.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN FOR MICHAEL A. AIMONE

Question 1. How has the U.S. military sought to protect its satellites, weapons, and other equipment against an EMP attack?

Since many U.S. military facilities are dependent on the U.S. electric grid, what steps has the U.S. military taken to protect its capabilities in the event of an EMP attack? Are these steps relevant to the protection of the U.S. electric grid?

Answer. Since the 1960s the Department of Defense (DoD) has been conducting on-going research focused on defining the nature of the electromagnetic pulse (EMP) threat, its effect on systems, and ways to protect both military assets and infrastructure against EMP threats. Mission-critical military systems are required to be hardened against the High-Altitude EMP (HEMP) threat specified in MIL–STD–2169, the HEMP threat environment, in accordance with DoDI 3150.09, CBRN Survivability Policy. Although there are several types of EMPs, HEMP is considered to be the primary threat to military assets. Military standards for protecting strategic C4I ground-mobile systems, fixed facilities, and aircraft have been enacted and standards for protecting maritime assets against nuclear HEMP and satellites against other nuclear weapon effects environments are currently being developed. Transportable and mobile military systems are powered by mobile generators which are hardened against the HEMP threat. Similarly, military ground (fixed) facilities performing mission-critical functions use EMP-hardened commercial power. If the commercial power source is unavailable (e.g. due to power grid outages), these facilities rely on HEMP-hardened backup generators.

Many EMP hardness protection methods and commercially available protection devices are generally applicable for use in protecting elements of the U.S. electric grid such as the universal Supervisory Control and Data Acquisition (SCADA) equipment which may be susceptible to and should be hardened against early-time HEMP. SCADA is a type of industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world. SCADA is critical to normal functioning of the grid. In addition, due to the unique nature of the grid, such as transmission of electric power over very long transmission lines containing numerous transformers and other high-voltage devices, the grid may be vulnerable to late-time effects of HEMP. The DoD's DTRA recently have been conducted two experimental research efforts at the Department of Energy's Idaho National Laboratory to define the nature and extent of late-time EMP effects on typical elements of the power grid and on protecting the grid against late-time HEMP.

DoD does not harden all military systems, but just those systems deemed to be mission-critical that are expected to operate in a nuclear environment. DoDI 3150.09, CBRN Survivability Policy, is the tool used to identify those systems.

Question 2. Have the effects of an EMP attack, solar storm, or other long-term disruption (such as the derecho) on the civilian recovery sectors (i.e., hospitals, police, fire departments) been adequately investigated and planned for? What about similar impacts on DoD assets and missions?

Answer. Lessons-learned from DoD hardening is applicable to civilian infrastructure, but the civilian infrastructure is not in DoD's mission space. DoD plans to operate mission-critical systems as necessary without civilian infrastructure. It is probably cost-prohibitive to harden all civilian infrastructure but it might be cost-effective to harden critical nodes such as SCADA. Overall, DoD has no responsibility to harden civilian infrastructure.

Based on results of past studies and limited HEMP testing, the effects of an EMP attack on the civilian recovery sectors (emergency services) may not, in some areas, be adequately planned for. The Congressional Commission on EMP Attack on the U.S. conducted a HEMP effects study on the emergency services sector in 2002–2003. The study, based on site visits, analyses, and limited testing, illustrated the

effects of plausible HEMP threats and scenarios on typical components of the sector including a preliminary vulnerability assessment of HEMP events on Public Safety Answering Points (PSAPS). While the PSAP facilities visited had lightning protection, they were not directly protected against the effects of HEMP. Limited HEMP testing was performed on actual (or similar) components in PSAP facilities and equipment used by the emergency services sector such as computers, hand-held radios, and a police vehicle.

In general, unhardened DoD assets and computer networks are vulnerable to high-level HEMP (e.g. <10kV/m). To the extent that DoD relies on unhardened assets to perform specific missions, these missions are at risk. Strategic missions, in general, rely on HEMP-protected assets. Non-strategic missions may rely on unhardened assets.

Question 3a. While the term "energy security" has been in vogue amongst policymakers, it is mainly used in terms of sustainability and alternative energy sources (i.e. freedom from foreign oil) rather than resiliency and counter-terrorism applications. Have the Departments of Defense and Homeland Security been directing their regulatory attention more towards these issues rather than securing its energy sources, particularly electricity, against the effects of a long-term disruption?

Answer. The Department of Defense defers to the Department of Homeland Security to provide the subcommittee with a description of the status of the U.S. Government's efforts to plan for EMP, solar storm, or long-term disruption effects on the civilian recovery sectors. The Department is largely in a supporting role to the lead civilian authorities in any event to mitigate the consequences of or remediate after an EMP attack, solar storm, or long-term disruption event in the homeland. DHS is the lead agency for National Critical Infrastructure Protection and leads the U.S. Government's contingency response plan efforts to mitigate the consequences of or remediate after an EMP attack, solar storm, or long-term disruption event. However, the Department of Defense is a significant stakeholder, and the Department's ability to perform its National security functions is largely dependent upon the reliability and resilience of the commercial electric power grid.

Question 3b. If so, are there plans to broaden your interpretation of energy security?

Answer. The Department is pursuing comprehensive energy security strategies through the Energy Grid Security Executive Council (EGSEC) co-chaired by the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs and the Deputy Under Secretary of Defense for Installations and Enviromnent. The council is working to improve the security, adequacy, and reliability of electricity supplies and related infrastructure key to the continuity of critical defense missions. The EGSEC works closely with the Departments of Energy and Homeland Security, along with private-sector partners.

Congress has issued a broader interpretation of energy security in Title 10, Section 2924, which the Department of Defense believes is a good start in defining energy security. This definition includes, "having assured access to reliable supplies of energy and the ability to protect and deliver sufficient energy to meet mission-essential requirements."

The Department's current facility energy strategy includes enhancing the energy security of DoD installations. The DoD Annual Energy Management Report (AEMR) for fiscal year 2011 describes the facility energy strategy and includes a chapter describing energy security activities for DoD installations (see Chapter 5 in the fiscal year 2011 AEMR).

The Department's Installation Energy Management policy in DoDI 4170.11 includes a broader interpretation of energy security (see Enclosure 3, Section 3c. in DoDI 4170.11). The Department is in the process of updating this policy to further broaden the interpretation of energy security for fixed installations.

Question 4. How is DoD using the inter-agency system to share its intelligence gathering and modeling capability with DHS and its partners to better understand potential EMP threats? Is DoD taking advantage of FERC, DoE, and DHS' planning and response capabilities?

Answer. DoD is using established intelligence community (IC) processes and mechanisms to share the results of its intelligence gathering on EMP threats with DoE, DHS, and other partners.

DoD components who are also elements within the IC, such as DIA and (by extension) the Service Intelligence Centers (NASIC, NGIC, aNI) produce assessments on different aspects of EMP threats. Completed intelligence analysis on EMP threats is shared directly in collaborative efforts and made broadly available through Intelink and other collaboration tools.

As a part of a 65-year partnership on nuclear weapons, DoD collaborates closely with DoE and its key laboratories to engage in research of common interest on EMP

and other nuclear-related effects. DoD relies on the deep technical expertise resident at DoE labs to supplement DoD's weapon-specific expertise. Each DoE National lab also has a field intelligence element that is responsible for coordinating IC-related activities at the lab and assisting with sharing of intelligence products.

DoD collaborates with DHS on EMP threats as just one of many areas of cooperation on homeland security. DHS has an extensive liaison relationship with NSA and an operational coordination relationship with USNORTHCOM.

Those organizations across DoD, DoE, and DHS that deal with EMP threats are well-connected at both the leadership and rank-and-file level, ensuring robust intelligence sharing.

Question 5. There is a DHS, DoD, and Department of Energy initiative to address EMP preparedness and grid reliability issues with private owners and operators. When was this partnership developed and what is its current status?

Answer. The Energy Sector Public-Private Partnership (ES3P) initiative was established in March 2012 by the Department of Energy, the Department of Homeland Security, and the Department of Defense to engage sector stakeholders to understand, and where necessary, improve the energy surety (reliability, security, and resiliency) of infrastructure which supports National security missions. ES3P does not specifically focus on EMP-related events.

The goal for the ES3P Joint Working Group (ES3PJWG) is to pull together the existing roles, responsibilities, and activities which currently support the Nation's public and privately-owned energy systems. Increasing efficiency through integrated activities across larger, interconnected systems should improve energy surety. This public-private partnership is intended to be a multi-stage initiative. Specifically, this initiative is designed to take a regional approach to the energy surety of critical infrastructure and installations.

Currently, ES3P is engaged in "The National Capital Region Initiative," which focuses on DoD mission assurance in the National Capital Region (NCR). Specifically, this initiative addresses the energy surety of DoD installations, critical infrastructure, and Defense Industrial Base (DIE) facilities that perform or support DoD critical missions in the NCR. Best practices established in the first stage will be applied in other National security mission areas in follow on stages.

QUESTIONS FROM RANKING MEMBER YVETTE D. CLARKE FOR CHRIS BECK

Question 1. In your recent London Conference, there were representatives from business and industry, in addition to governments.

Could you describe the conversations and discussions about how the insurance industry is viewing EMP and geomagnetic disturbances in the electric industry?

Answer. The insurance industry is now becoming very active in this area. While high-impact, low-frequency (HILF) risks are difficult to handle with traditional, actuarial-style risk analysis, the industry recognizes that the serious consequences resulting from a large EMP/GMD event means that mitigation actions must be taken. Insurance companies are very exposed to space weather costs, with the primary expense likely to be contingent business interruption costs, in addition to the need to cover direct costs of insured equipment that would be damaged. The EIS Summit III report, which I supplied to the committee as an addendum to my testimony summarizes the insurance industry discussions (see pages 30–35). In addition, Lloyd's of London issued a report on Space Weather in 2010, which I am also attaching for your convenience.*

Question 2. Is the council proposing international standards for EMP and geomagnetic disturbance mitigation? Who would oversee such an effort?

Answer. One of the broad, consensus recommendations that emerged during several of the discussions at our third Electric Infrastructure Security Summit on May 14–15, 2012, was the need for standards for electrical transformers and other electrical devices on electric grids throughout the world. Standards, whether National or international, are necessary to ensure some basic level of protection. Sweden, for example, has set a standard for the amount of geomagnetically-induced current (GIC) that all transformers on their grid must meet. Such standards allow electric grid owners and operators to procure equipment designed with GMD hazards taken into account. Without a standard, individual companies are doing the best they can, but this approach yields highly varied levels of protection. Because grids are all interconnected, "weak links" are present that put the entire system at risk. There are a number of approaches to begin developing such standards, including both rel-

*The information has been retained in committee files and is available at *http://www.lloyds.com/lloyds/press-centre/press-releases/2010/11//media/lloyds/reports/360/360%20space%20weather/7311__lloyds__360__space%20weather__03.pdf.*

evant Government agency efforts and input from industry on best practices and experiences. Whatever the choice, it will be important to have it clearly defined, and designed to accept input from all relevant stakeholders and experts.

Question 3. Electrical systems for countries are structured in different ways, for example we know that the system in S. Africa will need GMD protection that may vary from another country, and mitigation for GMD will have to be tailored to their needs.

How do you plan to propose international standards if there are so many discreet and individual systems that will need specialized mitigation?

Answer. The most fundamental standards required will refer to maximum tolerable off-nominal grid conditions. In the case of GMD, this would mean a standard that would limit maximum GIC flows in extra-high-voltage (EHV) transformers or provide corresponding GIC withstand ratings in EHV transformers. Since these are transformer-specific approaches, they would be country- and system-independent. The country-unique effort would take place in implementing the GMD standard, just as it does for implementing other standards, as each country, or coordinated group of system operators, works to evaluate—for their system—which approaches to assuring those standards/limits are met are best-suited to different elements of their power grid.

Question 4. If commercial suppliers can produce mitigation devices that address protective strategies for expensive electrical equipment, then, what, in your opinion, is preventing them from marketing their products if their customers express a need for them?

Answer. There are now three companies in the process of starting to market devices such as GIC current-blockers to customers, along with an increasing and impressive body of test data, which is a critical need to build confidence in their use by the energy sector. This marketing process has been slow to start due to the lack of any widely applicable standard, either voluntarily self-imposed, or else externally mandated. Once such a standard becomes available, and is broadly accepted, marketing of such devices will rapidly accelerate.