BLACKOUT! ARE WE PREPARED TO MANAGE THE AFTERMATH OF A CYBERATTACK OR OTHER FAILURE OF THE ELECTRICAL GRID?

(114–39)

HEARING

BEFORE THE

SUBCOMMITTEE ON
ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND
EMERGENCY MANAGEMENT

OF THE

COMMITTEE ON
TRANSPORTATION AND
INFRASTRUCTURE
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

APRIL 14, 2016

Printed for the use of the
Committee on Transportation and Infrastructure

Available online at: http://www.gpo.gov/fdsys/browse/
committee.action?chamber=house&committee=transportation

U.S. GOVERNMENT PUBLISHING OFFICE

99–931 PDF WASHINGTON : 2016

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

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

BILL SHUSTER, Pennsylvania, *Chairman*

DON YOUNG, Alaska
JOHN J. DUNCAN, JR., Tennessee, *Vice Chair*
JOHN L. MICA, Florida
FRANK A. LOBIONDO, New Jersey
SAM GRAVES, Missouri
CANDICE S. MILLER, Michigan
DUNCAN HUNTER, California
ERIC A. "RICK" CRAWFORD, Arkansas
LOU BARLETTA, Pennsylvania
BLAKE FARENTHOLD, Texas
BOB GIBBS, Ohio
RICHARD L. HANNA, New York
DANIEL WEBSTER, Florida
JEFF DENHAM, California
REID J. RIBBLE, Wisconsin
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
SCOTT PERRY, Pennsylvania
RODNEY DAVIS, Illinois
MARK SANFORD, South Carolina
ROB WOODALL, Georgia
TODD ROKITA, Indiana
JOHN KATKO, New York
BRIAN BABIN, Texas
CRESENT HARDY, Nevada
RYAN A. COSTELLO, Pennsylvania
GARRET GRAVES, Louisiana
MIMI WALTERS, California
BARBARA COMSTOCK, Virginia
CARLOS CURBELO, Florida
DAVID ROUZER, North Carolina
LEE M. ZELDIN, New York
MIKE BOST, Illinois
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
JERROLD NADLER, New York
CORRINE BROWN, Florida
EDDIE BERNICE JOHNSON, Texas
ELIJAH E. CUMMINGS, Maryland
RICK LARSEN, Washington
MICHAEL E. CAPUANO, Massachusetts
GRACE F. NAPOLITANO, California
DANIEL LIPINSKI, Illinois
STEVE COHEN, Tennessee
ALBIO SIRES, New Jersey
DONNA F. EDWARDS, Maryland
JOHN GARAMENDI, California
ANDRÉ CARSON, Indiana
JANICE HAHN, California
RICHARD M. NOLAN, Minnesota
ANN KIRKPATRICK, Arizona
DINA TITUS, Nevada
SEAN PATRICK MALONEY, New York
ELIZABETH H. ESTY, Connecticut
LOIS FRANKEL, Florida
CHERI BUSTOS, Illinois
JARED HUFFMAN, California
JULIA BROWNLEY, California

SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND EMERGENCY MANAGEMENT

LOU BARLETTA, Pennsylvania, *Chairman*

ERIC A. "RICK" CRAWFORD, Arkansas
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
SCOTT PERRY, Pennsylvania
RYAN A. COSTELLO, Pennsylvania
BARBARA COMSTOCK, Virginia
CARLOS CURBELO, Florida
DAVID ROUZER, North Carolina
BILL SHUSTER, Pennsylvania *(Ex Officio)*
ANDRÉ CARSON, Indiana
ELEANOR HOLMES NORTON, District of Columbia
ALBIO SIRES, New Jersey
DONNA F. EDWARDS, Maryland
DINA TITUS, Nevada
PETER A. DEFAZIO, Oregon *(Ex Officio)*
VACANCY

CONTENTS

Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster Chairman	Washington, DC 20515	Peter A. DeFazio Ranking Member
[illegible]		[illegible]

April 8, 2016

SUMMARY OF SUBJECT MATTER

TO:	Members, Subcommittee on Economic Development, Public Buildings, and Emergency Management
FROM:	Staff, Subcommittee on Economic Development, Public Buildings, and Emergency Management
RE:	Subcommittee Hearing on "Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?"

PURPOSE

The Subcommittee on Economic Development, Public Buildings, and Emergency Management will meet on Thursday, April 14, 2016, at 10:00 a.m. in 2167 Rayburn House Office Building for a hearing titled "Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?" The purpose of the hearing is twofold:

1. To explore the risks, vulnerabilities and consequences of a prolonged, widespread power outage and understand the primary federal roles, authorities and resources available to help communities, particularly at the local level, manage the aftermath of such a disaster; and
2. To assess the efforts and coordination among the participants—public, private and non-profit—in the electrical power sector, including planning, preparedness and mitigation efforts, response and recovery capabilities, information sharing, and standards setting.

The Subcommittee will receive testimony from the Federal Emergency Management Agency (FEMA), the Department of Energy (DOE), the Department of Homeland Security's National Protection and Programs Directorate, the Congressional Research Service (CRS), the North American Electric Reliability Corporation (NERC), and a representative from the electrical industry.

V

BACKGROUND

The Elements of the Electrical System

The electric grid is one of the Nation's most critical infrastructures. The bulk power system is a large, complex, and robust system of networked generation facilities, transmission and distribution lines, transformers and substations, and control and communication technologies which together, bring power to American homes and businesses (see Attachment A).

The Roles of Federal Entities

Federal Emergency Management Agency (FEMA)

FEMA coordinates the federal government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror.

Department of Energy Office of Electricity Delivery and Energy Reliability

DOE serves as the sector specific lead agency for grid security. The Office of Electricity Delivery and Energy Reliability (OE) works to ensure that the Nation's energy delivery system is secure, resilient and reliable and develops new technologies to improve the infrastructure and the federal and state electricity policies and programs. OE also works to bolster the resiliency of the electric grid and assists with restoration when major energy supply interruptions occur.

The Fixing America's Surface Transportation Act, or the FAST Act (P.L. 114-94), amended the Federal Power Act (16 U.S.C. 824 *et seq.*) to: (i) require DOE to develop procedures to improve emergency preparedness for energy supply disruptions; (ii) authorize DOE to take measures to address Presidentially-declared grid security emergencies and protect the bulk power system or defend critical electric infrastructure; and (iii) require DOE to establish a strategic transformer reserve to store spare large power transformers and emergency mobile substations in strategically located facilities for use during emergencies.[1]

Department of Homeland Security (DHS)

DHS coordinates security information and preparedness for the Nation's critical infrastructure. The National Protection and Programs Directorate (NPPD) executes the Department's mission related to enhancing the resilience of the Nation's infrastructure against cyber and physical threats. NPPD collaborates with federal, state, local, tribal, territorial, international, and private-sector entities to maintain situational awareness of both physical and cyber events, share information about risks that may disrupt critical infrastructure, and build capabilities to reduce those risks. NPPD, through its cyber protection programs housed in the National Cybersecurity and Communications Integration Center (NCCIC), shares cyber threat and mitigation information with government, private sector, and academic partners drawing on its operators and analysts while ensuring continuity of national security and emergency preparedness communications.

[1] Conference Report 114-357 to accompany H.R. 22 FAST Act, December 1, 2015.

Federal Energy Regulatory Commission (FERC)

FERC oversees the development and enforcement of mandatory reliability standards for the bulk power system. With representatives of other federal and state agencies and the electric industry, FERC helps identify and address threats to energy infrastructure security. The Federal Power Act directs FERC to work with an independent Electric Reliability Organization (ERO) to develop reliability standards for the bulk power system. In 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the ERO.

Other Entities

North American Electric Reliability Corporation (NERC)

Pursuant to the Energy Policy Act of 2005, NERC develops and establishes consensus industry standards pursuant to an open and inclusive stakeholder process with FERC oversight and approval. NERC also regularly conducts outreach to and training for industry partners through assessments, exercises, webinars, and guidelines. In 2011, NERC facilitated the first-ever play exercise and executive tabletop discussion, or GridEx, for the Electricity Sub-sector in North America. NERC now holds a biennial distributed play exercise and executive tabletop discussion to exercise readiness, review plans, and explore policy decisions. On March 31, 2016, NERC released the findings of GridExIII held in November 2015 which "showed continued improvement to coordination, communication and emergency response actions to how industry would respond to a cyber or physical attack from previous exercises."

Electricity Subsector Coordinating Council (ESCC)

Formed in 2013, the ESCC is the principal liaison between the electric sector and the federal government for coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. Electric company CEOs and senior Administration officials from DOE, DHS, the White House, and the Federal Bureau of Investigation (FBI) meet regularly to focus primarily on three key areas: tools and technology, information flow, and incident response. The ESCC focuses on threat mitigation through preparation, prevention, response, and recovery.

Electricity Information Sharing and Analysis Center (E-ISAC)

The E-ISAC gathers information from electric industry participants about security-related events, disturbances, and off-normal occurrences within the Electricity Sub-sector and shares that information with key governmental entities. In turn, these governmental entities provide the E-ISAC with information regarding risks, threats, and warnings that the E-ISAC then disseminates throughout the Electricity Sub-sector.

For example, immediately after a 2013 sniper attack on the Pacific Gas and Electric's Metcalf substation, located in California, the E-ISAC alerted industry of the event and provided advice on steps to mitigate and protect against such attacks. In addition, the E-ISAC, DOE, FERC, DHS, and FBI conducted outreach to raise awareness of the event, inform industry of mitigation activities, and provide a forum for industry to meet with state, local, and federal authorities to discuss physical security concerns. This was an unprecedented public-private

partnership effort to address physical security concerns and involved U.S. and Canadian interests.

Threats to the Grid

Any of the grid elements can be damaged by natural events, such as severe storms or geomagnetic disturbances, as well as intentional, malicious events, such as cyber and physical security attacks. Incidents may disrupt the flow of power or reduce the reliability of the system. Several, if not all, of the other critical infrastructure sectors, are dependent on electric power. Simply put, a massive power outage could interfere with the everyday lives of millions of Americans.

Cyber Threats

The electric power industry has been making cybersecurity an increasing priority. The DHS reports that the energy sector is the target of more than 40 percent of all reported cyberattacks.[2] In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into industrial control systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[3]

The electric power industry is the only critical infrastructure industry with mandatory and enforceable cybersecurity standards. NERC as the designated ERO, worked with the electric power industry to develop Critical Infrastructure Protection (CIP) standards, which were approved by FERC in 2008, making them mandatory for bulk electric system owners and operators. Since 2008, the standards have been updated as the threat landscape evolves.

Physical Threats

Unlike cyber threats, which are constantly evolving, many threats to physical infrastructure have been known for years, if not decades, and are more readily understood. Electric utilities take these threats seriously and deploy measures to mitigate such threats.

Simple mitigation techniques like cameras and locks can help utilities deal with routine problems. The key to electric utility physical security, however, is the industries' "defense-in-depth" approach, which uses modeling to assess criticality and to build redundancies, resiliency and the ability to recover, should an extraordinary event occur. While systems are built to withstand attacks, successful attacks may still occur even with such planning.

The topic of physical security has become more prominent since the 2013 sniper attack on the Metcalf substation. After that event, the entire electric sector assessed its impacts and shared lessons learned. DOE and DHS, in coordination with the FBI, the E-ISAC and industry experts, also held a series of briefings for utility owners and operators and local law enforcement regarding security of electric substations.

---

[2] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Monitor (ICS-MM201212), October-December 2012, Original release date: January 02, 2013 | Last revised: February 19, 2014 available at https://ics-cert.us-cert.gov/monitors/ICS-MM201212.

[3] Campbell, Richard J., "Cybersecurity Issues for the Bulk Power System," Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989 .

Consequences

Examples of consequences of events impacting the grid include:

- The 2003 blackout in Ohio, caused by a tree branch coupled with software issues and human error, was blamed for contributing directly to ten deaths with further indirect impact on the surrounding population. It took two days to return electricity to the entirety of the affected area.[4]
- After Superstorm Sandy in 2012, millions of people were left without power. Despite broad disaster relief efforts, it took thirteen days to restore power to at least 95 percent of customers in New York and eleven days to restore power to 95 percent of customers in New Jersey.[5]
- The Metcalf substation attack in 2013 caused over $15 million in damage, but did not lead to any loss of power or life.[6]

[4] Barron, James, "THE BLACKOUT OF 2003: The Overview: POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN 8 STATES AND CANADA; MIDDAY SHUTDOWNS DISRUPT MILLIONS," N.Y. Times, available at http://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html?pagewanted=all .

[5] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, "Comparing the Impacts of Northeast Hurricanes on Energy Infrastructure," April 2013, available at http://www.oe.netl.doe.gov/docs/Northeast%20Storm%20Comparison_FINAL_041513c.pdf .

[6] Smith, Rebecca, "Assault on California Power Station Raises Alarm on Potential for Terrorism," Wall Street Journal, February 5, 2014, available at http://www.wsj.com/articles/SB10001424052702304851104579359141941621778 .

WITNESS LIST

PANEL 1

The Honorable W. Craig Fugate
Administrator
Federal Emergency Management Agency

Ms. Patricia A. Hoffman
Assistant Secretary
Office of Electricity Delivery & Energy Reliability

Ms. Caitlin A. Durkovich
Assistant Secretary for Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Mr. Richard Campbell
Specialist in Energy Policy
Congressional Research Service

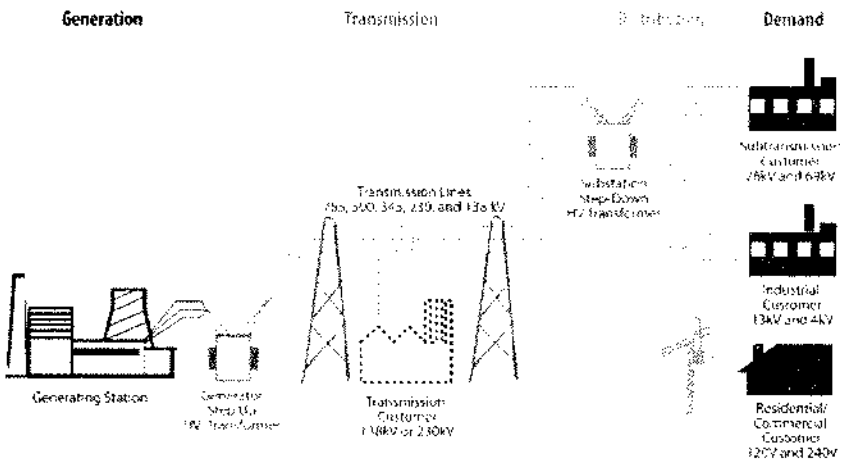
PANEL 2

Mr. Gerry W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation

Mr. William H. Spence
Chief Executive Officer
PPL Corporation

Ms. Bobbi J. Kilmer
President and CEO
Claverack Rural Electric Cooperative

Attachment A Electric Power System Elements



Source: Congressional Research Service, based on graphic found at https://reports.energy.gov/BlackoutFinal-Web.pdf .

BLACKOUT! ARE WE PREPARED TO MANAGE THE AFTERMATH OF A CYBERATTACK OR OTHER FAILURE OF THE ELECTRICAL GRID?

THURSDAY, APRIL 14, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT,
PUBLIC BUILDINGS, AND EMERGENCY MANAGEMENT,
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m. in room 2167, Rayburn House Office Building, Hon. Lou Barletta (Chairman of the subcommittee) presiding.

Mr. BARLETTA. The committee will come to order. Today we are holding a hearing to explore a critical and timely topic. There have been numerous congressional hearings on cybersecurity and how to stop the bad guys. What has not been discussed in great detail is what the consequence will be from a massive cyberattack that brings down, for example, a large portion of the electrical grid for an extended period of time.

The purpose of today's hearing is to answer an important question: With respect to cyberthreats to the electrical power system, what consequences should the Federal Government tell States and local governments to prepare for? In other words, for how many people and for how long should States plan on being without power?

The Federal Government does this now for almost every significant hazard that we face. Whether it is a category 5 hurricane hitting Miami or an 8.0 earthquake in Los Angeles, the Federal Government has realistic estimates or scenarios for States and cities to plan. The Federal Government does not have this basic planning scenario for a cyberthreat to the power system, and there is a huge disparity in what different groups think is a potential scenario for which States and local governments should prepare.

And the difference would be significant for local governments. If the power is out for a few days, it can be an inconvenience, but if it is out for several weeks, or a month or more, the local government has to potentially plan for increased public safety, water treatment, sheltering, or evacuation, fuel delivery for generators, and many other contingencies.

What should we plan for? Ted Koppel, in his book, says that we should plan on 6 to 18 months of uninterrupted blackouts. The industry seems to say a cyberattack could, at most, cause an inter-

ruption in terms of days, not weeks. And today we are going to hear testimony from the Federal Emergency Management Agency, the Department of Energy, the Department of Homeland Security's National Protection and Programs Directorate, the Congressional Research Service, the North American Electric Reliability Corporation, and representatives from the electrical industry. I hope to get an answer to this question for State and local governments who are on the ground and will be first charged with protection of people and property.

Imagine what we would do without electricity for a day, a week, a month, a year. Virtually all critical infrastructure is dependent on the electrical grid, particularly the lifeline sectors: telecommunications, transportation, water, and financial services. And if the goal of the bad guys is to collapse the United States economic system, they are going to try to cut off the power.

There have been reports of hacking attempts on electrical facilities by foreign and domestic parties. Our national security, public safety, economic competitiveness, and personal privacy is at risk. According to the Department of Homeland Security, the energy sector was the target of more than 40 percent of all reported cyberattacks.

And even more disconcerting was the December 2015 cyberattack on Ukraine's electric grid, which affected four dozen substations and left one-quarter of a million people without power. At the same time as the attack on the grid itself, call centers were hit with a telephony denial-of-service attack as customers were trying to report the outages. If anyone thought this was a glitch, think again.

The electrical grid is not only under attack from cyberspace, the electric power sector is all too familiar with the devastation storms like Hurricane Sandy can leave behind, or physical attacks like the 2013 incident at the Metcalf substation in California. Thankfully, in the cases of storms and physical attacks, the power sector has strong plans in place and redundant systems to restore power quickly and to avoid the loss of life and property.

But I am concerned about a cyberattack. Are there similar plans in place for industry and for State and local government? Will those redundancies provide the same types of protections?

Most recently, I have been discussing this topic with constituents in my district, asking what they will do in their communities if the power is out for a prolonged period of time. Honestly, most of them don't know because we don't know what to plan for. We have brought together the right people here to tell us today.

We are also going to discuss what preparedness looks like, best practices, and how we can achieve a greater level of readiness, all the way down to the local mayors and township supervisors. I am encouraged to hear all the industry talk about an all-hazards approach and focusing on mitigating the greatest risks, but I think there are some unique characteristics of the cyberthreat that require specific planning guidelines.

I know we cannot goldplate the system, but given the interdependency of electricity with our daily lives, it is crucial that we understand the risks and be prepared for the likely consequences possible from the failure of that system.

I look forward to this conversation today, starting with our witnesses, and I thank you all for being here.

I now call on Ranking Member DeFazio for his comments.

Mr. DEFAZIO. Thank you, Mr. Chairman. Mr. Chairman, you certainly laid out well the potential threats of a cyberattack against our critical electrical grid. We know there is constant probing, some of it being done by nation-states, not just terrorist groups, nation-states hostile to the U.S. And we need to be certain that we are as prepared, well prepared, as we can be. The Ukraine attack was perhaps a harbinger of things to come.

The—I do believe, though, that the all-hazards approach can also cover the cyberattack area. The issue of probably most immediate concern to those of us who live in the Northwestern United States is the threat of Cascadia subduction zone quake in the magnitude of 9 or 9-plus, which will inevitably knock out our grid. So, you know, there are going to be exercises conducted, two exercises this year, with the cooperation of the Department of Homeland Security and all the local and State authorities in the region to simulate what would be possible in the face of that sort of a disaster.

Many of the problems that could occur will be the same. You know, the loss of transformers is particularly of concern, and I am going to be probing that issue with some of the witnesses today. There is a question whether the Federal Government should be perhaps stockpiling these transformers, since now they are basically custom orders. They take 6 to 18 months.

What if we lose a dozen large critical transformers because of an earthquake, tsunami, or a cyberattack? You know, it seems to me kind of a no-brainer that we should, either through Government sources or through cooperation with the industry, be creating a critical infrastructure component stockpile here in the United States to deal with any and all of these sorts of potential attacks. And a coordinated, physical attack and cyberattack could, of course, be the most devastating, outside of a massive earthquake/tsunami. And again, many of the same issues arise.

And then one that doesn't get talked about very much any more but we held a series of hearings on it years ago in the Committee on Natural Resources—then called the Committee on Interior and Insular Affairs—when we had jurisdiction over nuclear power is the potential for a bomb in place. That is, a nuclear plant. If you destroy the backup system—take over the plant, destroy the backup system and the incoming power, you can create a meltdown. And how good is the security at our nuclear plants these days? I know this hearing isn't going to get to that topic, I am not certain it is even within our jurisdiction, but it is of concern to me, and I just wanted to raise that issue, too.

So, like aviation, you know, electricity, the grid, the—and nuclear plants are of interest to terrorist groups and hostile nation-states, so we have got to be prepared. So I am pleased you are holding this hearing today.

Mr. BARLETTA. Thank you. We will have two panels of witnesses today. And on our first panel we will have Administrator Fugate, the current Administrator of the Federal Emergency Management Agency, the Federal coordinator for consequence management; Assistant Secretary Hoffman from the Department of Energy's Office

of Electricity Delivery and Energy Reliability—this is the office charged with coordinating the Federal efforts to facilitate the recovery from disruptions in the emergency and the energy supply; Assistant Secretary Durkovich, the Assistant Secretary for Infrastructure Protection from the Department of Homeland Security; and Mr. Richard Campbell, an expert at the Congressional Research Service in the electric power sector.

On our second panel we will be joined by Mr. Gerry Cauley, the president and CEO of the North American Electric Reliability Corporation, the international regulatory authority whose mission is to assure the reliability of the bulk power system in North America; Mr. William Spence, CEO of the PPL Corporation, one of the largest investor-owned utility companies in the United States; and Ms. Bobbi Kilmer, president and CEO of the Claverack Rural Electric Cooperative, a nonprofit electric utility serving 2,250 square miles in northeastern Pennsylvania.

I ask unanimous consent that the witnesses' full statement be included in the record.

[No response.]

Mr. BARLETTA. Without objection, so ordered. Since your written testimony has been made a part of the record, the subcommittee would request that you limit your oral testimony to 5 minutes.

Let's start with our first panel. Administrator Fugate, you may proceed.

TESTIMONY OF HON. W. CRAIG FUGATE, ADMINISTRATOR, FEDERAL EMERGENCY MANAGEMENT AGENCY; PATRICIA A. HOFFMAN, ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, DEPARTMENT OF ENERGY; CAITLIN A. DURKOVICH, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY; AND RICHARD CAMPBELL, SPECIALIST IN ENERGY POLICY, CONGRESSIONAL RESEARCH SERVICE

Mr. FUGATE. Thank you, Mr. Chairman, Ranking Members, Members. I want to address your questions. What does a local official need? What do they need to plan for? And I think, based upon our experiences dealing with other hazards that have caused disruptions, planning needs to be measured in weeks, particularly if there is damage to infrastructure. And again, with cyber, we have seen restoration potentially very quickly if there is not physical damage. But if you do have damage to things like very large transformers or generator capacity, that will extend it.

We do know that it is important that in an initial response, that you provide for safety and security. When lights are out, power is out—we have had major metropolitan areas go through this—you have a flurry of activity with people trapped in elevators, traffic control, and the fact that initial response may mean going out on patrol and looking for problems, rather than waiting for the traditional call to 911, which may or may not be impacted, as you have pointed out before, with denial-of-service attacks.

Your next steps are pretty much, again, as the ranking member points out, all hazards. You have to then provide for the most im-

mediate needs. Hopefully, your critical infrastructure has power and emergency power, you have the fuel supply you need. We have found in many cases communities haven't planned for that. Either they don't have critical equipment on backup power or they don't have adequate fuel supplies—usually only enough fuel to run their weekly or monthly test, but not to operate in a crisis.

Generators are very expensive. And so, in many cases, there are other options, such as putting in transfer switches. The idea is what are the things that are required to keep the community up and running until power can be restored that are lifelines? Water systems, wastewater treatment, communications, your hospitals, and your 911 and other dispatch facilities. Generally, these have emergency power, but it has to be planned for real, not that it just works during the monthly test.

And then, as you have pointed out, Mr. Chairman, the duration now starts driving additional issues. As we saw in New Jersey and New York, the longer you have power disruptions, the more you have cascading effects, from everything to not being able to get to retail stores, grocery stores, others, gasoline distribution. And again, as a community starts to try to recover and get back to normal, these all become challenges.

So, the planning really is based upon safety, keeping your primary life support systems up, focusing on the restoration of the grid, and the reality that your residential areas will probably be last to get power because you are going to try to get your retail sectors and major core centers up first.

The industry has shown a lot of resiliency capabilities of doing those things in physical destructions. And we think that the lessons we have learned there would apply, again, to cyber. But cyber has a lot of unknowns. And I will defer to my experts to my left on what those impacts are, the potential threats, and how likely these are.

But you said how big is big. We actually looked at a natural phenomenon that is actually big, and that would be geomagnetic storms. Because of the way our grid is built, and the vulnerabilities to very large transformers, this administration has already developed a working plan of what we would do in the event of major geomagnetic storms, its impacts on satellites and terrestrial systems.

We are working currently now on the lessons from the previous power outages on the annex to add to the National Response Framework to look at the power outages because of a lot of the unique capabilities the Federal Government brings, but also this has got to be a true working relationship with the utilities. We cannot do this separate. It is a partnership. It has got to involve all levels, because the primary place we regulate power is at the States, through the, you know, utility regulatory operations the—State managed.

That framework this summer will be going to our senior leadership in the agencies to begin that process of concurrence and updating it, but it serves as a framework if something was to happen now, based upon our lessons from Sandy, and going all the way back to previous hurricanes and other disruptions.

But the challenge is, I think, for people to look at planning not for what they do every day, but what would happen if power was out for not just hours but days or weeks. Do they really understand what their capabilities are, and the things they need to do to ensure that their critical lifelines have enough power?

And trust me, sir, I have been through enough hurricanes to find out too many facilities only had enough emergency power to pass whatever requirements were there, but under full load in a crisis they failed. They didn't operate them under loads, they didn't maintain enough fuel in the systems for that. They did not have contracts for firm deliveries when the crisis occurred. So you really need to get people to focus on this, that if you are going to provide emergency power it has got to be for real, and it has got to be able to operate for long periods of time.

And you need to really plan for this from the standpoint of a phased approach, because oftentimes when this starts we don't know how long it is going to be out. So we have immediate response steps, but you also need to start asking the question if power isn't on in 72 hours, what are the next things we have to focus on? If we are out for a week, what are the next things we have to focus on?

But I think the story from industry is also good. We have learned a lot about how to get systems back up. We have learned how to bypass fail systems. And, in many cases, the automation has replaced the man in the middle. And sometimes we have to put people back in and run less efficient systems, but we can get power back.

So I think there is both a good news story, but there is still a lot that we don't know. So against that we are not going to be able to write a plan for everything that can happen. We need to write plans based upon consequences. And again, as we have a better understanding of the duration of impacts, that will help us shape that guidance to State and local officials for dealing with extensive power outages, pretty much irregardless of the cause of it, but really looking at it over the time phase of what would be happening and what the next steps are.

But again, a lot of the lessons have been learned from natural hazards. The question in cyber is how widespread and how many jurisdictions simultaneously will be impacted. That is probably the one difference that a physical specific such as a hurricane or earthquake—we know the geographical area, which cyber—it won't be defined by political or physical boundaries, it would be systemwide. And that is another area that we ask questions about.

But not much dissimilar to the threat from geomagnetic storms. That is a hemispheric risk, and that is probably—when you—outside of a A&P detonation in space, it is probably the largest potential impact to the utilities, and again, a lot of work has been done to minimize those impacts.

So, Mr. Chairman, I stand ready for questions, but I wanted to try to answer your questions in my opening statements.

Mr. BARLETTA. Thank you for your testimony. Before we move on I want to recognize the ranking member of the subcommittee, Mr. Carson, for his opening statement.

Mr. CARSON. Well, Chairman Barletta, thank—we had a hearing with the CIA [Central Intelligence Agency] Director and I didn't have access to my phone. And then, when I finally escaped I saw the messages. But my apologies. But I want to thank you guys.

Chairman, I think—for the sake of time, I think we should still continue, because I was the one who was late, so thank you.

Mr. BARLETTA. Thank you. We will now move on to Assistant Secretary Hoffman. You may proceed.

Ms. HOFFMAN. Chairman Barletta, Ranking Member Carson, members of the subcommittee, thank you very much for focusing attention on the importance of being prepared for an outage, and for the opportunity to discuss the Department of Energy's role in helping ensure resilient, reliable, and flexible electricity systems in an increasingly challenging environment.

Our economy, national security, even the health and safety of citizens depend on reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability is to strengthen, transform, and improve our energy infrastructure to ensure access to reliable, secure, and clean sources of energy. We are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure, including the electric power grid, from disruptions, whether it be caused by natural or manmade events, including severe weather, physical attacks, and cyberattacks.

A crucial factor in meeting these challenges is to be proactive, and cultivate what I call an ecosystem of resilience, a network of owners and operators, regulators, vendors, Federal partners, and consumers acting together to strengthen our ability to prepare, respond, and recover. Our organization works on indepth strategies, products, and tools to inform and educate State and local officials in their energy emergency preparedness activity. This is done through forums, trainings, and tabletop exercises that include Federal, State, and local energy officials.

In the area of cybersecurity, as part of the administration's effort to improve electricity subsector cybersecurity capabilities, the Department of Energy and industry partners have developed the Electricity Subsector Cybersecurity Capability Maturity Model. This is an evaluation tool that helps organizations prioritize and develop cybersecurity capabilities.

In April, DOE [Department of Energy] will lead Clear Path IV in Portland, Oregon, and Washington, DC. Clear Path is an interagency exercise focused on testing and evaluating the energy sector roles and responsibilities and response plans utilized for a Cascadia subduction zone 9.0 earthquake and tsunami. When a response is required and needed, the Department of Energy serves as lead agency for this response under the National Response Framework and under FEMA's [Federal Emergency Management Agency's] leadership.

The Department of Energy works with industry and Federal partners to assess the impacts of disaster on local and regional energy infrastructure, coordinate delivery of assets, monitor and report on restoration efforts, and provide regular situational awareness to key decisionmakers in the States, the White House, and our interagency partners.

DOE also provides strategic leadership by requesting and facilitating the development of an energy Information Sharing and Analysis Center, as well as the development of an Electricity Subsector Coordinating Council. This council is a group of leaders from across the electric sector that meet regularly with Government to coordinate and share information. When power goes out, the local utility is the first responder. Should any threat or emergency exceed the capability of any local or private-sector resources, the Federal Government and the electric sector, through the council, will engage in coordinating a response to this type of a crisis.

Congress enacted several important new security measures in the FAST Act [Fixing America's Surface Transportation Act]. This act affirms DOE's responsibility in cybersecurity coordination, oil and gas information sharing, and the development of a transformer reserve plan. In addition, the FAST Act provides the Secretary of Energy with a new authority: Upon declaration of a grid security emergency by the President, the Secretary can issue orders to protect and restore critical electric infrastructure, or defense critical electric infrastructure. This authority allows DOE to respond as needed to cyberthreats or physical threats to the grid. The Department is actively engaging in the process and procedure for implementing this new authority.

The keys to strengthening resilience are not only understanding threat insight and response, but it is also through innovation. Advanced technology and innovation in cybersecurity storage microgrids will also help the industry get ahead of these risks.

In conclusion, the threats will continue to evolve. DOE is working diligently to stay ahead of the curve. To accomplish this we must invest in resilience, encourage innovation, and use the best practices to help raise the sector's cyber and physical security maturity, as well as strengthen local incident response and recovery capabilities.

Thank you for your time. And this concludes my remarks. I look forward to any questions you have.

Mr. BARLETTA. Thank you for your testimony, Assistant Secretary Hoffman.

Assistant Secretary Durkovich, you may proceed.

Ms. DURKOVICH. Good morning, Chairman Barletta, Ranking Member Carson, and members of the subcommittee. My name is Caitlin Durkovich, and I am the Assistant Secretary for Infrastructure Protection within the National Protection and Programs Directorate at the Department of Homeland Security. Thank you for the opportunity to discuss how NPPD, which leads the national effort to secure and enhance the resilience of our Nation's infrastructure, fulfils its responsibility to support the Federal Government's preparedness for, response to, and recovery from all-hazard events, including the physical impacts of cyber incidents.

I want to begin by acknowledging that protecting the electric grid is a top priority of this administration and of the Department of Homeland Security. It is also worth underscoring, as you will hear from our industry partners later, that the grid, by its very design, is resilient. It is a complex network of electric infrastructure assets that has built-in redundancies and can adapt to rapidly changing demand, load, climate, and a host of other factors.

In short, the electric grid has been engineered with one principle in mind: reliability. Thousands of companies work together with the Government to run the most reliable grid in the world. And while over 85 percent of the Nation's electricity infrastructure is in private hands, the Federal Government recognizes we must work in partnership with industry to protect our grid because of its importance to national security, economic prosperity, and community resilience.

I have the privilege of working with industries that span the 16 critical infrastructure sectors, and can say with confidence that the electric industry takes a multilayered approach to risk management, and is committed to continuous adaptation, based on lessons learned from real-world events and exercises, and an understanding of the dynamic risk environment. Industry and Government acknowledge, however, we cannot stop every threat and natural hazard, and that we must be prepared to respond to a range of events and their consequences.

The Federal Government's voluntary partnership with the electric sector, which is defined under the National Infrastructure Protection Plan, reached new levels in 2012 following two important events. The first was a report published by the Presidential advisory committee, the National Infrastructure Advisory Council, in 2011 on the resilience of the electric and nuclear sectors, and called for the most senior executives from industry and Government to convene on a regular basis to craft a risk management agenda that was reflective of the increasingly chaotic threat environment.

Nearly a year later our country awoke to the scenes of an earthquake, tsunami, and subsequent failure at the Fukushima Nuclear Power Plant in Japan that put new emphasis on the need for the public and private sector and the United States to come together to plan for a catastrophic national incident.

For nearly 4 years now, 30 CEOs representing the breadth of the electric power industry have comprised the Electricity Subsector Coordinating Council, and meet regularly with their counterparts at DHS [Department of Homeland Security], DOE, and other members of the interagency to address the growing number of sophisticated factors that put our grid at risk. This risk management approach is focused on ensuring that the consequences of the most catastrophic events are minimized, and that the value of our relationship is strengthened by identifying joint priorities enabled by robust information sharing, continuous planning, and regular testing and exercise of these plans.

Projects conducted through this partnership include action-oriented information sharing around physical and cyber events, including black energy: a 2013–2014 security outreach campaign around threats to substations recommended security best practices and the importance of reporting suspicious activity; an Electricity Subsector Coordinating Council playbook, which is a crisis management framework to enable senior executives from industry and Government to coordinate effectively on response and recovery issues; as well as work by DHS and DOE with the Electricity Subsector Coordinating Council on efforts to institutionalize coordination with other lifeline functions.

In addition to our ESCC [Electricity Subsector Coordinating Council] work, DHS works directly with owners and operators to help enhance their security and resilience posture, understand dependencies and interdependencies, and exercise with their State, local, tribal, and territorial partners for a range of possible scenarios. This engagement would not be possible without a cadre of security specialists around the country who engage with asset owners on a regular basis to help them understand the risk posed by cyber and physical threats, perform assessments, share information, and ensure they are connected to the broader homeland security community to include State and local officials.

NPPD also works with partners across the Government in the event of a needed response to a major disaster or attack resulting in a failure of the electric grid. NPPD supports FEMA during response operation, and helps provide an understanding of the infrastructure of concern in an impacted area, and decision support in prioritizing restoration and recovery, as well as ensuring the resilience of our communications infrastructure.

During a cyber or communication incident, NPPD's National Cybersecurity and Communications Integration Center is able to coordinate with State, local, and private-sector partners, including law enforcement and intelligence communities, so that the full capabilities of the Federal Government can be brought to bear in a coordinated manner.

The Industrial Control Systems Cyber Emergency Response Team is the response component of the NCCIC [National Cybersecurity and Communications Integration Center] and provides on-site support to private-sector industrial control system owners and operators.

In conclusion, Government and industry have engaged in an unprecedented effort to assess and mitigate the risks from cyberattacks, physical sabotage, and natural disasters, all of which can result in disruptions to the electric grid. In a major step toward this unified approach, the Department proposed to transition NPPD to an operational component, the Cyber and Infrastructure Protection Agency. This transition would elevate cyber operations and provide more comprehensive, coordinated risk management support to our stakeholders that reflect the growing convergence of cyber and physical threats.

Chairman Barletta, Ranking Member Carson, and members of the subcommittee, thank you again for the opportunity to appear before you today and to discuss NPPD's efforts in managing the physical consequences of cyberthreats.

I look forward to your questions.

Mr. BARLETTA. Thank you for your testimony, Ms. Durkovich.

Mr. Campbell, you may proceed.

Mr. CAMPBELL. Good morning, Chairman, Ranking Member, and members of the subcommittee. My name is Richard Campbell. I am a specialist in energy policy for the Congressional Research Service, CRS. On behalf of CRS I would like to thank the committee for inviting me here to testify today.

My testimony will provide background on the possible consequences of a failure of the electric grid, the roles with respect to parties, and some of the objective challenges in the recovery efforts.

I should note that CRS does not advocate policy or take a position on specific legislation.

Electric power generation is vital to the commerce and daily functioning of the United States. While the electric grid has operated historically with a high level of reliability, various parts of the electric power system are vulnerable to failure due to natural, operational, or manmade events. Natural events include severe weather and even solar storms. Operational events can result from failures of grid components or systems. And manmade events would include actual attacks on the grid. The extent to which these events could damage the grid would depend upon the severity of the incident.

Much of the infrastructure which serves the U.S. power grid is aging. As the grid is modernized, new technologies utilizing two-way communications and other digital capabilities are being incorporated with Internet connectivity. While these advances can improve the efficiency and performance of the grid——

Mr. BARLETTA. Mr. Campbell, excuse me. Can you pull the microphone just a little closer? Thank you.

Mr. CAMPBELL. While these advances can improve the efficiency and performance of the grid, they may also increase its vulnerability to cyberattacks launched from the Internet.

In 2014 the National Security Agency reported that it had seen intrusions into industrial control systems with the apparent technical capability to take down the controls to operate U.S. power grids, water systems, and other critical infrastructure. Although there has not been a cybersecurity event resulting in a power outage in the United States, the potential still exists for such attacks to cause a wide-scale, long-lasting outage.

The first blackouts attributed to a cyberattack happened in Ukraine in December 2015. The attack targeted industrial control and operating systems in multiple regional utilities. Other critical infrastructure was also targeted, apparently in an attempt to impair recovery efforts. A report released by the National Research Council in 2012 concluded that well-informed terrorists could black out a large region of the country for weeks or even months. It said that if such an attack occurred during times of extreme weather, hundreds or thousands of deaths could occur from heat stress or extended exposure to the cold. A systematic attack of this sort could cost the U.S. economy hundreds of billions of dollars.

Recovery from a well-planned cyber and physical attack on the grid could be complicated by the cost and vulnerability of critical components. For example, the strategic destruction of a number of critical, high-voltage transformers could use up the limited inventory of spare units, and it may take months or even years to build new units.

The electric utility industry generally prepares for outages from weather-related events, and views the potential for a major cybersecurity attack or similar event as a low-probability risk. If an event is severe enough to be a federally declared disaster, then FEMA, the Federal Energy Management Agency, can provide financial assistance to eligible utilities for the recovery effort.

And in 2015 Congress gave the Department of Energy new authority to order electric utilities and the North American Electric

Reliability Corporation, NERC, to implement emergency security measures in the Fixing America's Surface Transportation Act.

However, given the potential for damage to the Nation's economy from a major attack on the grid, some might suggest that the greater focus on recovery is needed, and should become as much a part of the grid security strategy as the efforts to secure the grid. A focus on recovery should consider the mutual dependence and implications to other critical infrastructure of an electric grid failure, and how quickly such impacts could proliferate, if not planned for in advance.

Congress may also want to consider how the grid of the future will address cyber and physical security concerns. Incorporating elements to increase system resiliency as it develops will aid in reducing the vulnerability of the system.

Finally, NERC has stated that after a major grid disruption, restarting generation and energizing transmission and distribution systems will be a first priority. Restoring service to communications systems, fuel, water supply and treatment and hospital customers will be a secondary priority. Congress may want to consider how planning for the subsequent restoration of services would proceed to ensure that all civilian communities are kept informed, and they are treated as equitably as possible in disaster recovery efforts.

This concludes my brief remarks. I look forward to your questions.

Mr. BARLETTA. Thank you for your testimony, Mr. Campbell. I will now begin the first round of questions, limited to 5 minutes for each Member. If there are additional questions following the first round, we will have additional rounds of questions as needed. And I will start with Administrator Fugate.

Could you please walk the committee through a timeline of consequences that we could expect to experience in the event of a large-scale and a prolonged power outage which is the result of a combined cyber and physical attack?

Let's assume over 10 million people are out of power in the Northeast and it lasts for over a month.

Mr. FUGATE. The first thing——

Mr. BARLETTA. I am not talking about how to turn the power back on. But what consequences will State and local governments and residents have to deal with because the power is out? And this is my concern. I am going to put my mayor's hat back on. And, you know, I have been listening to a lot of how prepared we are, what we can—what is typical, what is unlikely, and what we are going to do. But I am not convinced that we have connected the dots all the way down to the local government.

I haven't talked to a mayor or a township supervisor yet. When I ask them the question, "In the event of an unusual and an unlikely event that power is out in a cyberattack, how long are you prepared to provide services?" nobody can give me that answer. You know, I know it is an unlikely event. So was the chance of two planes running into the twin towers in New York, very unlikely.

So, that is what I am hoping to get at today is, for example, in the first few days—because these are the people—I was a mayor. When something like this happens there is going to be panic, and

people are going to want to know how long can we expect—and I don't know if anybody has yet given me a clear answer.

In the event of both a physical attack and cyberattack, the worst-case scenario—very unlikely, very unusual, but still, as a mayor and a supervisor, I want to be prepared for that worst-case circumstance. So, for example, in the first few days there will be thousands of people stuck in elevators. After 3 or 4 days, hospitals and other critical infrastructure will need fuel for generators. After a week, clean water and waste disposal may be—may have serious problems. And at some point people may start to self-evacuate in large numbers.

Please walk us through that timeline of increasing consequences, as the duration of this scenario increases.

Mr. FUGATE. Mr. Chairman, first challenge, having actually had this happen during accidents where human error causes power outages, we don't know at first how long it is going to be out. And oftentimes you only know that you are having power outages; you are not aware of what is happening outside. Situation awareness will be key, because your initial response will not be any different.

We have had numerous communities go through power outages very substantial that resulted in having to do mass rescues and elevator operations, deal with the traffic control issues, hitting at commuter times with commuter rail being knocked off with electricity. We have seen those. I think most communities that are doing effective planning, those are things that they will be doing almost from the beginning. What is critical—and this goes back to what my partners to the left will be focused on—is this a short-term duration or is it longer.

We faced this in Florida, actually, when I was still in the State. We had power knocked out that was not occurring in any set pattern. It was occurring all over the State simultaneously. We didn't know what was going on. By the time we had situational awareness, the next question was, "Will this go into the night hours?" Because if so, the Governor will call out the National Guard to provide additional law enforcement support.

And so, again, you start focusing on those immediate things of life safety. Also safety in your communities, because when you lose power and you start seeing those disruptions, you have to provide a much more visible form of policing and give people a sense of safety in their communities. That is going to require more manpower, more people on the streets. You start looking at my generators are now running, what systems will need refueling next? Is it going to be the next 72 hours?

And this is something I think is important. I learned this the hard way. A lot of communities do not plan for refueling in a crisis. And there are certain contractual things you have to have to make sure you get deliveries, and those deliveries to suppliers may not be local. Again, if you are talking 10 million people, we were shipping fuel as far away as Philadelphia back into New Jersey and New York to provide gas. We found all kinds of regulatory challenges.

But again, you start going, "OK, my first step is pretty much my emergency response. My next step is the next 72 hours. Which of my critical facilities will start running out of fuel or are having

generator problems?" This is—by this time we would hopefully have assessed this is a much larger event than local. We start looking at mobilizing resources from the outside, generators, fuel, other things to keep those on.

It is key to keep the water systems and wastewater running. Electricity has got a lot of problems, but water and wastewater are almost impossible to make up the differences in dense populations. There is not really a good way to manage that if those systems go offline for extensive periods of time. And so you continue to escalate.

Once you get to past my 72 hours—and I am starting to talk my first week—now you start really looking at what does the retail sector supply chain look like. Florida learned this hard lesson, that many of our gas stations, grocery stores, and even pharmacies now have emergency power, they have transfer switches because, as we were dealing with power outages measured in weeks, literally, from hurricanes—and some of our duration of outages actually went to almost a month—we found that retail was doing a lot of things that we had to start supporting because they were bringing in generators, they were getting themselves back open.

But we weren't doing it as a partnership, we actually found ourselves competing with them. So you really want to plan this. And I think most communities, that initial response, if they have got good plans, they have done this, or they are prepared to do it. It is once you get past 72 hours that I think that they really need to start thinking through their plans. Where are they going to get fuel? What kind of things do they have to keep up? And then where will be the next points?

As we saw with New Jersey and New York, initially it was the rescues and the trapped people and stuff like that. A lot of people evacuated. But then it became the fuel, it became pharmacies, grocery stores. And so you started seeing cascading effects. And again, those are the things I think that, once you are past 72 hours, you need to start planning out, OK, I am out for 1 week, I am out for 2 weeks, I am out for 3 weeks. How much of my core am I bringing up?

Again, the utilities aren't waiting. They are not going to be nothing happening for a month. But you are not going to get power back to everybody, and you are not going to get power back particularly to a lot of your residential areas. So can you get enough life support back up and running where people that still don't have power can get the essentials? It won't be easy, it will be difficult.

But the thing here now is to continue to trade off. Where can I make activities to buy more time to keep my population stable? Evacuations, maybe self-evacuating. Where people have that option, they will. But you won't see large numbers, because it is unlikely in widespread outages there is going to be places to go to.

So again, it becomes this time of stabilization, continue to look at the down-range impacts, what we are able to bring up, where we prioritize that. But the reality is that almost all these scenarios, including the cyber as well as the physical, residential areas are probably going to be the last ones to get that power. So can you get enough life support and infrastructure going to keep the major supply lines up? And you are not going to have everything. You are

not going to have what the normal consumption rates are. You may have to do what Governor Christie did and go with rationing of gasoline to start normalizing what is available versus demand signals.

But this means you have to plan out not just the power went out, but now what are the impacts of that as you go through—and then, hopefully, this is what our partners are working on, is to give you better information about how much time are we talking about before key systems come up. When will we get the final power turned back on? Because in the absence of information, I think that generates its own problems. If we know that it is going to be out for 3 weeks, we can plan. People are more resilient than we give them credit for. But the lack of information, that in itself becomes a challenge.

So I ran over my time, Mr. Chairman, but I was trying to——

Mr. BARLETTA. That is OK, because it is important, because that is what I am trying to get at, is are these conversations—and who is responsible for these conversations with people at the local level, because this is an unknown. If there is a storm coming, a hurricane, an ice storm, a—we are prepared for that. We can expect—we know what is coming. An earthquake, not so. You don't know it is coming, but still we have experience with that. But a widespread cyberattack with a physical attack attached to it is unknown. And who is having that conversation with people at the local level that—we don't know. It could be out a week, it could be out longer than a week. You need to be prepared.

And are those conversations actually happening? I don't—I am not convinced that they are. And that is where the life will be lost. And I think we need to begin to find out how do we connect the dots. Who is responsible for having those conversations down at the lowest level of the people who will be first charged with trying to protect lives.

I am going to turn to Ranking Member Carson for his questions.

Mr. CARSON. Thank you very much, Chairman Barletta. Madam Hoffman, your testimony notes that the Department's research and development activities with respect to developing spare transformer components, what is the cost to manufacturers when we are making these alternative components? And has a domestic manufacturer been identified so that we can ensure that there is no disruption to its prior usage?

Ms. HOFFMAN. So thank you very much for the question. Transformers are a very critical component to the electric sector as was stated in the testimonies and some of the conversations earlier.

With respect to transformers, the price of a transformer ranges anywhere between $5 million and $10 million. And so these are significant components. So what is our research program, or what are the activities looking for, dealing with the transformer issues? It is, first of all, looking at the spare components that—and the spare transformers that industry has, and then industry is looking at having spare capacity on their system.

We are also looking at how do we develop the next generation transformer, which might be a transformer that you have the ability to produce more quickly, and also have more standardization

and flexibility. So that includes, in our research component, the development of power electronics and hybrid transformers.

Our 2017 budget request has a very strong program looking at transformers, which is about $10 million, in which we are going to look at developing the next generation transformers, as well as doing testing of transformers to make sure we understand any vulnerabilities that may exist.

Mr. CARSON. Thank you. Administrator Fugate, in the event of a widespread outage, what are FEMA's plans for communicating with citizens on response and recovery efforts when there is essentially zero electricity?

Mr. FUGATE. Not much different than what we have faced in other significant outages. We have a variety of tools.

First of all, within the emergency alert system, the radio stations, TV stations, many of the—that have emergency power, TV stations partner with radio stations. We can get signals. And in addition, if we lose a—and this will be something that we will be looking at in Oregon during the Cascadia—it is not uncommon that you are going to lose radio and TV stations in the area of impact.

But we work with the FCC [Federal Communications Commission] for the nonimpacted stations to increase power to get signal back in. That is why we continue to encourage people, have that battery-operated radio. That is why we encourage the idea of FM chips in cell phones, because we can get signals in from the outside, but people need to receive it to get the information.

But part of this is going to be where the information is coming from. We are going to be working through the Governor's office because Governors and their teams are going to be the best information at the local level. Our job, really, on the Federal side is to provide the backup and tools required. And we are prepared to work with the FCC and broadcasters to get signal from the outside. In addition, we have gone as far—and we did this in the Sandy response—bring in satellite communications and set up WiFi in some of the areas that have lost some of the cellular communications.

But we have another backup, and, self-disclosure, I am an amateur radio operator. But I think sometimes the more we look at the complexity of our risk, we forget that we have some very resilient systems that aren't part of Government, but they oftentimes are the last thing running when everything else has failed. So we look from everything from our systems and satellite technology, working with nonimpacted stations how to broadcast in, amateur radios are all part of that.

But it is important that people take the steps to be able to get the information when we can get the signal in, and that is why it may seem very passe in an area of streaming everything that a battery-powered radio may be that lifeline of communication link to get information, because we have seen, even in large-scale—like Katrina—stations outside the area get broadcast in, but you had to have a way to receive the information.

Mr. CARSON. And lastly, Madam Durkovich, have our most critical transformers and substations within the bulk power system been identified so that we have a clear comprehension of system dependencies? And even cascading impacts from a widespread power outage, regardless of the cost?

Ms. DURKOVICH. Thank you very much for that question, Ranking Member Carson.

We work very closely with the utility owners, with our partners at DOE, as well as NERC and FERC [Federal Energy Regulatory Commission], to understand the most critical aspects of the electric grid. We have a number of programs that we leverage to help assess the vulnerabilities of these particular assets, and to work with owners and operators to help enhance the security and resilience to provide recommendations. But equally important, as you will hear later from Gerry Cauley, who is the president and CEO of NERC, we have a series of standards that are intended to guide the security of some of these most critical assets.

Increasingly within my office we are working to better understand the dependencies and interdependencies on some of these critical energy assets to be able to visualize what an outage is—the impacts it is going to have to other key lifeline sectors, and to be able to provide that information as leaders to include Administrator Fugate and those of the utilities working to get power restored. Thank you.

Mr. CARSON. Thank you, ma'am.

Chairman, I yield back.

Mr. BARLETTA. Thank you. The Chair recognizes Mr. Meadows for 5 minutes.

Mr. MEADOWS. Thank you, Mr. Chairman, for this important topic. I think this is one of the interesting aspects that I get asked about more than anything else.

Let me tell you why I am a little bit troubled here today is that I hear a lot of rhetoric that acts like we have our act together from a Federal standpoint, when really the vast majority of the job that gets done is really with the stakeholders, with those public utilities that, for years, have been prepared for mass outages, but perhaps the scope of the threat, the cyberthreat—and when we are talking about mass outages, you know, we can talk about Hurricane Sandy, we can talk about, you know, other storms. They are used to that.

I am just telling you, they have got—I used to work for an electric utility many years ago. I was around—I have got enough gray hair, I was around when the DOE was actually formed. And so when we look at this, to suggest that the Federal Government is here to help, I want to make sure that you are helping.

And the chairman talked about the real communication that is being done. The real communication that is being done is really being done by the public utilities at the local level. If any is getting done. You know, it is crickets when it comes to the other Federal agencies as it relates to this. Now, I say that as a criticism, only because we have to figure out that we are sick before we start to figure out the diagnosis and how to fix it.

So let me ask Assistant Secretary Hoffman for your help on one particular area. In your testimony you were talking about national security and how you can reprioritize and make sure that those national security interests are supplied by public utilities or governmental agencies.

Here is my concern. Many of our national security interests actually have their own generating and own distribution capacity. And

yet I find them woefully underprepared for cyberattacks. You know, some of them are primary metered at the point of entrance, so you may have a public utility providing the generating capacity. They do the distribution. So as we look at this, what kind of turf war do we get in between DOD [Department of Defense] and DOE with regards to being ready for a cyberattack that would have national security implications?

Ms. HOFFMAN. Thank you, Congressman, for that question. When we deal with any sort of event, we are going to act as a whole of Government. So, whether it is a cyber event——

Mr. MEADOWS. But who is in charge? Here is the problem, is—and I have dealt with a number of agencies. So we get FEMA that comes in, and we get local emergency management responses. And what you have is you have different people saying different things.

So with regards to national security, who is in charge of the power grid? Is it DOE or is it DOD?

Ms. HOFFMAN. The owners and operators are ultimately in charge of the power grid. The support to the power grid is going to come both from DOE with respect to working with the owners and operators to restore power and DOD has a responsibility with respect to national security and protection. So, from a physical security perspective, we may look at law enforcement to help the utilities protect substations. It depends on the event, but the response will be coordinated.

Mr. MEADOWS. All right. So you have a plan, a coordinated plan that I could look at today on how that would happen.

Ms. HOFFMAN. So for——

Mr. MEADOWS. That you can give to this committee in terms of the—because here is what happens, is most of the time an event happens and then you go out and you figure out the problems. You know, Mr. Fugate was talking about the fact that we learn lessons from each event that we have.

But the problem is, with a cyber event as we are looking at in the Ukraine, you know, here we have an outage to over 200,000 people, where it was cut off. But the real problem was—is they were in the system for almost 6 months and we didn't know about it.

So I guess the question is how many times are we getting attacked? And are they in our systems without our knowledge?

Ms. HOFFMAN. Well, you bring up a good point, Congressman, thank you. But the issue is every event and every incident, as Administrator Fugate brought up, is going to be different, and we are going to have to think about the capabilities. When somebody can take someone's access credentials, we have to think about that and look at that as an industry. So we are taking the lessons learned——

Mr. MEADOWS. But that is more of a physical threat. I want to go back to the cyber aspect, because what we are doing is—and I heard Ms. Durkovich talk about this—is that we are looking at risk management. And really, what we need to start to focus on is a real comprehensive plan on how we are going to partner with the private sector or public utilities on doing this, because what happens is we get a little check box and we say, "well, we have gone and we have talked to XYZ and we have asked them to make sure

that they are vigilant about cybersecurity," which most of them are.

But yet, what happens is we don't have a comprehensive plan at a Federal level to look at how we can support them in the event of a national attack that would come in the way of cyber. So I am not talking about storms, and I am not talking about stealing a credential. I am talking about the real attacks that we get hit with every single day.

Do we know—have we done a risk assessment where we have intelligence? And have we shared that with the public utilities? Because a lot of times we have this national security concern that we don't want to share that with an outside, you know, group because of national security concerns.

Ms. HOFFMAN. So thank you. You bring up very good points in your discussion.

First of all, we follow the National Response Framework. As Administrator Fugate talked about, regardless of whether it is a physical or cyber or weather-related event, we are going to act as a whole of Government in responding to that.

With respect to your question on intelligence, we are sharing information with the private sector. DHS and DOE regularly host classified briefings with the private sector to share actionable information. And that is the information that the utilities are able to take back and really do response force.

With respect to specific events such as the Ukraine incident, ICS [industrial control system] alert has provided very specific actionable information. DOE, working with the Electricity Information Sharing and Analysis Center, has provided actionable information to the industry to learn from these events and prepare. And that is what is important. Each event is going to be different. We have to take those events and learn from them.

Mr. MEADOWS. I have run out of time. I will yield back, Mr. Chairman. Thank you for your patience.

Mr. BARLETTA. Thank you. The Chair recognizes Mr. DeFazio for 5 minutes.

Mr. DEFAZIO. Thank you, Mr. Chairman. I regret I had to step out to go to a hearing upstairs. We should—the committee should look at not scheduling hearings in different subcommittees at the same time.

Administrator Fugate, I think you made a number of excellent points. And when you talked about being a ham radio operator, obviously that is a potential backup. But I was recently in Japan and one of their greatest regrets is that they didn't have enough deep ocean sensors, and they underestimated the size of the tsunami. And they did manage to get out a warning with that original estimate before the electrical grid went down in those areas, and they had no further capability of broadcasting and warning people. And therefore, many people sheltered in places that actually were below the crest of the tsunami and died.

So they have now moved to a cell phone-based system, and required resilient cell towers to be built. Are we looking at anything like that here, in the U.S.?

Mr. FUGATE. Yes, sir. Part of the charge you gave us and the FCC was to develop wireless emergency alerts, which, working

with the carriers, we actually implemented faster than we thought. So right now, every cell phone being manufactured today is required to be able to transmit a wireless emergency alert, part of the emergency alert system. Tsunami warnings are built into those.

So, if there is a triggering event, the originator for that will be the National Weather Service tsunami warning centers. In the case of Oregon it is going to be the Alaska Warning Center. It would go out. It is geocoded to the areas of impact, so those counties and communities at risk would get those notifications over your cell phones. You cannot—you don't have to opt in, you don't have to sign up. The only thing you can do with a cell phone is turn it off and not get the alerts. So, unless you have done that, a tsunami warning would be issued, it would be transmitted upon that point and go out.

I think you do point out, though, one of the challenges, which is why we work very closely at the local levels. It is hard to get the magnitude of the tsunami, so the evacuation zones pretty much have to be what is the maximum risk, we got to move now. A phased approach, we generally don't have time, particularly with Cascadia. It is too close to the coast. And that is why we tell people, "even before you get the warning, if you feel shaking you got to move to higher ground," because even with a warning you only have minutes to move.

But the cell phone system now, as soon as the Weather Service issues the warning, it will get transmitted to those areas. We have actually seen this occur already. But it has answered this question of what will wake people up in the middle of the night. And your cell phone buzzing and humming and making strange noises was the whole purpose of the wireless emergency alert system.

Mr. DEFAZIO. And when—phones manufactured after what date were required to have that, do you know?

Mr. FUGATE. It started—I believe it is—I would have to look at the exact date, but it has been about the last—2010, 2011.

Mr. DEFAZIO. OK.

Mr. FUGATE. That all new handsets—Apple, the iOS, was the last of the handsets to incorporate this in. And so pretty much all the new handsets now have this. And, as we see the replacement cycle of cell phones, we have actually now—third, fourth, fifth replacement cycles. So we are getting good penetration now with those systems.

Mr. DEFAZIO. That is great. Yes, I have actually been on an airplane here where we were held on the ground because of thunderstorms, and everybody's cell phone started buzzing as they had, like, a tornado alert or something. I can't remember what it was.

Mr. FUGATE. Yes, sir.

Mr. DEFAZIO. So that is great progress. To the Honorable Ms. Hoffman, just on the issue I raised earlier, you know, the transformer issue, it does seem really critical and they are very expensive, they are cumbersome, hard to move. But, I mean, where are you at in evaluating the potential or possibility of having some, you know, backup or replacement transformers in a strategic reserve?

Is it—you are analyzing that, or where are you at in that process?

Ms. HOFFMAN. Thank you very much, Congressman, for the question. The transformer reserve plan that was required as part of the FAST Act is in progress. We have contracted with Oak Ridge National Laboratory to do an assessment with respect to transformers, the transportation issues, any sort of where they would be placed, the volumes and size. As you are well aware, the transformers in the United States are quite unique, and we have to also look at a parallel process for how do we look at standardization, look at next generation transformer for additional manufacturing.

We are also in the process of assessing transformer manufacturing in the U.S. DOE has had several reports out with respect to transformer manufacturing. There are several manufacturing entities in the U.S., including EFACEC, Georgia Transformer, ABB, Waukesha, Prolec GE and Hyundai. Those are the transformer manufacturers in the U.S. Is that enough for the capacity we need? I would say we need more capacity with respect to transformers. So it is important that we continue to look at a transformer sharing program.

So we are in progress and on target to meeting that deliverable for the committee.

Mr. DEFAZIO. So what was the timeline that was established for the——

Ms. HOFFMAN. The timeline that was established in the FAST Act was 1 year from enactment. So it would be due in December.

Mr. DEFAZIO. OK, great. Are you aware whether or not the regional power administration, the Bonneville Power Administration, is, you know—I mean are you working with them? Because they obviously have most of the—are interlinked in some places with private, but for the most part provide for the, you know power transmission and—high-voltage power transmission. And half of that—well, part of it is DC. So we actually have two different sets of transformers.

Ms. HOFFMAN. So thank you very much for highlighting that. Yes, we are working with the power marketing administrations, which includes WAPA and Bonneville. They are a core asset to the Department of Energy, as well as a core asset to the electric infrastructure writ large. So they are a very important part of the conversation.

As required by the FAST Act, we will do consultation with industry and with experts in this area.

Mr. DEFAZIO. OK, thank you.

Thank you, Mr. Chairman.

Mr. BARLETTA. The Chair recognizes Mr. Perry for 5 minutes.

Mr. PERRY. Thank you, Mr. Chairman.

Secretary Hoffman, the FAST Act you were just discussing includes what you were just discussing, some additional roles and authorities. Can you talk a little further about the importance of the transformer reserve and what your thoughts on that are, particularly?

Ms. HOFFMAN. Thank you very much for the question. The transformers in the United States are a very critical component of the system. The FAST Act recognizes the criticality of these transformers, as well as the need to assess where are we at with respect

to any sort of need to develop a plan for transformer spare capacity.

So what this means is really evaluating the spare capacity in the United States and the ability to transport transformers. So where should a transformer stockpile, if necessary, be located because of the different sizes and dimensions of the transformers.

So part of the plan of what we are looking at with Oak Ridge National Laboratory, our other national laboratories and industry—is assessing the number of transformers, the size of transformers, meaning the different voltage classes, and then where those transformers could potentially be needed to be located because of transportation issues.

The industry has had discussions with the Class A railroads and looking at the transportation of transformers. You may not be aware, but a lot of substations are in very remote locations. So really, the criticality and some of the time is not only manufacturing the transformers, but it is actually the transportation of those transformers to a location.

Mr. PERRY. Will you be considering the timeline for manufacture of transformers, as well, in that study, and when is the—when can we expect the results?

Ms. HOFFMAN. Yes, the—we have started looking and have had several reports out with respect to transformer manufacturing. And those are on DOE's Web site. But the results of that will be included in the report in December.

Mr. PERRY. Do you discuss cost or reimbursement at all in your report?

Ms. HOFFMAN. So part of the request is to look at policy implications and the cost and financing of that. We are going to work within the Department of Energy with our energy policy and systems analysis group and assess what are some of the financial implications to setting up and developing a transformer reserve.

Mr. PERRY. All right, thank you. In my opinion, the EPA [Environmental Protection Agency] continues to over-regulate the energy industry. And with that, I don't think they have the ability to determine or examine the requirements.

Mr. Fugate, do you—I mean I am sure you are aware, based on what I have here, as of December of 2015 we are retiring—due to EPA policy, retiring or converting 81,423 megawatts, or 499 units, based on regulation. Has FEMA done an examination of how the EPA regulations affect the grid and the capacity? Are you interested in doing that? Do you know what the capacity is, and do you know the ramification of the loss of the 499 units and the 81,000-plus megawatts?

Mr. FUGATE. To be honest, Congressman, we really depend upon our partners and DHS that do that. We are not the subject matter experts. We determine for our infrastructure protection what that means and what those impacts are.

Having come from the State of Florida, I will tell you that, as we have seen these types of changes, we have seen dependency move from coal fire to natural gas to peaker units. So we had to start planning for what happens there. I actually was in probably a unique experience of having a natural gas pipeline sever due to lightning strike. Knocked out all the natural gas to the southern

and middle parts of the State. And we suddenly realized that we had a tremendous dependency on natural gas peaker units, and we were fortunate that we had mild weather. Otherwise, we would have had generator capacity shortfalls that would not be made up. So we——

Mr. PERRY. So if I could just——

Mr. FUGATE [continuing]. Partners for the information——

Mr. PERRY. I got a limited amount of time here. So if FEMA is not doing it particularly, who are you getting the—which partner are you getting that information from? Who is assessing the effect of the regulation, the loss of capacity and the timing of that loss? Who is doing that, of your partners?

Mr. FUGATE. I would depend upon my partners to the left. We look at energy as a function of Government, because, as you point out, there are numerous parts of the regulatory and response structure. So we concentrate onto function——

Mr. PERRY. So, with all due respect, may I ask your partner to the left? Do you have that information? Are you tracking that?

Ms. HOFFMAN. So thank you very much for the question. The Department does look at reliability implications with respect to any sort of change in generation mix in the United States.

With respect to the Clean Power Plan, it is really going to be as the States develop their implementation plans the assessment will occur with the regional reliability entities and the independent system operators, where they will coordinate and understand the reliability impacts.

Mr. PERRY. So you don't know what it is upfront, or you don't assess it as it occurs? You don't know that, you know, so many plants and so much capacity is leaving in Ohio or Pennsylvania or Alabama, you don't know that in advance and make an assessment of the potential risk that is involved?

Ms. HOFFMAN. So—thank you. From a widespread reliability point of view, DOE believes that the Clean Power Plan and the regulations will not have any widespread reliability impacts. But the specific——

Mr. PERRY. Well, hold on a second. Hold on. With the chairman's indulgence—you believe that, but do you believe that because you have empirical data to support that belief, or you believe that because somebody is telling you that, or you believe that because you don't have any reason to disbelieve it?

Ms. HOFFMAN. Right now the utilities will work very hard to ensure reliability of the system. And our past experience is, as any sort of any reliability concerns come up, there is strong coordination within the industry to address any sort of reliability impacts. So——

Mr. PERRY. So does that mean, if you thought that there was going to be a reliability impact based on the regulation and the capacity reduction that you would essentially exonerate or waive the requirements for a period of time to make sure that the capacity remains? Do you have a policy to do that, or is there a thought to that? Or what is your plan, if you come up against something that doesn't comport with what you think it needs to be, from a capacity standpoint?

Ms. HOFFMAN. Within the Clean Power Plan the States, as they develop their Clean Power Plan, their State plans, they will be coordinating with the reliability entities, the ISOs [independent system operators] and the RTOs [regional transmission organizations], looking at any potential reliability implications, and——

Mr. PERRY. But how does that work since, for instance, I live in the PJM, which is a multistate organization? It is not State by State, it is multistates that all feed into the same grid. So how does one State's plan affect another, and how—who coordinates reliability or capacity issues in that regard?

Ms. HOFFMAN. So the States are required, as part of the Clean Power Plan, to coordinate with PJM, and PJM has and will continue to do reliability analysis for that region.

Mr. PERRY. Thank you, Mr. Chairman. I appreciate your indulgence.

Mr. BARLETTA. Thank you. The Chair recognizes Mr. Sires.

Mr. SIRES. Thank you, Chairman and Ranking Member, for holding this hearing. It is very important.

I represent the Eighth District of New Jersey, which has Hoboken and some other areas—Jersey City—which got hit very hard by Sandy. And if I learned anything about our infrastructure, it is how unprepared we were for a storm or anything else. And there is plenty of blame to go around. Everybody always points to the Federal Government, but in reality the States could do a lot of things and the locals could do a lot of things and the power companies could do a lot of things.

I always think of the example—and I gave this once before to the chairman as an example—there was a generator in the flood zone. And the power company was protecting it with a chain link fence. So when it flooded, obviously, the chain link fence did not hold the water back. So what I am trying to get at is these are the kind of simple things that we can do to protect, you know, this particular transformer.

The other thing was in terms of the gas station. You were talking about—I mean we have plenty of gas, quite frankly, but they couldn't pump it. So a simple thing like a small generator to just move the pump and move the gas from the—you know, from the containers to the people, I mean, would it suffice? So when I say to you that everybody has shares of blame in this, I just hope that we have come from Sandy far enough to learn some of these mistakes and we are correcting them.

So, Honorable Fugate, would you please tell me that we have come a long way from where we were?

Mr. FUGATE. We have come a long ways, we haven't gone far enough. And I think, Congressman, you point out what I see is the real challenge, and which cyber highlights. The tendency is to plan for what we are used to dealing with, not for what could happen.

And so, again, as you point out, we put a fence around a generator in a flood zone. Well, the reason you have a generator is the power goes out, one of the likely causes for power outages would be a coastal storm. But you hadn't had one in a long time, so you were more concerned about somebody breaking in and damaging the transformer. And that is the trap we fall into.

And I think this is what the chairman is raising. Cyber is new. A lot of things we are going to do won't be new in response to the consequences, but if we don't know what we are planning against, we may run the risk of only planning for what we have been used to having, maybe short-term power outages, maybe disruptions that are strictly local, and not plan for what could happen and plan against it.

And unfortunately, as you point out, we try to promote these lessons, but it seems to, again, be one of our challenges. How do you get people to change? Let's talk about gas stations. That is a private entity. Putting in a generator is a cost. Most people say, "well, you could just ship a generator there." Doesn't work that well, because most of those utilities were underground and it was hard to get a generator hooked up to it.

So in some States that have dealt with this they have put in incentives that gas stations would be required through regulation to put in a transfer switch. It was a good compromise. That way, if they did lose power for long periods of time, we could get generators in there, hook it up, and pump gas.

But this is where we got to be very careful. It is easy to say, "this is the fix" until you ask who is paying for it. And I think this is the tradeoff of what would make sense, either through incentives, tax credits, regulatory oversight, to get these changes, because I can't ask a business to lose money if their other partners or competitors aren't doing the same thing.

And at the same time, you know, the response was, "you got to put a generator in every gas station." That is also not necessarily a great idea, either. But putting in a transfer switch was a good compromise.

So again, I think, as we learn these lessons we go back to this trap of we plan for what we have experienced in the past, and that does not always scale up for the future impacts. We have got the lessons learned, we are putting the information out there. But the receptiveness of that audience is oftentimes based upon do they perceive this threat as applying to them.

And, as you know for your community, we talk about hurricanes and hurricane evacuations, and most people said, "we don't have hurricanes, we have northeasters." So it is getting people planning. In many cases we know what these impacts are, but it is really the challenge of getting people to plan for what can happen, not what they are prepared to do based upon only their past experiences.

As the chairman points out, we have not had a lot of experience with cyber. So part of this, again, is getting—what are we planning against, and then what will we do differently. And if that requires resources, where are those resources coming from?

Mr. SIRES. I also think that we have to be prepared post-Sandy or post—because one of the issues—we still have problems in New Jersey where people are still out of their homes years later. And to me that is really unacceptable, 2 or 3 years later, that we have these issues where people with the insurance or with the valuation of the property—I mean somehow we have to be prepared for some of these things because it impacts real people.

Mr. FUGATE. It does. And our experience is, coming out of Hurricane Katrina, 5 years after that we still had over 5,000 families living in travel trailers because we didn't have the right answers.

So, rebuilding after disaster is, again, very time consuming. There's a lot of hurdles to go through. And I agree, it is ideal to get people back in their homes as quickly as possible. But that requires a lot of things that go beyond even some of my programs. It is really, as you point out, State and locals and——

Mr. SIRES. I am not just putting the blame on you, I am also putting the blame on, you know, the locals and the State, that we should be prepared for any of these storms or whatever we have.

Thank you, Mr. Chairman.

Mr. BARLETTA. Thank you. The Chair recognizes Mr. Massie.

Mr. MASSIE. Thank you, Mr. Chairman. I am going to yield as much of my time as he might consume to the gentleman from North Carolina.

Mr. MEADOWS. I thank the gentleman from Kentucky for yielding. And, Ms. Hoffman, I want to follow up on one thing. Because, as you talked about the transformers and the—having these backup transformers as a redundancy, one of my major concerns is that decisions that get made by DOE or DHS or FEMA—all the sudden what we do is we transfer that liability to others that are providing service.

So what we—you know, right now all utilities have backup transformers, primarily for distribution purposes, but even for larger, you know, transmission-related transformers and switches. However, if you are going to make a decision, it directly impacts rateholders for two reasons. I mean if they are—happen to have $10 million transformers sitting there, I don't know that they can get a return on that investment, necessarily.

And so, if you start to extrapolate that out, if it is not in service, you know, it just kind of like—generated capacity, there is a certain length of time that they have in order to bring that online so that they can get a return. But ultimately, it affects the ratepayer, anything that you do.

And so, I guess when we start to look at the security implications, what I would encourage both of you to do is look at it as we would from FEMA—is that it is a Federal redundancy that is required, not a redundancy that needs to be done by utility to utility to utility. Do I have that commitment from both of you, that you would look at it as a Federal obligation, versus a private obligation?

Ms. HOFFMAN. Yes, Congressman. Thank you.

Mr. MEADOWS. All right. OK. I see you nodding your——

Ms. DURKOVICH. Yes, sir.

Mr. MEADOWS. For the record——

Ms. DURKOVICH. Yes, sir.

Mr. MEADOWS [continuing]. Both of them said yes. And so let me finish with one other, I guess, concern. When we are talking about sharing in a classified setting with the stakeholders, have all of the utilities participated in that secured setting, where you have let them know of both the threats—potential and real threats that we already have experienced?

So, you know, you were saying that we have done that in a classified setting, and I just find that interesting. I am not challenging, but I want to drill down on that because I don't know of too many—you know, maybe the big utilities but there are, you know, hundreds of utilities. And so they come in to a classified setting and say, "this is your risk, this is where it is." That is your testimony here today.

Ms. HOFFMAN. So thank you for that question. Information sharing occurs at multiple levels. We do have classified information with the Electricity Subsector Coordinating Council, which is 30 CEOs from across the whole sector, so there are investor-owned utilities, there are municipals, there are co-op utilities that participate in that information sharing, that classified information.

In addition we have had 1-day read-ins where we have brought a larger section of utilities in to do classified information sharing. We have done that. DHS has done regional information sharing meetings, where they have had opportunities to bring folks in and do information—so it occurs on multiple levels. Have we hit every single of those——

Mr. MEADOWS. Yes, and I am not saying—I want it to be systemic, and I guess I will yield back to my good friend from Kentucky here in just a couple of seconds, but I want to make sure that I am clear. As we get to stakeholders what I want it to be is more than just a box that we are checking off. I want EEI [Edison Electric Institute], I want all of the groups that are there to buy in and say, "we have a plan." We do it for mass outages like Sandy and other hurricanes. We haven't done that, I believe, adequately as it relates to cyber. And do I have both of your commitments that you will redouble your efforts to include them as stakeholders?

Ms. HOFFMAN. Yes, yes, we will redouble our efforts. And the one thing that I would say codifies how we are redoubling our efforts is the exercise that happens between industry and utilities where we are actively exercising this.

Mr. MEADOWS. I will yield back to my good friend.

Mr. MASSIE. Thank you. I just have a brief question that occurs to me during Mr. Meadows' question which is, of this classified information, if we sought to get a brief on that would you make yourself available in a classified setting for us, as we contemplate what sort of legislation might be necessary?

Ms. HOFFMAN. Yes, Congressman. We would be glad to have a briefing with you.

Mr. MASSIE. Is that the case for everybody?

Ms. DURKOVICH. Yes, sir. Of course.

Mr. MASSIE. Mr. Fugate?

Mr. FUGATE. I wouldn't originate most of the data, but I would be there. Most of the origination of the classified information would actually come from my partners to the left.

Mr. MASSIE. Understood. Thank you very much. And I yield back.

Mr. BARLETTA. Thank you. With respect to time for our second panel, we are going to move on. And I think, if I can summarize—and I thank you all for participating today—I think if I could summarize, Administrator Fugate, that planning for local and State governments should be—needs to be in terms of weeks, not days.

And that is important because that is the first time I have actually heard what we need to begin to look at in the event of an attack.

So again, I want to thank you all for your testimony. Your comments have been very helpful in today's discussion. And we will now call on our second panel.

[Pause.]

Mr. BARLETTA. I remind you of the subcommittee's request to limit your oral testimony to 5 minutes.

Mr. Cauley, you may proceed.

TESTIMONY OF GERRY W. CAULEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION; WILLIAM H. SPENCE, CHAIRMAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER, PPL CORPORATION; AND BOBBI J. KILMER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CLAVERACK RURAL ELECTRIC COOPERATIVE

Mr. CAULEY. Good morning, Chairman Barletta, Ranking Member Carson, and members of the subcommittee. Very glad to be here today, testifying. My name is Gerry Cauley, I am the president and CEO of the North American Electric Reliability Corporation. NERC is a nonprofit international organization overseeing the reliability and security of the power grid in the United States, Canada, and a portion of Mexico. We have authority assigned by Congress to develop and enforce standards affecting reliability and security of the grid, and that authority is overseen by the Federal Energy Regulatory Commission.

We can all agree that electricity is the most critical lifeline sector for national security, for other lifeline sectors like finance, water, and transportation, for the economy, and for public safety. Every day we are reminded of the seriousness of our job related to securing the grid. There have been terrorist attacks in France and Belgium and even here, domestically. There have been cyberattacks and data breaches across various industries and across Government.

Of particular relevance to our grid, on December 23, 2015, there was a cyberattack in the Ukraine which was launched against three distribution companies and in which the perpetrators gained control of three distribution companies and were able to put out the lights for 225,000 customers for up to 6 hours.

A team from the U.S. went to investigate that incident in the Ukraine, including a member of the NERC staff. And what I can tell you is that the cyberthreats are real, but I think we have a very different situation in the Ukraine as compared to what we have in the United States and North America. Our security controls in North America are very different.

We are the only industry with mandatory and enforceable reliability standards affecting physical and cybersecurity. We are currently in the fifth generation of our cybersecurity standards. They are risk-based standards based on NIST-type [National Institute of Standards and Technology-type] controls, so they are adaptable and can keep up with the current threats.

We have a very robust compliance monitoring and enforcement program. System operators use modern controls to ensure the secu-

rity of the system, including separation of corporate and business systems from control systems, physical access controls, patch management, aggressive threat hunting and mitigation, and employee and contractor training, and many other measures that they take.

We have established the Electricity Subsector Coordinating Council, as we heard previously, at the highest levels of industry and Government, including CEOs and top officials from Government. The CEOs and boards of power companies take security very seriously, and security is one of their highest priorities on a regular basis.

Our Information Sharing and Analysis Center, which you have heard about, the ISAC, provides robust information sharing regarding cyber and physical threats. With the engagement of industry leaders we have recently gone through a review and upgrade of the capabilities of the ISAC, and the ISAC, I believe, is closely integrated with the security operations and information sharing at individual companies, as well as the State fusion centers and other sectors.

We also operate a tool called CRISP [Cybersecurity Risk Information Sharing Program], which is a way to monitor the electronic Internet traffic to key sites around the industry, and compare the traffic to threats and vulnerabilities that we are aware of worldwide, and warn the utilities about issues that they may be experiencing in real time.

In the unlikely event of a successful cyber or physical attack, I believe that we are well prepared. FERC and NERC recently completed a study of the restoration and recovery capability plans and drills and exercises of nine major companies in the industry, and that report is available publicly, and it is posted on the NERC Web site. But I think it demonstrated that the preparation is there, and that the plans have been exercised.

As you have heard before, on November of this past year NERC led what I believe is the largest grid security exercise in the world called GridEx III. Over 400 entities in North America participated. We had over 4,400 registered users and, in my estimation, there were probably closer to 10,000 actual participants. The distributed—this is where we are in a central, controlled place, and we inject the attacks outward, and so the power companies are actually engaged in the exercise locally in their own control centers, in their own substations and power plants. They are receiving the information from us.

That portion of the exercise—I apologize for my voice; I am just getting over a cold—that portion of the exercise lasted 2 days and on the second day there was an executive tabletop which brought it all together for senior executives from industry and Government. The scenario included cyberattacks, physical attacks, including active shooters, truck-mounted and explosive devices, and unmanned surveillance drones. This hypothetical event was extreme, and it was intentionally extreme to really go beyond our capability and to test the system. And really, the point was to find out what can we learn and what do we need to do to improve.

During the distributed play exercise we caused outages in a simulated fashion—no one was actually controlled or affected, but we simulated 5 million customers who were out. And in—during the

executive session, to invoke all the policy questions at the national level that we were looking to pull out we actually had 15 million customers out and those outages were projected to be extended for weeks and even into months to really push the questions that the chairman is trying to raise today.

Participating entities worked through their emergency procedures. They had very extensive contacts with local law enforcement and first responders. And actually, those local government officials and first responders did participate in the exercise. We had—in the exercise we had the White House, DHS, DOE, Department of Defense, Cyber Command, NSA [National Security Agency], NORTHCOM [U.S. Northern Command], FBI [Federal Bureau of Investigation], FEMA, and the Illinois and Wisconsin National Guards are some of the players who participated directly in the executive exercise.

A number of key takeaways were to make sure that we are able to better coordinate between industry and Government in terms of the situation assessment, and what do we communicate to the public. It will be a constant race with regard to information to the public. We all know social media and the news are very quick, and we want to make sure that we are getting reliable information out to the public.

We are focused on ensuring unity of effort and unity of scale, and that we can resolve all of our resources from both industry and Government together.

Looking forward, I would say in this exercise we will continue to expand the role of State and local governments and participants in the exercise to make sure we can exercise some of the things that the chairman is looking to get here, which is how do we engage, how do we inform, and how do we set expectations.

And I look forward to your questions, thank you.

Mr. BARLETTA. Thank you for your testimony, Mr. Cauley.

Mr. Spence, you may proceed.

Mr. SPENCE. Good morning, Chairman Barletta, Ranking Member Carson, and members of the committee. My name is Bill Spence. I am president, chairman, and CEO of PPL Corporation. We deliver electricity to more than 10 million customers in the U.S. and the U.K. Beyond my role overseeing PPL's operations, I am also on the EEI Policy Committee on Reliability and Business Continuity. I also am a member of the Electricity Subsector Coordinating Council that you heard about earlier today. The ESCC serves as a principal liaison between the Federal Government and the electric power sector to protect against cyberthreats to the Nation's power grid.

Protecting the Nation's power grid, as you heard earlier, is not only a top priority of the Federal Government, it is also a top priority for the industry. We have a very strong record of working together closely in all kinds of disasters and storms. Along with our Government partners, we identify, assess, and respond to all threats.

The electric sector takes a defense and indepth approach to protecting grid assets. This approach really includes three key elements. The first is rigorous mandatory enforceable and regularly audited reliability standards. Gerry talked about that in his testi-

mony. Also close coordination among industry and with Government partners at all levels. And thirdly, efforts to prepare, respond, and recover, should power grid operations be affected.

Our industry already maintains hundreds of spare transformers. I don't believe that came up earlier, but you should be aware of that. In addition, we just recently launched, as an industry, a new project called Grid Assurance. Under Grid Assurance, many of the major utilities in this sector are coming together to establish regional centers where we will not only store spare transformers, but other critical equipment necessary to quickly recover the power system in any type of an event.

Among all the critical infrastructure sectors, you should know that the electric sector invests more annually than any other critical infrastructure sector. Last year alone we invested more than $100 billion.

Regarding security standards and regulations, as you heard we are subject to NERC's reliability standards. Entities found violating these standards face penalties of up to $1 million per violation per day. In fact, our industry is the only industry subject to mandatory, federally enforceable cyber and physical standards.

The industry is also implementing requirements for physical security as part of a broader suite of NERC standards, and using voluntary standards, as well, to drive improvement. Secondly, we are coordinating closely with the Federal Government, sharing threat information between the Government and industry to protect the grid.

According to the National Infrastructure Advisory Council, the electric power sector is viewed as a model for how other critical infrastructure sectors can more effectively partner with the Government. Our intent is to keep it that way. The Electricity Subsector Coordinating Council brings senior Government and industry executives like myself together with agency officials to improve sectorwide resilience against all hazards and potential threats.

The ESCC and our Electricity Information Sharing and Analysis Center offer programs like the Cybersecurity Risk Information Sharing Program, as Gerry also mentioned, through which we share information on potential threats. This is an area where I think the Federal Government has been very helpful to the industry, by allowing us to utilize proprietary hardware and software that was developed at the national labs and is now helping to protect the grid.

Over 75 percent of the U.S. customer base is covered by industry participation in this critical program. The ESCC has also focused on several other key areas, including planning and exercising responses to major disruptions. Our last exercise was a combined cyber and physical threat scenario.

In addition, we are focused on rapid threat communication amongst share owners and stakeholders. We are also developing Government-held technologies on electric power systems that improve situational awareness and cross-sector coordination.

Last but not least we are focused on incident response and recovery efforts. Electric power companies continuously plan and exercise for a broad range of potential threats. We share crews and equipment in times of trouble, and we regularly drill for potential

emergencies. For our part, PPL is actively engaged in the industry efforts I have highlighted, and pursing an aggressive defense-in-depth approach to protecting the power grid.

Thank you, and I look forward to your questions.

Mr. BARLETTA. Thank you for your testimony, Mr. Spence.

Ms. Kilmer, you may proceed.

Ms. KILMER. Chairman Barletta, Ranking Member Carson, and all members of the committee, thank you for inviting me to testify today on how electric cooperatives manage the consequences of a power outage.

Regardless of the cause, getting power restored quickly and safely requires advance thinking and planning. My name is Bobbi Kilmer, and I am testifying today on behalf of Claverack Rural Electric Cooperative and the National Rural Electric Cooperative Association.

Claverack delivers electricity to member owners at over 18,000 locations in rural northeastern Pennsylvania. We have low consumer density, averaging less than six consumers per mile of line, and we serve primarily residential accounts. We are 1 of Pennsylvania's 13 electric cooperatives, and our electric distribution system is not directly connected to the bulk power system.

The National Rural Electric Cooperative Association, NRECA, is the service organization dedicated to representing the national interests of electric cooperatives and their consumers. NRECA represents more than 900 not-for-profit, consumer-owned rural electric utilities that provide electricity to over 42 million people in 47 States.

Electric co-ops are accountable to their consumer members. Those same members own and govern the co-op through a locally elected board of directors. Electric co-ops reflect the values of their membership and are uniquely focused on providing reliable energy at the lowest reasonable cost.

Responding to power outages is a major part of our business. Assessing the situation, knowing who to call, and determining how to proceed is imperative, and it requires coordinated efforts in the public and private sectors during major events. One of the seven principles of the cooperative business model is cooperation among cooperatives. This cooperation is integral to our emergency planning and response.

In Pennsylvania, as in many States, the electric cooperative statewide association plays an important role in emergency coordination. Electric co-ops have mutual assistance agreements between one another so that during a major event the process of securing additional crews and resources is simplified. There is also a national cooperative database which facilitates cross-state mutual assistance. As I noted in my written testimony, this network helped our statewide association secure crews from Florida to assist us in our restoration following Hurricane Sandy.

Also important are the relationships that we have with State and local government agencies. During major events our statewide association is in regular contact with the Pennsylvania Public Utility Commission and the Pennsylvania Emergency Management Agency. The statewide association communicates outage information as well as requests for assistance from other governmental divisions

on our behalf. Locally, we are in touch with our county emergency management agencies. We advise them of outages in their counties and expected restoration times. This allows them to coordinate with other organizations like the Red Cross to set up services such as warming shelters.

We also have close relationships with our local police and fire departments, and along with other agencies and utilities we too participate in tabletop exercises which simulate emergency scenarios and strengthen our community networks.

Communication with our members is important, too. We always provide the option to speak with a live customer service representative. We use outgoing telephone messages, informational postings on our Web site and social media, and use radio and television broadcasts, which could be used, even in the event the Internet is down, to keep members and the public informed about outages.

We test our business continuity and disaster recovery plans annually, and we have plans in place so that we could operate from a remote location, if necessary.

Cybersecurity and awareness is a critical part of our operational preparedness. Though we are a small utility, we strive to follow industry best practices, such as the use of network scanning and intrusion detection programs in protecting our operational data, as well as our business and member information. We also participate in the Pennsylvania Department of Homeland Security's Task Force on Cybersecurity.

Our preparedness in the field is tested throughout the year during localized outages caused by weather events and other conditions. Lessons learned through experience, along with the coordination with our national, statewide, and local networks would form the basis of our response to a national or cyber event.

Again, thank you for the opportunity to testify today on our emergency preparations and recovery efforts.

Mr. BARLETTA. Thank you for your testimony, Ms. Kilmer. I will now begin our first round of questioning. And this question is to all.

I am going to ask you the same question I asked our first panel. What is the planning scenario that State and local governments should be using for a cyberattack on the electric grid? Will the power be out for days or weeks or months, considering both a cyberattack and a physical attack? The worst-case scenario, how widespread could the outage be?

Mr. Cauley, NERC runs an exercise on the failure of the grid. What scenario do you use? And I will let you begin.

Mr. CAULEY. Thank you, Mr. Chairman, for the question. As I mentioned in my presentation, we do probably pose a scenario that is 10 times beyond any sort of realistic expectation, in terms of the magnitude. That is really to test and sort of shake this out and see what we can do.

I think the difficulty in understanding the question is that there is many kinds of hazards that can cause outages. And in fact, if we look at—we do a lot of data and analysis about what causes blackouts. That is one of our jobs. And since 2011—so 4 years running—in our data weather has been in the top 10 causes of all major outages in North America. So we have that sort of baseline.

So the question for me, I phrase it as what kinds of things can cause outages from a few hours up to 2 to 3 days? And there are a lot of things that can contribute toward that and what kind of response capability we could have. So it could be storms, it could be equipment failure, it could be a number of things.

And then I think, as we get to the kinds of things we are talking about here, in terms of cyber and physical attacks, I think it is reasonable to ask—and severe storms, ice storms, hurricanes—it is reasonable to ask the question, "How are we taking care of people in a 1- to 2-week outage?" It may not be everywhere, but it might be in some local areas, it might be some cities that could reasonably be facing a 1- to 2-week outage.

But I would hate for us to say, "it is a cyber event," or, "it is a storm," because, really, the public safety issue is very similar. The major difference would be—to me, the major difference would be we know there is some kind of security concerns, law enforcement would be involved. But it is still the same fundamental—without electricity, you need to take care of people, you need to get them fuel and food and water, those kinds of things.

The one scenario I think that is the exception—and I think it was appropriate that the committee participated in the legislation around spare equipment—the one scenario I think realistically concerns me longer than the 1- to 2-week timeframe is damage to spare equipment, particularly the transformers. That could happen from a bomb blast, shootings, other—GMD [geomagnetic disturbance] storms. The question is not what caused it, but the question is what are you going to do if you lose transformers. And they are not going to be replaceable for an extended period of time.

Mr. BARLETTA. I guess what I am getting at, what—I want to get this down—to connect the dots down to the local and State. And you know, I feel pretty confident that getting to that point we have got all the ducks in order. I am just concerned that there is a missing link to what should the States and local governments be preparing for or planning for in length of time, because they need to do the same thing that you are doing. They need to know the scenario of worst-case, what do we need to prepare for.

Mr. CAULEY. Right. And I have been doing reliability for 35 years. I really think there are two levels. There is normal expected, you would see a number of times a year, is that 1 to 3 days as a normal kind of scenario that everybody should be prepared for. I think a 1- to 2-week scenario is a scenario that, if you are prudent, I would be talking with the mayors and the city councils about what you can do to be ready for a 1- to 2-week outage in the extreme case of hurricanes, earthquakes, and those kinds of things. My only exception is spare equipment damage may be more challenging.

But I think it really is independent of the cost, whether it is cyberattack—I can't imagine a cyberattack that is going to damage equipment to have an outage more than hours or days.

Mr. SPENCE. I would agree with Mr. Cauley. I think the prudent thing would be the same as what we are doing today for devastating storms, which is really a 1- to 2-week outage preparation.

I think there are a lot of resources that are currently available to local communities, both at the State and the local community

level that are really great resources that, unfortunately, I don't think all the towns and communities take full advantage of. There are a lot of really good best practices that have been used by towns and cities that have been more experienced with devastating storms. For example, the State of Florida has a lot of experience, so there is a lot of lessons learned there that are available to towns and communities.

I think the other thing—and I think this was mentioned by the representative of FEMA earlier today—it really boils down to, in many cases, the probability of the event happening, the risk of the event, and willingness to put in place and spend the money for backup generation or other backstops that would be necessary for a 1- to 2-week event. So I think that is where I would direct the towns and communities to be aware of what is available, utilize that fully, and then make the critical investments that they need to survive a 1- to 2-week period.

Mr. BARLETTA. OK. I am going to connect the dots. So do you think it is the Federal Government's responsibility or the State government's responsibility to make sure that the local government is doing all that? Because I am just concerned that we are going to have everybody pointing fingers at each other, "well, I thought you had said," "I thought you did," and nobody did.

Whose responsibility should it be that we make sure that the local governments are prepared? Because today is really the first time that I am hearing a length of time.

Mr. SPENCE. Right.

Mr. BARLETTA. And you know, in my own mind—again, I am going to keep putting that mayor's hat back on—I am beginning to think, well, geez, if it is 1 week or 2 weeks, there's a lot of things I need to be prepared for here, and we are probably not.

Mr. SPENCE. Well——

Mr. BARLETTA. Which means that most cities are probably not prepared——

Mr. SPENCE. Yes.

Mr. BARLETTA [continuing]. And I think that is what this hearing is about——

Mr. SPENCE. Right.

Mr. BARLETTA [continuing]. Is really to raise a red flag here today that we are not prepared in the event of something drastic, major, unlikely, but could be——

Mr. SPENCE. Well, a couple comments, Mr. Chairman. First I would say—and you probably would not want to hear this, necessarily, but I think it is a shared responsibility between local government and the Federal Government. And I really do believe that because you are just not going to be able to have Federal boots on the ground in all these local communities to get the communities back up and running.

Secondly, I would say that, you know, there are things that the local utilities do have at their disposal to help local communities in terms of communication and even backup generators, portable generators, that we can deploy to high-priority areas to make sure that when we need to restore the system and we can't do it in a timely fashion, then at least there is some basic level of service that we can provide.

So I think in an extended period of outage, you are still going to have power to certain areas. You are going to have a backbone of power. It may not be this town or that town. But I think, collectively, there will be ways to get resources available to the local towns and communities.

You know, to be quite frank, I was very skeptical when we started this Electricity Subsector Coordinating Council, on whether the Federal Government was really going to be able to help us, as an industry, to restore power quicker. But I have been pleasantly surprised at the level of cooperation and collaboration that has gone on in the last 3 to 4 years. And there are simple things like providing fuel that we desperately needed during Hurricane Sandy to restore towns and communities in New Jersey and Pennsylvania.

And there are other things, like providing beds for crews that are coming from out of State. We were able to access barracks at the Department of Defense facilities. We were able to access portable generators. We were able to access experts in emergency response. So there are some things that the Federal Government can be very, very helpful for.

And I think, now that we have a playbook that really dictates who does what when, which was always my concern in a major event—who do I call, and are they going to be ready for that call—I can say that, from what I have seen so far, I believe we are more ready than we have ever been in the past, and we have a very good system and a playbook that we can go right down the line and have access—in this case, when we are talking about this committee—to cyber resources at the highest levels of the Federal Government.

Mr. BARLETTA. Thank you.

Ms. Kilmer?

Ms. KILMER. I agree with my fellow panelists on the shared responsibility.

I would also like to emphasize to the subcommittee the importance of communications during crisis periods. My experience has been that sometimes it is not the length of the outage, but simply knowing how long it is going to be, or what the expectation is. It can help both residential consumers, as well as townships and towns, understand how they need to plan.

I would also like to add one thing that we have seen in our rural area, especially since Hurricane Sandy, and that is a focus on individual preparedness. I am seeing our local county emergency management agencies doing a great job in trying to educate the public on being prepared. We try to do the same thing. Of course, we are in a rural area, we are subject to many weather events. So I think that our consumers are relatively prepared. And again, I am not suggesting that we can rely on that, but I think that that is an element in all of this. Thank you.

Mr. BARLETTA. The Chair recognizes Ranking Member Carson.

Mr. CARSON. Thank you, Chairman Barletta.

Ms. Kilmer, you mentioned that Claverack Rural is not connected to the bulk power system, but you receive services from a subtransmission system. What does that mean for your cooperative in the event of a nationwide cyberattack on the grid?

Ms. KILMER. In the event there was a cyberattack that took down the grid, we would be affected by that. If Penelec's transmission

system was affected and power was disrupted to our substations, we would also be out of power.

Mr. CARSON. Mr. Cauley, there was a newspaper article yesterday that indicated that the FBI and the Department of Homeland Security have been warning the power industry over the last month about a potential cyberattack. What role has the Electricity Information Sharing and Analysis Center—what role might they play in distributing this kind of information?

Mr. CAULEY. Thank you, Congressman. That is exactly really what the Information Sharing and Analysis Center does. We—in fact, I am not aware of that particular one, but we do dozens of these a day. We get information out, post it to industry. We have several thousand participants in industry who receive those notices every day.

Mr. CARSON. Yes, sir.

I yield back, Mr. Chairman. Thank you.

Mr. BARLETTA. The Chair recognizes Mr. Meadows.

Mr. MEADOWS. Thank you, Mr. Chairman.

Mr. Cauley, did I hear you correctly? You said that in the event of a cyberattack, the longest period of time that people would be without power—an hour? Is that what you said?

Mr. CAULEY. Thank you for allowing me to follow up on my—whatever I said. My point——

Mr. MEADOWS. Sometimes I don't hear correctly, but I just wanted to give you a chance——

Mr. CAULEY. The point I was trying to get to—but I rushed—was it is a very difficult form of attack to go from a cyberattack—it is easier to steal information or disrupt electronics. It is very technically challenging to go from an electronic cyberattack to causing physical damage to equipment.

Even in the Ukraine attack there was no damage to the equipment. It was opened, the breakers were operated to basically shut down the feeders that were going to the customers, but there was no damage, so that once they realized what was happening they basically could defeat the computers and have people go to the station manually, flip the switch, which is a mechanical switch, and put the power back on.

So, my point—and I would love to continue working on this and getting some actual data to support that—is it is very hard to transform from a cyberattack into long-term damage that would be measured in weeks or months——

Mr. MEADOWS. All right.

Mr. CAULEY [continuing]. Because you have to hurt the equipment to do that.

Mr. MEADOWS. OK. And that is really my focus, is not turning a switch off here or there or, you know, tripping a breaker or, you know, making a jack go out. That is minor.

I guess the type of cyberattacks that we are seeing and hearing about in classified settings not directly related to the electric utility business are very sophisticated. And so, being able to come in and—so I assume, you know, going into a generated capacity—so let's say you got a generator and you—you know, there is all kinds of controls and switches to make sure that you don't run into problems with the electrons, let's put it that way.

And so, all the sudden, somebody coming in with nefarious—not just turning a switch off, you know, can scramble it in such a way that it would create unbelievable damage, certainly from a standpoint of generated capacity, I mean—I don't want to talk about it in an open forum like this, but I guess my concern—are you not having those kinds of conversations which are more than just turning the power switch off, as happened in the Ukraine, but really causing long-term damage either to generation capacity or transmission capacity?

Mr. CAULEY. Yes, Congressman. I have the privilege of going to very similar highly classified briefings, as well. But I also have 35 years of experience working in substations with equipment. And I understand the threats of black energy or aurora, or those things. It is very difficult to transform an action—the predominant behavior we are seeing today is surveillance-type behavior. But to transform that into an action that destroys a piece of equipment is technically very——

Mr. MEADOWS. Well, that is comforting to know. I mean——

Mr. CAULEY [continuing]. Very complex.

Mr. MEADOWS. And so that is real comforting, because what I am going to do is I will follow up with both you and Mr. Spence as it relates to this because, you know, again, it is one of the number-one questions that I get, is just a real concern. You know, it is about hitting the grid. And most people don't understand the interconnectivity between utilities. And so a lot of that gets blown way out of proportion.

Mr. CAULEY. Right.

Mr. MEADOWS. But yet, at the same time, your confidence level, if there were a cyberattack on an investor-owned utility, you know, somewhere in the Midwest, the damage they could cause, in your opinion, would be minimal.

Mr. CAULEY. The damage on the——

Mr. MEADOWS. Physical damage.

Mr. CAULEY [continuing]. Business and information systems, that would be their business risk. But on the grid it is very difficult. It is very unlikely to put a grid out for 1 to 2 weeks. I think——

Mr. MEADOWS. So what you are saying is mass outages for multiple weeks or days, are—in your opinion, is going to be a weather-related event.

Mr. CAULEY. Or the other thing is a physical attack, which is shooting explosive devices at the substation are the two things I think can get into that 1 to 2 weeks and beyond——

Mr. MEADOWS. But those are a lot easier to anticipate and plan for.

Mr. CAULEY. It is very complicated to do 20 sites at once with a physical attack with the current law enforcement we have. So I think that risk is mitigated as well. But it is the one I worry about the most, is a physical attack.

Mr. MEADOWS. Well, that is very helpful. I will follow up with all of you. And from an REA [Rural Electrification Administration] standpoint I just want to say thank you, as a member of my local REA. I have a great affinity for my REAs.

Ms. KILMER. Thank you very much.

Mr. MEADOWS. All right. I yield back.

Mr. BARLETTA. Thank you. I just have one more question, Mr. Spence. My colleague—Mr. Spence, my colleague from Pennsylvania highlighted that too many coal power plants have closed. Are you concerned that having fewer generation facilities online makes the grid, as a whole, more vulnerable?

Mr. SPENCE. I am not. In fact, Mr. Cauley and his team are also responsible, as part of their duties, to evaluate with very detailed modeling region by region, the impact of retirements of any sort on the grid of a major power station. So they have evaluated this multiple times, in fact, and have found that we continue to maintain an adequate reserve of capacity, should we see more retirements than actually forecast.

So, even with the forecasted retirements, which are many, particularly on the coal side, we still have adequate capacity to meet all of our projected needs for power.

Mr. BARLETTA. Thank you. I look forward to working with each and every one of you, and welcome your input as we move forward on this initiative.

I thank you all for your testimony. Your comments have been helpful to today's discussion.

If there are no further questions, I would ask unanimous consent that the record of today's hearing remain open until such time as our witnesses have provided answers to any questions that may be submitted to them in writing, and unanimous consent that the record remain open for 15 days for any additional comments and information submitted by Members or witnesses to be included in a record of today's hearing.

[No response.]

Mr. BARLETTA. Without objection, so ordered.

I would like to thank our witnesses again for their testimony. If there are no further questions to add, the subcommittee stands adjourned.

[Whereupon, at 1 p.m., the subcommittee was adjourned.]

STATEMENT OF
THE HONORABLE ANDRÉ CARSON
RANKING MEMBER, SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS AND EMERGENCY MANAGEMENT
HOUSE TRANSPORTATION AND INFRASTRUCTURE COMMITTEE

"BLACKOUT! ARE WE PREPARED TO MANAGE THE AFTERMATH OF A CYBER-ATTACK OR OTHER FAILURE OF THE ELECTRICAL GRID?"

April 14, 2016

Good morning. I want to thank Chairman Barletta for scheduling today's hearing and join him in welcoming today's witnesses.

The electrical grid is a critical part of the daily life of every American. Most of our critical infrastructure depends on electricity for operation, including mass transportation, energy generation, communications, and much more. Because of this dependency, our Nation must better prepare for power outages, whether they result from a natural disaster or an act of terrorism.

As hurricane season is fast approaching, this morning's hearing on our preparedness for an electrical grid failure is timely. In 2012, Hurricane Sandy caused intense damage and left some areas of New York and New Jersey without power for over 11 very long days. That storm tested our response plans as first responders from across the country, from all levels of government, and the private sector, were eventually able to restore power, but it still took days. We learned a great deal from that storm and I am very interested in hearing how emergency response plans have been improved, and what still needs to be done to better protect our infrastructure against natural disasters.

While Mother Nature has caused most of the power outages, realistically, a sophisticated cyberattack can potentially cause widespread damage to our Nation's grid. Ukraine recently experienced a coordinated cyberattack on its power system. I've heard competing opinions – from those who say it can never happen to us, to those who say we are completely unprepared. Given views by cyber experts and security agencies that our grid is not as secure as needed, I believe there is the possibility of a cyberattack on our power grid. But I also believe that with better oversight and preparation, we must take steps now to further mitigate and lessen the severity of impacts from future outages. We must take a cyberattack threat seriously and ensure that we are prepared for this possibility here.

While many of the response and recovery efforts will be the same for a power outage caused by a natural disaster or manmade attack, we must make sure that the roles and responsibilities of all parties are clearly defined. This may be complicated by the fact that most of the Nation's electrical grid infrastructure is privately owned and operated. Because of this, we should ensure continued and effective communication and coordination efforts between the federal, state and local governments, and the owners and operators of the electrical grid systems.

Being prepared means not only having contingency plans in place but also regularly exercising those plans with robust testing and comprehensive drills. I look forward to hearing about last year's GridEx III outcomes and subsequent training, plus identifying any gaps that need to be filled.

I look forward to your testimony, and again, thank you for participating in today's hearing.

FEMA

STATEMENT

OF

W. CRAIG FUGATE
ADMINISTRATOR
FEDERAL EMERGENCY MANAGEMENT AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

COMMITTEE ON TRANSPORTATION AND INFASTRUCTURE
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS AND EMERGENCY MANAGEMENT

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

"BLACKOUT! ARE WE PREPARED TO MANAGE THE AFTERMATH OF A CYBER-ATTACK OR OTHER FAILURE OF THE ELECTRICAL GRID?"

Submitted
By

Federal Emergency Management Agency
500 C Street, S.W.
Washington, D.C. 20472

April 14, 2016

Introduction
Chairman Barletta, Ranking Member Carson and Members of this Subcommittee, good afternoon. My name is Craig Fugate and I am the Administrator of the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA). Thank you for the opportunity to discuss how FEMA fulfills its responsibility to lead the Nation's response and recovery efforts for all hazards, to include the physical impacts of a massive power outage.

The most effective way for the federal government to plan for and respond to the potentially life-threatening physical consequences of a cyber incident on our nation's power grid is to be as prepared as possible to handle the consequences of any type of catastrophic event, regardless of the cause. Whether it's a cyber incident, a space weather event, or a Category 5 hurricane making landfall, FEMA, in partnership with its federal partners, has the plans and resources in place for a robust federal effort to support state, local, tribal, territorial governments, the private sector, and citizens to appropriately respond to any hazard.

Over the past several years, FEMA – in close coordination with our federal interagency partners, the public and private sectors, and other key stakeholders – has made important progress in addressing ways in which we respond to, recover from, and mitigate all hazards, including malicious cyber activity and the physical consequences of cyber incidents.

In my testimony today, I will highlight the overarching catastrophic planning frameworks that guide FEMA's response to large-scale complex incidents; current efforts underway to supplement all-hazards plans to specifically address cyber incident considerations; and ways in which FEMA and other critical stakeholders exercise our ability to respond to catastrophic events, including the physical impacts of cyber incidents.

Overview of Planning and Catastrophic Planning Efforts

Response Planning
FEMA's Planning and Exercise Division is responsible for a number of planning actions, including developing and coordinating joint state and federal catastrophic plans; leading the development and alignment of regional-to-national-level interagency catastrophic planning efforts; supporting regional planning initiatives to align all catastrophic planning; and the overall development and delivery of the updated Power Outage Incident Annex, which I will discuss later in this testimony.

Additionally, we coordinate closely with our federal partners on other preparation efforts, including the development of pre-scripted mission assignments, interagency agreements, and advanced contracts for commodities. These partnerships are essential to FEMA's ability to carry out its mission by leveraging the full capacity of the federal government to prepare for, protect against, respond to, recover from and mitigate catastrophic incidents, including cyber incidents.

Presidential Policy Directive 8: National Preparedness
Recognizing that this nation's preparedness is a shared responsibility across all sectors of our society, on March 30, 2011, the President signed *Presidential Policy Directive (PPD)-8: National Preparedness*. PPD-8 aims to strengthen the security and resilience of this nation through systematic preparation for the threats and hazards that pose the greatest risk to national security.

PPD-8 called for a National Preparedness Goal to guide and align the nation's preparedness efforts at all levels. The National Preparedness Goal is: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." The Goal is also the cornerstone for the implementation of PPD-8.

The President's issuance of PPD-8 significantly aided the alignment and integration of operational planning under a single National Preparedness System. The five mission frameworks – (Prevention, Protection, Mitigation, Response, and Recovery) – set forth the policy, roles and responsibilities of the community of partners across Federal, state, local, tribal and territorial governments, non-governmental organizations, and individual citizens.

National Response Framework

The National Response Framework (NRF) is an essential component of the National Preparedness System mandated in PPD-8. It is a guide to how the nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System (NIMS) to align key roles and responsibilities across the nation. The NRF describes specific authorities and best practices for managing incidents that range from the serious, but purely local, to large-scale terrorist attacks or catastrophic natural disasters. The NRF defines a catastrophic incident as "any natural or manmade incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, or government functions." Furthermore, the NRF describes structures for implementing a nationwide response policy and operational coordination for all types of domestic incidents—underscoring the importance of how risk informs response planning. The Framework is always in effect and applies to all catastrophic incidents, including the physical impacts of malicious cyber activity.

The NRF organizes the implementation of federal response capabilities and expertise into 14 Emergency Support Functions (ESFs) to provide the planning, support, resources, program implementation, and emergency services needed during a disaster. The ESFs, coordinated by FEMA, serve as the primary operational-level mechanisms in support of state, local, tribal, and territorial efforts. During a cyber incident that results in physical impacts, most of the ESFs would play some role. For example, ESF #6: Mass Care would coordinate the delivery of federal mass care, emergency assistance, housing, and human services, while ESF #12: Energy would facilitate the restoration of damaged energy systems and components for incidents requiring a coordinated Federal response. Federal departments and agencies provide substantial disaster response assistance in their areas of expertise, as well as operational support when mission assigned to support the disaster response.

Revision of the National Response Framework (NRF)

Originally published in 2008 to replace the National Response Plan, the NRF was revised in 2013, to focus on how the NRF fits into the National Preparedness System called for in PPD-8. The NRF was refreshed again in 2015 to better integrate with the other mission areas. For example, the Framework describes in greater detail how "non-Stafford incidents" can employ and utilize the NRF to help organize, guide, and streamline incident response. The NRF is intended to be a

strategic document, with tactical planning and concept of operations content reserved for the Federal Interagency Operational Plans.

Federal Interagency Operations Plans (FIOPs)
The FIOPs build upon the National Planning Frameworks (including the NRF highlighted above), which set the strategy and doctrine for how the community partners at all levels build, sustain, and deliver the core capabilities identified in the National Preparedness Goal. The Response FIOPs is structured to address the "maximum of maximum" planning factors for the nation or any given region while being flexible and adaptable for the full range of threats that face the nation. A single all-hazard FIOP serves to operationalize the roles and responsibilities for each mission framework (Prevention, Protection, Mitigation, Response, and Recovery). This all-hazards approach includes events that would result from a cyber incident, including effects on infrastructure and individuals. The single operational plan for each mission framework allows for increased coordination across responders, including coordinated use and maintenance.

Incident Specific Annexes
The Incident Annexes to the FIOP address specific contingency or hazard situations or an element of an incident requiring specialized application of the general response concept of operations. They describe coordinating structures, in addition to the ESFs, that may be used to deliver core capabilities and support response missions that are unique to a specific type of incident. Incident annexes also describe specialized response teams and resources, incident-specific roles and responsibilities, other scenario-specific considerations and an execution schedule to guide the employment and deployment of assets. Incident Annexes currently under development include:

- Oil and Chemical Incident;
- Nuclear/Radiological Incident;
- Biological Incident;
- Food and Agriculture Incident;
- Mass Evacuation Incident; and
- Power Outage Incident.

Power Outage Incident Annex
FEMA is developing a new Power Outage Incident Annex to the Response and Recovery FIOPs, which will address the response and recovery to a mass or long-term power outage regardless of cause, but including the impacts of a cyber incident.

This annex is nearing completion of an operational draft in partnership with the Department of Energy, recognizing their role as the ESF #12 lead agency and as the Energy Sector Specific Agency (SSA), and with the Sector Coordinating Councils (SCCs) for critical infrastructure. This annex will address a serious threat: a significant disruption to our nation's energy grid–whether caused by a natural disaster, cyber or manmade event. FEMA expects that this incident annex will also be a valuable tool for other threats that may impact our energy infrastructure, such as significant space weather. We anticipate this annex will be released later this year.

In the coming years FEMA will expand this national planning effort to include joint federal-state plans conducted at our FEMA Regions to increase fidelity into our plans and expand our partnership to local and regional power providers.

FEMA will maintain the final versions of the annex via FEMA's interagency consequence management system and intranet websites, and will notify Congress and other key stakeholders (including the public and private sectors) when they are completed.

While we plan at the federal level, we are also developing tools to support planning across the whole community. FEMA is currently leading the development of cybersecurity resource typing definitions and job title position qualifications in collaboration with DHS' National Protection and Programs Directorate (NPPD), specifically the National Cybersecurity and Communications Integration Center (NCCIC). This will establish a common language for defining the capabilities of resources used to respond to cyber incidents via the NIMS. Also, FEMA will partner with relevant cyber subject matter experts across the federal government to support eligible jurisdictions on improving cybersecurity planning and increasing their ability to maintain cyber-dependent essential functions following a catastrophic event.

National Level Exercise (NLE) 2012
Many of the efforts I have previously described build on the lessons learned from our exercise program. NLE 2012 directly examined the nation's ability to coordinate and implement prevention, preparedness, response, and recovery plans and capabilities pertaining to a series of significant cyber events. The scenario of this major exercise was based on a nation state which sought to disrupt Critical Infrastructure and Key Resources, logistics systems, and communications capabilities of U.S. federal agencies as a way to erode the public's trust in its security and safety, and cause impacts to the U.S. economy. This scenario emphasized the shared responsibility among all levels of government, the private sector, and the international community to secure cyber networks and coordinate response and recovery actions. The exercise tested our national response plans and procedures, including the NRF.

The exercise:

- Evaluated government (federal, state, local, tribal, territorial, and international) roles and responsibilities in coordinating national cyber response efforts and their nexus with physical response efforts, including allocation of resources;
- Examined the ability to share information across all levels of government and with the private sector as well as the general public, to create and maintain cyber incident situational awareness, and coordinate response and recovery efforts; and
- Assessed key decision points and decision making in a significant cyber event.

As described in FEMA's NLE 2012 Quick Look Report, this exercise demonstrated the critical importance of coordinating national and international response efforts as well as integrating the private sector into decision-making. We continue to use lessons learned out of this and other exercises as we update and validate our response plans.

Conclusion
Our nation will continue to face significant and increasing malicious cyber activity. FEMA, working alongside our federal interagency partners, the public and private sectors, and other critical stakeholders, continues to lean forward to be able to respond to and recover from these ever growing and sophisticated threats.

Responding to events like these is a shared responsibility nationwide, including the federal government, states, local communities, businesses and individual families themselves. That is why we have partnered with communities across the nation to provide vital resources to make sure Americans know how to prepare for the potential physical consequences of a cyber incident like a major power failure—building understanding of what steps to take before, during, and after such an event.

As outlined in my testimony today, we remain steadfast and earnestly committed in our efforts to continue building robust planning capabilities and partnerships that strengthen our resilience to these types of incidents.

Chairman Barletta, and members of this subcommittee, thank you again for the opportunity to appear before you today to discuss FEMA's efforts in managing the physical consequences resulting from cyber incidents.

I look forward to your questions.

Testimony of Patricia A. Hoffman

Assistant Secretary for Office of Electricity Delivery and Energy Reliability

U.S. Department of Energy

Before the

Committee on Transportation and Infrastructure

Subcommittee on Economic Development, Public Buildings, and Emergency Management

U.S. House of Representatives

April 14, 2016

Chairman Barletta, Ranking Member Carson, and Members of the Subcommittee, thank you for focusing attention on the importance of a resilient electrical grid, and for the opportunity to discuss the Department of Energy's role in helping to ensure a resilient, reliable, and flexible electricity system in an increasingly challenging environment.

Our economy, national security and even the health and safety of citizens depend on the reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) is to strengthen, transform, and improve energy infrastructure to ensure access to reliable, secure, and clean sources of energy. We are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure, including the electric power grid, from disruptions caused by natural and manmade events, such as severe weather, physical attacks, and cyber-attacks.

The electrical grid is more than just infrastructure. It is an ecosystem of asset owners, manufacturers, service providers, and government officials at Federal, state, and local levels, all working together to run one of the most reliable power grids in the world. Ninety percent of the nation's energy infrastructure is in private hands, and 3,306 electricity providers serve approximately 148 million people[1] through a network of 450,000 miles of high-voltage transmission lines.

There are plenty of risks beyond cyber, including physical, severe weather, natural disasters, aging infrastructure, and infrastructure interdependencies. My testimony today will focus on how, in the face of these diverse threats, we can help ensure that the grid is poised to recover quickly following an incident and how partnerships with public and private stakeholders play a critical and necessary role in this work.

THE ECOSYSTEM OF RESILIENCE

A crucial factor to meeting these challenges is to be proactive and cultivate what I call an "ecosystem of resilience": A network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover. We continue to partner with industry, other Federal agencies, local governments, and other stakeholders to

[1] Energy Information Administration Forms EIA-861 and 861S, 2013. Does not include U.S. territories.

quickly identify threats, develop in-depth strategies to mitigate those threats, and rapidly respond to any disruptions.

Our resilience efforts are further bolstered by our broader grid modernization activities, for instance our support of the research, development and deployment of advanced technologies, and our work with state, local, tribal, and territorial stakeholders to help them improve their local resilience and energy emergency response capabilities. Of the $4.5 billion that we invested in grid modernization through the American Recovery and Reinvestment Act (ARRA), $3.4 billion was used to help industry accelerate the deployment of advanced technologies that are now reducing costs and keeping the lights on more reliably and efficiently. This smarter grid is helping to prevent outages, reduce storm impacts, and restore service faster when outages occur.

Our model is partnerships first. We are all in this together. It is through working together that we continue to strengthen our ability to bounce back following an event.

PARTNERSHIPS FOR READINESS

DOE-OE has been working with utility owners and operators, regulators, and state and local officials across the country concerning threats to cyber-security and other risks. Through these partnerships, we are providing tools, best practices, new technologies, and matching funds to support their many ongoing efforts.

We directly support preparedness efforts at the community level, in part through products and tools produced by our Infrastructure Security and Energy Restoration (ISER) division, which inform and educate state and local officials in their energy emergency preparedness activities. This is done through forums, training, and tabletop exercises for federal, state, and local energy officials.

In early February, DOE Secretary Ernest Moniz signed an updated Energy Emergency Assurance Coordinators (EEAC) Agreement with the National Association of State Energy Officials (NASEO), National Association of Regulatory Utility Commissioners (NARUC), National Governors Association (NGA), and National Emergency Management Association (NEMA). This updated EEAC Agreement lays out concrete items to improve our collective ability to share information, which is essential for making sound response and restoration decisions during emergencies. To support this effort, DOE and state officials will develop information-sharing protocols and processes to streamline response operations. We will also test these processes and information-sharing mechanisms through routine drills and exercises.

The President's FY 2017 Budget includes a request for $15 million for a State Energy Assurance program to foster regional hazard preparedness. This program would focus on providing state, local, tribal, and territorial governments with analysis, training, and exercising of shared regional risk factors where entities depend on each other for energy supplies and must work together to resolve energy disruptions to restore energy infrastructure.

This new program would be facilitated through competitive regional cooperative assistance awards to state and local partners. As needed, DOE, including our National Laboratory expertise and capability, would be available to the awardees to enhance preparation and allow for real-world energy emergency support. Lessons learned will be shared with other communities to leverage the program across the nation and help improve resiliency planning.

DOE-OE also focuses on enabling our state, local, and utility partners with information. EAGLE-I (Environment for Analysis of Geo-Located Energy Information), for example, is a DOE-designed and operated web tool that automatically gathers electrical grid service status data from company websites every 15 minutes, and organizes it into an easy to read picture of electrical service status nationwide. Now covering 75 percent of all U.S. electricity customers, it provides real-time information about the grid – what is up, what is down, the number and location of outages, when service is restored – to DOE and, through our information-sharing efforts, with other Federal agencies.

Cyber-security and Resilience

Intentional, malicious challenges to our energy systems are on the rise. We are seeing threats continually increase in numbers and sophistication. This evolution has profound impacts on this sector, which is why we've made cyber-security one of our highest priorities at DOE.

As there has been an increase in malicious cyber activity, we work closely with the energy sector to share cyber threat information. Since 2010, DOE-OE has invested more than $180 million in cyber-security research, development and demonstration projects that are led by industry, universities and National Labs. Since then, more than 20 new technologies that our investments helped support are now being used to further advance the resilience of the Nation's energy delivery systems. For example, SecureSmart is a capability to identify bad actors on networks and Hyperion is a capability to evaluate and expose malicious content and third-party software.

All of OE's cyber-security research initiatives are based upon industry involvement, joint funding through matching funds, and development with an end goal of practical use.

The Cyber-security Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE-OE and industry. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the National Intelligence Community to better inform the energy sector of the high-level cyber risks. Current CRISP participants provide power to over 50 percent of the total number of continental U.S. Electricity Subsector customers.

Cyber-security preparedness was part of the Smart Grid Investment Grants (SGIG) awarded by OE through ARRA. Each of the 99 projects that received this funding was required to develop a cyber-security plan. Participants included investor owned utilities, public power utilities, and cooperatives. This process truly raised the bar of awareness of cyber-security risks and jumpstarted progress in cyber-security protection actions and best practices.

As part of the Administration's efforts to improve electricity subsector cyber-security capabilities, DOE-OE and industry partners developed the Electricity Subsector Cyber-security Capability Maturity Model (C2M2) to improve cyber-security capabilities and to help private sector owners and operators better assess cyber-security posture of the energy sector. The C2M2 provides an evaluation tool that helps organizations evaluate, prioritize and improve cyber-security capabilities.

Since the C2M2 program's inception in June 2012, more than 750 organizations have requested and received the C2M2 toolkit, including more than 400 electricity subsector organizations, and the number of participants is growing steadily. This is a comprehensive and credible approach that all energy sector companies can use to improve their cyber-security posture. DOE-OE also released versions of the C2M2 for the oil and natural gas sector and for industry at large.

Preparedness Exercises

DOE leads preparedness exercises at the local, state, and national levels. In November 2015, for example, DOE led the Federal participation in the North American Electric Reliability Corporation's Grid Ex III, the largest electricity sector crisis response exercise ever. More than 350 government and industry organizations, as well as 4,500 participants played a role in testing and shaping the national response plan.

In April, DOE will lead Clear Path IV in Portland, Oregon and Washington, DC. Clear Path IV is an interagency exercise focused on testing and evaluating energy sector roles and responsibilities within response plans utilized for a Cascadia Subduction Zone (CSZ) 9.0 earthquake and tsunami. Clear Path IV includes representation from 10 Federal agencies, seven states, five local governments, 15 oil and natural gas companies, 18 electric utilities, six trade associations, and four state associations with more than 175 participants.

Through this broad range of activities with our private and public partners, we are continuing to make good progress in creating a comprehensive ecosystem of resilience.

PARTNERSHIPS FOR RESPONSE

Our partnerships with private and public stakeholders also focus on quickly identifying threats, developing in-depth strategies to mitigate them and rapidly responding to any disruptions. With 90 percent of the Nation's power infrastructure privately held, coordinating and aligning efforts between the government and the private sector is the only viable path to success.

Under Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, DOE is the Sector-Specific Agency (SSA) for electrical infrastructure. The SSA plays the pivotal role of ensuring unity of effort and message across government partners, including the White House, the Department of Homeland Security, the Department of Defense and other Offices within DOE.

As the Energy SSA we also serve as the day-to-day Federal interface for the prioritization and coordination of activities to strengthen the security and resilience of critical infrastructure in the energy sector. This involves building, maintaining and advancing our relationships and collaborative efforts with the energy sector. We have invested in public/private partnership programs and initiatives that involve sharing real time information, assessing vulnerabilities, clarifying responsibilities, and engaging in training and exercises.

In addition, the Department of Energy serves as the lead agency for Emergency Support Function 12 (ESF-12) under the National Response Framework. As the lead for ESF-12, the DOE is responsible for facilitating the restoration of damaged energy infrastructure. During a response operation, the Department works with industry and federal/state/local partners to:

- Assess the impacts of a disaster on the local and regional energy infrastructure;
- Coordinate the delivery of assets to repair that damaged infrastructure;

- Monitor and report on restoration efforts; and
- Provide regular situational awareness updates to key decision makers in the Administration and our interagency partners.

To achieve these operational priorities, the Department deploys responders who work directly with the affected utilities and local officials on the ground during a disaster. They provide expertise on a variety of energy issues, and have direct access to subject matter experts back at our headquarters in Washington, DC. These experts work with our interagency partners to coordinate the appropriate waivers, when needed, to further speed restoration efforts. In extreme cases, the Department can use its legal authorities under the Federal Power Act, the Defense Production Act, and the recently-passed FAST Act (Fixing America's Surface Transportation Act, P.L. 114-94) to assist in response and recovery operations.

The national electricity infrastructure spans 19,000 power plants, 450,000 miles of transmission lines, 55,000 substations, and 6 million miles of distribution lines. The grid is truly a national system of complex systems, where small variations in power output or quality can be felt almost instantly several states away. That said, every piece of that infrastructure is local.

A fallen tree or dedicated hacker from overseas can threaten the broader transmission system and the distribution system. When the power goes out, the local utility is the first responder. Should any threat or emergency exceed local public or private resources, or require a full-blown national response, a utility CEO, or a representative trade association member of the Electricity Subsector Coordinating Council (ESCC) member, the Electricity – Information Sharing and Analysis Center (E-ISAC), or the Federal Government can request what is called a Crisis State Activity. Crisis State Activities are coordinated through the ESCC because, as with preparedness, we respond through partnerships. The ESCC is a group of leaders from across the electricity subsector that meet regularly with government to coordinate and share information. Together, we work toward collective actions to address the threat or risk. The ESCC is the strategic communication and coordination mechanism of industry and government for collective actions toward national critical infrastructure security and resilience.

Congress enacted several important new energy security measures in the FAST Act. The Secretary of Energy was provided a new authority, upon declaration of a "Grid Security Emergency" by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks on the grid. DOE is working to issue rules of procedure regarding this new authority and will continue its partnership with the energy sector to ensure the maximum effectiveness of this authority.

The FAST Act also codifies DOE's role as the lead SSA for energy sector cyber incident coordination. These actions provide a central point of action for the energy sector and can expedite recovery from cyber and physical incidents.

The FAST Act protections afforded to critical electric infrastructure information provide essential information-sharing tools to enhance the Federal Government's situational awareness while assuring the private sector that sensitive information on vulnerabilities will be safeguarded.

DOE looks forward to consulting in depth with FERC on the forthcoming critical electric infrastructure information rulemaking.

The FAST Act will enable a more robust response for energy incidents, and DOE is on track to implement the energy security provisions.

PARTNERSHIPS FOR INNOVATION

The myth that older infrastructure is more resilient because it is safe from cyber-attack is just that – a myth. In some cases the aging infrastructure of the grid itself can be a liability or risk. This infrastructure is less sophisticated, less stable, less tolerant to heat and cold, and less able to absorb voltage and frequency variations.

The keys to strengthening resilience are not only better threat insight and response, but also innovation and preparedness. In January 2016, the DOE built upon its Grid Modernization Initiative – an ongoing effort that reflects the Obama Administration's commitment to improving the resiliency, reliability, and security of the Nation's electricity delivery system – by releasing a comprehensive new Grid Modernization Multi-Year Program Plan (MYPP). The MYPP, developed in close collaboration with a wide range of key external partners, lays out a blueprint for DOE's research, development, and demonstration agenda to enable a modernized grid, building on concepts and recommendations from the recent Quadrennial Energy Review (QER 1.0) and Quadrennial Technology Review (QTR).

One technology ripe for innovation is large power transformers. These important grid assets can weigh hundreds of tons, are expensive, and are typically custom made with procurement lead times of 1 year or more. Significant numbers of damaged transformers from any type of hazard, can result in a long-term impact on the overall resilience of the grid. The first installment of the QER 1.0 recognized the risks associated with the loss of large power transformers. The QER recommended that DOE work with other Federal agencies, states, and industry on an initiative to mitigate these risks. Approaches envisioned in the QER include the development of one or more strategic transformer reserves through a staged process, beginning with an assessment of technical specifications and whether new Federal regulatory authorities or cost-share are necessary and appropriate.

The Transformer Resilience and Advanced Components (TRAC) program also includes a number of R&D activities to improve the resilience of transformers. Replacing aging grid assets with long-lived outdated technology will lead to infrastructure lock-in that increases the total cost of grid modernization. The average lead time between a large power transformer order and the date of delivery ranges from five to 12 months for domestic producers and six to 16 months for producers outside the United States. However, this lead time could extend beyond 20 months and up to five years in extreme cases if the manufacturer has difficulties obtaining any key inputs, such as bushings and other key raw materials. The President's FY 2017 budget request included $15 million for TRAC to develop cost-effective, next generation components that are inherently more resilient.

The FAST Act also addressed this issue and required DOE to submit a plan to Congress evaluating the feasibility of establishing a Strategic Transformer Reserve for the storage, in strategically-located facilities, of spare large power transformers in sufficient numbers to

temporarily replace critically damaged large power transformers. In January, DOE-OE awarded this analysis project to a team led by the Oak Ridge National Laboratory. The project team includes researchers from the University of Tennessee-Knoxville, Sandia National Laboratory, the Electric Power Research Institute, and Dominion Virginia Power.

Secretary Moniz also announced last January an award of up to $220 million over three years, subject to congressional appropriations, to DOE's National Laboratories and partners to support critical research and development in advanced storage systems, clean energy integration, standards and test procedures, and a number of other key grid modernization areas. This Grid Modernization Laboratory Consortium effort recognizes regional differences and will strengthen regional strategies while defining a diverse and balanced national strategy. In addition to projects that address the needs of incorporating individual grid technologies like solar or energy storage, DOE is also developing crosscutting projects that have impact across multiple technologies. As Secretary Moniz said at the announcement, "Modernizing the U.S. electrical grid is essential to reducing carbon emissions, creating safeguards against attacks on our infrastructure, and keeping the lights on."

Energy storage is another key technology for whole-grid resilience. Energy storage fundamentally changes the relationship between when energy is produced and when it is consumed. The President's FY 2017 budget request would support OE's work on materials research, device development, demonstrations, and grid analysis to help transition selected energy storage technologies from R&D to industrially relevant scales with improved safety, industry acceptance, and reduced cost. Improved energy storage technologies will enable the stability, resiliency and reliability of the future electric utility grid, as well as increase the deployment of variable renewable energy resources. All of these advances will strengthen resilience.

We have been proactive in advancing technologies to modernize and make our grids "smarter" and therefore more adaptive to the challenges that various threats pose to the grid. For example, DOE-OE has made key investments in the area of synchrophasor technology, which reduces grid vulnerabilities by providing timely and accurate power outage information and better self-healing capabilities, and has also invested in microgrids, which keep local communities up and running during regional and other outages and help supply power to effected areas.

Many of these projects are working in local jurisdictions throughout the United States. Supporting the research, development, and deployment of next-generation technologies enhances the grid's ability to recover quickly from disruptions.

CONCLUDING STATEMENT

Threats will continue to evolve, and DOE is working diligently to stay ahead of the curve. The solution is an "ecosystem of resilience" that works in partnership with local, state and industry stakeholders to help provide the methods, strategies, and tools needed to help protect local communities through increased resilience and flexibility. To accomplish this, we must accelerate information sharing to inform better local investment decisions, encourage innovation and the use of best practices to help raise the sector's cyber-security maturity, and strengthen local incident response and recovery capabilities, especially through participation in training programs and disaster and threat exercises.

Building an ecosystem of resilience is – by definition – a shared endeavor, of which keeping a focus on local communities remains a top imperative. Because DOE has spent decades building—and continue to build— local partnerships and investing in technologies to enhance resilience, the grid is better able to withstand and recover quickly from a disaster or attack.

TESTIMONY

OF

CAITLIN DURKOVICH
ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS AND EMERGENCY MANAGEMENT

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

"BLACKOUT! ARE WE PREPARED TO MANAGE THE AFTERMATH OF A CYBER-ATTACK OR OTHER FAILURE OF THE ELECTRICAL GRID?"

April 14, 2016

Introduction

Chairman Barletta, Ranking Member Carson and Members of this Subcommittee, good afternoon. My name is Caitlin Durkovich and I am the Assistant Secretary for Infrastructure Protection within the National Protection and Programs Directorate (NPPD). Thank you for the opportunity to discuss how the NPPD fulfills its responsibility to support the Federal government's response to and recovery from all-hazards events, including the physical impacts of cyber incidents.

NPPD carries out the Department's cyber and infrastructure protection mission by leading the national effort to secure and enhance the resilience of the Nation's infrastructure. To carry out this mission, the Office of Infrastructure Protection leads and coordinates national programs and policies, and established strong partnerships across government and the private sector. We conduct and facilitate vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners understand and address risks. We provide information on emerging threats and hazards so that appropriate actions can be taken. We offer tools and training to our partners to help them manage the risks to their assets, systems, and networks.[1]

The partnerships and coordination structures we maintain and support during steady state conditions—before incidents occur—set the stage for the way we execute our responsibilities following an incident. To that end, my testimony today will provide you with an overview of the work that NPPD conducts to promote and maintain sector coordination structures, characterize national level risks to infrastructure (in particular the electric grid), and support response efforts in the event of an incident.

A robust, secure, and resilient energy infrastructure is essential to serving the needs of today's society, protecting public health and safety, economic security, and national security. U.S. infrastructure by its very nature supports communities with constantly evolving requirements. The electricity sub-sector in particular is currently facing a variety of threats and hazards, including malicious cyber activity, physical attacks, aging infrastructure, equipment failure, and extreme weather-related events.

A targeted cyber incident—either alone or combined with a physical attack—on the power system could lead to huge costs and cascading effects, with sustained outages over large portions of the electric grid and prolonged disruptions in communications, water and wastewater treatment services, health care delivery, financial services, and transportation. For example, the results of a 2015 Lloyds of London study suggested that a widespread cyber-attack on the Northeastern region of the United States, i.e., damaging 50 generators (approximately seven

[1] NPPD carries out its private sector engagement under and through authority delegated to the Directorate by the DHS Secretary, which includes but is not limited to: 6 U.S.C. §§ 121(d)(5), 121(d)(6), 121(d)(8), and 121(d)(10).

percent) could trigger a scenario where 93 million people are without power and the impact on the U.S. economy could range from $243 billion to $544 billion, or around a trillion dollars in the most extreme scenario (where 14 percent of the generators are damaged).[2]

Coordination Structures and Voluntary Partnerships

Since DHS was formed in 2003, we have been working with private sector partners to help them build the Nation's resilience to all types of threats. Under the National Infrastructure Protection Plan (NIPP), DHS is the lead, or co-lead, for ten of the 16 infrastructure sectors. In addition, the Office of Infrastructure Protection (IP) provides cross sector collaboration and coordination functions across all the 16 sectors by sharing information, conducting assessments of critical assets, and engaging in joint planning and exercises in order to support a national understanding of physical and cyber risks. This includes working in close partnership with the Department of Energy regarding the security of the electric grid.

Most of the Department's work with owners and operators is voluntary and the successful execution of the critical infrastructure mission relies on strong voluntary collaboration with the private sector. One key approach is to ensure that information about threats is communicated quickly to owners and operators. Through our work, DHS participates in joint Federal Government/Private Sector information sharing designed to ensure that our partners understand how disruptions and attacks on infrastructure can impact homeland security, community resilience, and our economy, and take informed action to mitigate those risks.

Industry Partnerships

Sector Councils

The partnership approach is driven by work conducted with the critical infrastructure councils, including the Electricity Subsector Coordinating Council (ESCC). The ESCC includes Chief Executive Officers (CEOs) representing each segment of the electric power industry, as well as heads of the major industry trade associations related to the Subsector. A major priority of the partnership is unifying industry and government efforts to plan and prepare coordinated responses to incidents of national significance—whether physical or cyber. The ESCC and government meetings, which take place three times a year, provide a venue to discuss national-level responses to major incidents, physical security and cybersecurity, grid resilience, and progress made on joint industry/government initiatives. These meetings are made possible by the Critical Infrastructure Partnership Advisory Council (CIPAC), an authority which allows government to engage in discussions about joint critical infrastructure planning, coordination, implementation, and operational issues, along with other relevant matters.

[2] Lloyd's and the University of Cambridge Centre for Risk Studies, *Business Blackout: The insurance implications of a cyber attack on the US power grid*, Emerging Risk Report 2015, innovation series (London, UK: 2015). The report also noted that while the scenario was improbable, it is technologically possible.

DHS and the Department of Energy (DOE), which serves as the Energy Sector-Specific Agency (SSA), collaborate with other interagency partners to provide classified threat briefings to CEOs on physical and cyber threats.

Meetings with the ESCC enable industry and government to share perspectives, identify joint priorities, and track progress. Projects conducted through this partnership include:

- The Electricity Substation Security Awareness Campaign: A 2013-2014 campaign conducted in close collaboration and coordination with DOE, the Department of Justice's Federal Bureau of Investigation (FBI), the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and multiple industry partners. Taking place in ten U.S. and three Canadian cities, it increased awareness of the evolving risk environment and promoted increased collaboration on risk mitigation strategies, protective measures, and industry best practices.
- The ESCC Playbook: The Playbook is a crisis management framework to enable senior executives from industry and government to coordinate effectively on response and recovery matters. Following GridEx II, the ESCC developed the Playbook for responding to a National-level incident that disrupts the electric grid. The framework ensures senior government and industry executives are communicating and are available to support response and recovery efforts. By opening and formalizing these lines of communication, the industry and government can better coordinate efforts to protect the electric grid and recover from incidents as quickly as possible. The Playbook was tested through tabletop exercises with the ESCC and their staff. It was tested again as part of GridEx III.
- Cross-sector coordination: DHS and DOE work with the ESCC on efforts to institutionalize coordination with other sectors (e.g. telecommunications and transportation dependencies and interdependencies).

Assessing Infrastructure Security and Managing Infrastructure Risk

Risks, in particular grid related risks, do not conform to traditional boundaries of domain, sector, or geography. This makes the work that IP does in assessing interdependencies and larger scale vulnerabilities and consequences all the more important for gaining a full picture of risk, and informing risk decisions before, during, and after an incident.

Analyzing Interdependencies and Cascading Effects

Through our Protective Security Advisors (PSAs) located across the country, we offer critical infrastructure partners hands on assistance with vulnerability and security assessments like the Regional Resiliency Assessment Program (RRAP). The RRAP is an IP-led assessment of specific critical infrastructure and regional analysis of the surrounding infrastructure to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective. The assessment identifies dependencies, interdependencies, cascading effects, resiliency

characteristics, and gaps. Energy is one of the primary focuses of a number of RRAP projects, and the dependence of other infrastructure sectors on energy, especially electric power, is regularly examined during the course of other projects. Since 2014, several RRAP projects included an assessment of security, resilience, and criticality of Business Systems, Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) systems that provide a key service or function within a broader community or system of critical infrastructure.

Conducting the RRAP projects in the Energy Sector helps mitigate high-risk single points of failure and the lack of redundancy across systems, improve emergency response capabilities, and identify critical supply chain vulnerabilities. One example of a successful RRAP is a 2016 Region I Energy project that focuses on electric power substations with large power transformers and their resilience to extreme weather events. Based on recommendations and findings from the Quadrennial Energy Review conducted by DOE, the RRAP project will identify large power transformers in substations across Region I, assess their vulnerabilities, and provide data to decision makers who might better focus resources to protect the most vulnerable assets.

In addition to the RRAP Program, IP conducts site assistance visits and voluntary inspections using the Infrastructure Support Tool (IST). The IST makes use of a threat agnostic, model based risk analysis methodology, allowing owners and operators of critical infrastructure to apply the results of an IST inspection to a multitude of threat and hazard scenarios, informing their decisions about buying down risk.

National Response and Infrastructure Systems

The response to a major disaster or attack resulting in a failure of the electrical grid would require a nationwide effort, drawing on the catastrophic planning frameworks that make up the National Preparedness System. Such a response effort also requires the support of steady-state coordination structures established under the NIPP. NPPD supports FEMA and our interagency and whole community partners in strengthening the connection between the National Preparedness System and the partnership structures established under the National Infrastructure Protection Plan.

The coordination structures maintained under the NIPP provide a mechanism for cross-sector, coordinated information support for both situational awareness and planning efforts during response. Information requests and the development of incident-specific analysis contribute to the assessment, prioritization, restoration, and protection of infrastructure systems.

As the infrastructure coordination element of the National Operations Center (NOC), the National Infrastructure Coordinating Center (NICC) receives situational, operational, and incident-related information regarding the status of the Nation's critical infrastructure sectors during incidents and collects input from every SSA that is consolidated into comprehensive reporting.

Sharing Information Quickly and Efficiently

Information sharing is a key part of NPPD's mission to create shared situational awareness of infrastructure impacts and vulnerabilities. NPPD, through its National Cybersecurity and Communications Integration Center (NCCIC), actively collaborates with public and private sector partners every day to make sure they have the information and tools they need to protect the systems we all rely on and continues to monitor the situation closely.

During a cyber or communications incident, the NCCIC is able to coordinate with State, local, and private sector partners as well as its own incident response entities and Federal partners, including law enforcement and the intelligence community so that the full capabilities of the Federal Government can be brought to bear in a coordinated manner. As the Federal Government's 24/7 hub for cybersecurity information sharing, incident response, and coordination, the NCCIC is critical in our efforts to ensure our nation's cybersecurity.

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is a response component of the NCCIC, which responds to cyber incidents, vulnerabilities, and threats that can impact industrial control systems which operate critical infrastructure across the United States. In responding to cyber incidents, the ICS-CERT coordinates with law enforcement agencies; the intelligence community; Federal and SLTT governments; and control systems owners, operators, and vendors to reduce risk to the nation's critical infrastructure. The ICS-CERT team can provide onsite support to private sector industrial control system owners and operators, including analytic support (malware, hard drive, and log file analysis) and detailed remediation recommendations.

Over the last few years, the ICS-CERT and the FBI have responded to sophisticated cyber exploitation campaigns against U.S. critical infrastructure industrial control systems (ICS). These campaigns involved two different sets of malware; both of which use tactics to target and gain access to the control systems environments. The characteristics of this activity include the use of ICS zero-day vulnerabilities, malicious ICS payloads, and specific targeting of the operations environment across a variety of sectors including energy, water, critical manufacturing, communications, and more.

ICS-CERT continuously responds to this activity, conducting incident response and analysis, issuing alerts and warnings, and conducting briefings and outreach to highlight these campaigns. ICS-CERT is highly concerned as the sophistication of the threat actors and exploitation techniques used represent an elevated level of risk for critical infrastructure asset owners and operators.

By virtue of the fact that the majority of the nation's critical infrastructure is owned and operated by the private sector, DHS builds and maintains strong partnerships with owners and operators,

recognizing that disruptions and attacks on infrastructure impact homeland security, community resilience, and our economy. This collaboration extends back for many years, with the recent focus on raising awareness of Black Energy and other types of ICS malware. This ICS campaign also included efforts to mitigate the threat and ensure the nation's electric grid protection.

Recent cyberattacks against the power grid in the Ukraine also underscore the importance of maintaining partnerships for risk management in advance of incidents, and applying the full spectrum of capabilities and tools for managing such complex risks.

Conclusion

The electric grid transcends political and geographic boundaries and its operations shift based on demand or availability of natural resources. Innovation has the potential to strengthen some aspects of the grid while at the same time creating new vulnerabilities. Making the grid secure and resilient requires focus on both the grid of today as well as the electric grid of the future. With these realities in mind, the United States and Canada have agreed to develop a joint strategy for strengthening the security and resilience of the North American electricity grid. This strategy will outline a collaborative effort to secure the grid and make it resilient against all hazards, including cyber threats.

The energy industry takes a holistic approach to assessing and mitigating risks from cyber attacks, physical sabotage, and natural disasters, all of which can all result in disruptions to the electric grid. As our nation continues to face increasing and evolving cyber threats and other risks to the U.S. electric grid, the Department must likewise use an integrated approach in preparing for these threats.

In a major step toward this unified approach, the Department proposed to transition NPPD to an operational component, the Cyber and Infrastructure Protection Agency. This transition would elevate cyber operations and provide more comprehensive, coordinated risk management support to our stakeholders that reflect the growing convergence of cyber and physical threats. As one of the current priorities of the Secretary, the Department submitted a plan to the authorizers and appropriators calling for Congressional support and action. The transition, if implemented, would improve the services provided to NPPD's stakeholders. Not only will the transition provide a more comprehensive approach to national level stakeholder engagement and relationship management, but stakeholders in the field will also have access to a unified catalog of services and tools that spans across all of NPPD. For example, the plan proposes to establish regional offices to better integrate field staff like Protective Security Advisors and Cyber Advisors, and support coordinated engagement with electric and other industry partners on cyber and physical vulnerability assessments, information sharing, incident response and other efforts.

We need to position ourselves to successfully address the realities of today's cyber environment and its impacts on critical infrastructure. The proposed structural changes at the headquarters and regional levels will enable NPPD to be more efficient and effectively deliver the important tools

and resources to electric industry partners and other critical infrastructure stakeholders that need them the most. As outlined in my testimony today, the partnership and coordination structures that NPPD facilitates are crucial for supporting both steady-state risk management and incident response. NPPD is committed to ensuring that our partners understand how disruptions and attacks on infrastructure can impact homeland security, community resilience, and our economy, and have the tools to drive informed action to mitigate those risks.

Chairman Barletta, and members of this subcommittee, thank you again for the opportunity to appear before you today to discuss NPPD's efforts in managing the physical consequences of cyber threats.

I look forward to your questions.

Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM April 11, 2016

To: Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management
Attention: Pamela Williams

From: Richard Campbell, Specialist in Energy Policy, x 7-7905

Subject: **Testimony - Blackout! Are we Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?**

Good Morning Chairman, Ranking Member, and Members of the Subcommittee. My name is Richard Campbell. I am a Specialist in Energy Policy for the Congressional Research Service (CRS). On behalf of CRS, I would like to thank the Committee for inviting me to testify here today.

My testimony will provide background on the possible consequences of a failure of the electric grid, the roles and responsibilities of the respective parties, and some of the objective challenges in the recovery efforts. I should note that CRS does not advocate policy, or take a position on specific legislation.

Potential Failure of the Electric Grid

The electric power grid in the United States comprises all of the power plants generating electricity, together with the transmission and distribution lines and systems which bring power to end-use customers. The grid also connects the many publicly and privately owned electric utility and other wholesale power companies in different states and regions of the United States.[1] However, with changes in federal law,[2] regulatory changes, and modernization of the electric power infrastructure as drivers, the grid is changing from a largely patchwork system built to serve the needs of individual electric utility companies to essentially a national interconnected system, accommodating massive transfers of electrical energy among regions of the United States.

Electricity generation is vital to the commerce and daily functioning of United States. While the U.S. electric grid has operated historically with a high level of reliability, the various parts of the electric power system are all vulnerable to failure due to natural, operational, or manmade events.

[1] As of 2013, there were 189 investor-owned electric utilities, 2,013 publicly-owned electric utilities, 887 consumer-owned rural electric cooperatives, and nine federal electric utilities. American Public Power Association, *U.S. Electric Utility Industry Statistics*, 2015, http://www.publicpower.org/files/PDFs/USElectricUtilityIndustryStatistics.pdf.

[2] Key legislation includes the Public Utility Regulatory Policies Act of 1978 (P.L. 95-617, as amended), the Energy Policy Act of 1992 (P.L. 102-486), the Energy Policy Act of 2005 (P.L.109-58), and the Energy Independence and Security Act of 2007 (P.L. 110–140).

Electric power is generated and sent over transmission lines to substations which reduce the voltage levels for distribution to end-use customers. The cables carrying electric power to customers generally exist in an exterior or "above ground" environment largely exposed to the elements. As such, power outages can result from floods or seasonal storms which often combine the furies of wind, rain, snow, or ice. The more severe weather events can damage electric power transmission and distribution infrastructure as trees or overhanging branches fall on electricity lines. Most failures of the grid occur in local distribution systems rather than bulk power transmission systems, as the rights-of-way for transmission lines are wider, and are cleared to prevent damage from trees. The cost of weather-related power outages may range from $25 billion to $55 billion annually.[3]

Other impairment or failure of the grid can potentially result from attacks, terrorism, or even extremes of space weather. For example, a nuclear weapon exploded at a high altitude over the United States would cause an electromagnetic pulse which could destroy power transformers and other critical components.[4] Similarly, a severe solar storm could have damaging impacts on power transformers. Sunspots send plasma from coronal mass ejections into space, which could interact with the Earth's magnetic field causing ground induced currents powerful enough to overload transformers. The last major solar flare eruption in 1989 caused blackouts in the Canadian province of Quebec. Even greater solar storms occur in cycles of approximately 100 years, with major events being recorded in 1859 and 1921.[5]

Much of the infrastructure which serves the U.S. power grid is aging. As of 2009, the average age of power plants was over 30 years, with most of these facilities having a life expectancy of 40 years.[6] Electric transmission and distribution system components are similarly aging, with power transformers averaging over 40 years of age,[7] and 70% of transmission lines being 25 years old or older,[8] as of 2007.

As the grid is modernized, new intelligent technologies utilizing two-way communications and other digital capabilities, are being incorporated with Internet connectivity. The "Smart Grid" refers to this evolving electric power network.[9] While these advances may improve the efficiency and performance of the grid, they also increase its vulnerability to cyberattacks launched from the Internet. The potential for a major disruption or widespread damage to the nation's power system from a large-scale cyberattack has increased focus on the cybersecurity of the grid. Modernization of many industrial control systems (ICS), in particular, Supervisory Control and Data Acquisition (SCADA) systems used by electric utilities, have also resulted in connections to the Internet.[10] The increasing frequency of cyber intrusions on ICS is a concern to the electric power sector. Power production and flows on the grid are controlled remotely by a number of IC technologies. The National Security Agency reported that it has seen intrusions into IC

---

[3] "Power outages can impact electricity consumers primarily through property loss and business disruption. This can result in lost orders, and damage to perishable goods and inventories for businesses. Power outages can critically affect manufacturing operations mainly through downtime as workers are idled, and potentially damage equipment and production processes." CRS Report R42696, *Weather-Related Power Outages and Electric System Resiliency*, by Richard J. Campbell.

[4] See Congressional Distribution Memorandum, *Space Weather and EMP threats to the Grid*, 2015, by Richard Campbell.

[5] Ibid.

[6] Massachusetts Institute of Technology, Retrofitting of Coal-Fired Power Plants for CO2 Emissions Reductions, March 23, 2009, http://web.mit.edu/mitei/docs/reports/meeting-report.pdf.

[7] Thomas A. Prevost and David J. Woodcock, *Transformer Fleet Health and Risk Assessment*, Weidman Electrical Technology, IEEE PES Transformers Committee Tutorial, March 13, 2007, http://grouper.ieee.org/groups/transformers/info/S07/S07-TR_LifeExtension.pdf.

[8] K. Anderson, D. Furey, and K. Omar. *Frayed Wires: U.S. Transmission System Shows its Age*, Fitch Ratings, October 25, 2006.

[9] In recognition of the need to deploy new technologies, Congress indicated its support for grid modernization in the Energy Independence and Security Act of 2007 (EISA) (P.L. 110-140). Specifically, Section 1301 of the act states: "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth ... which together characterize a Smart Grid."

[10] CRS Report R43989, *Cybersecurity Issues for the Bulk Power System*, by Richard J. Campbell. (Hereinafter, CIBS).

systems by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[11]

Although there has not been a publicly-reported cybersecurity event or physical attack resulting in a large scale power outage in the United States,[12] the potential for such attacks to cause a wide scale, long lasting outage cannot be dismissed. The first blackouts attributed to a cyberattack happened in the Ukraine in December 2015.[13] The power outages affected approximately 225,000 customers, and are said to have originated from remote cyber intrusions at three regional electric power distribution companies. The cyberattackers targeted industrial control and operating systems at multiple central and regional facilities. The cyberattack also targeted other critical infrastructure,[14] apparently in an attempt to impair recovery efforts.

A report[15] released by the National Research Council (NRC) in 2012 concluded that well-informed terrorists could black out a large region of the country for weeks or even months.

> An event of this magnitude and duration could lead to turmoil, widespread public fear and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold*.
>
> The largest power system disruptions experienced to date in the United States have caused high economic impacts. Considering that a systematically designed and executed terrorist attack could cause disruptions that were even more widespread and of longer duration, it is no stretch of the imagination to think that such attacks could entail costs of hundreds of billions of dollars—that is, perhaps as much as a few percent of the U.S. gross domestic product (GDP), which is currently about $12.5 trillion.[16]

The NRC report further commented on the potential effects of a combined cyber and physical attack on the grid.

> If they could gain access, hackers could manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, or disable protective systems. Cyber attacks are unlikely to cause extended outages, but if well coordinated they could magnify the damage of a physical attack. For example, a cascading outage would be aggravated if operators did not get the information to learn that it had started, or if protective devices were disabled.[17]

Similar conclusions were reached in a 2015 report from Cambridge University and Lloyds of London, which theorized that a targeted cyberattack could leave 15 states and 93 million people from New York City to Washington, D.C. without power. The scenario estimated the total impact to the U.S. economy at between $243 billion and $1 trillion, resulting from "direct damage to assets and infrastructure, decline in

---

[11] Peter Behr, *Cyberattackers have penetrated U.S. infrastructure systems – NSA Chief*, Environment & Energy Daily, November 21, 2014, http://www.eenews.net/energywire/stories/1060009391.

[12] Steve Reilly, *Bracing for a big power grid attack: 'One is too many'*, USA Today, March 24, 2015, http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/.

[13] DHS - Industrial Control Systems Cyber Emergency Response team, *Cyber-Attack Against Ukrainian Critical Infrastructure*, Alert (IR-ALERT-H-16-056-01), February 25, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[14] "In addition, three other organizations, some from other critical infrastructure sectors, were also intruded upon but did not experience operational impacts." Ibid.

[15] National Academy of Sciences, *Terrorism and the Electric Power Delivery System*, 2012, http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system.

[16] Ibid, page 1.

[17] Ibid, page 2.

sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain."[18]

The 2013 attack on the Metcalf substation in California further cast light on the physical vulnerabilities of the grid. After someone broke into a nearby underground vault to cut telephone cables, snipers opened fire on the substation, knocking out 17 large power transformers sending power to Silicon Valley. A blackout was averted by rerouting power around the substation, and local power plants had to produce more electricity. But it took the local utility 27 days to restore the substation. The Federal Energy Regulatory Commission's (FERC's) chairman at the time (Jon Wellinghoff) reportedly said that "if [the attack] were widely replicated across the country, it could take down the U.S. electric grid and black out much of the country."[19]

Recovery from a well-planned cyber and physical attack on the grid could be complicated by the cost and vulnerability of critical components. While a physical attack on transmission towers to bring down power lines could cause blackouts, the strategic destruction of a number of critical high-voltage transformers could cause long-lasting power outages. These transformers are very large, and difficult to move. A large scale attack may use up the limited inventory of spare units,[20] and it may take months or even years to build new units. The availability of other large components, such as high-voltage circuit breakers could also hamper recovery efforts.[21]

Industry and Government Coordination on Recovery Efforts

The electric utility industry generally prepares for power outages from weather-related events, and views the potential for a major cybersecurity attack or similar event as a low probability risk. As such, the industry seeks to balance grid security efforts and expenditures with the perceived risks. In the event of a large power outage, electric utilities often call upon other utilities via their mutual assistance agreements[22] (MAAs) to help restore services. MAAs can help to reduce the duration of weather-related outages by bringing in outside resources to aid the recovery effort.

If an event is severe enough to be a federally-declared disaster,[23] the Department of Homeland Security's (DHS's) Federal Emergency Management Agency (FEMA) is empowered to provide federal assistance.

---

[18] University of Cambridge Centre for Risk Studies and Lloyds of London, *Business Blackout*, The insurance implications of a cyber attack on the US Power Grid, 2015, https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

[19] Rebecca Smith, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, Wall Street Journal, February 5, 2014, http://www.wsj.com/articles/SB10001424052702304851104579359141941621778.

[20] The electric power industry has several programs for participating companies to share spare transformer equipment. For example," [the Edison Electric Institute's Spare Transformer Equipment Program] requires participating utilities to maintain (or acquire) a specific number of transformers up to 500 kV to be made available to other utilities in case of a critical substation failure. Sharing of transformers is mandatory based on a binding contract subject to a 'triggering event'—a coordinated act of deliberate, documented terrorism resulting in the destruction or disabling of a transmission substation and the declaration of a state of emergency by the President...[and in] 2012, NERC initiated its Spare Equipment Database program intended to serve as a tool to 'facilitate timely communications between those needing long-lead time equipment damaged in a [high impact, low frequency] event and those equipment owners who may be able to share existing equipment being held as spares by their organization.'" See CRS Report R43604, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak.

[21] NAS.

[22] Edison Electric Institute, *Understanding the Electric Power Industry's Response and Restoration Process*, May 2014, http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf.

[23] "[The] Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 100-707, signed into law November 23, (continued...)

> FEMA's mission is to reduce the loss of life and property and protect communities nationwide from all hazards, including natural disasters, acts of terrorism, and other man-made disasters. FEMA leads and supports the nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery and mitigation.[24]

FEMA can provide financial assistance to electric utilities to aid in disaster recovery efforts. In general, FEMA will determine a utility's eligibility, and "will cover at least 75 percent of the repair, restoration or replacement costs for infrastructure owned by eligible applicants."[25]

The electric power industry also works with the Departments of Energy and Homeland Security on a number of cyber and physical security initiatives.[26] The Electricity Sub-Sector Coordinating Council (ESCC) is the principal liaison between the federal government and the electric power sector. It represents the electricity sub-sector (as part of the Energy Critical Infrastructure sector)[27] under DHS's National Infrastructure Protection Plan (NIPP).[28] The ESCC draws its membership from all segments of the electric utility industry, and is led by three chief executive officers – one each from the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association.[29] Among its activities, the ESCC coordinates industry and government efforts on grid security, guides infrastructure investments and R&D for critical infrastructure protection, seeks to improve threat information sharing and processes with public- and private-sector stakeholders, and coordinates cross sector activities with other critical infrastructure sectors.

The bulk electric power system has mandatory and enforceable standards for cybersecurity. The Energy Policy Act of 2005 (EPACT) (P.L. 109-58) gave the Federal Energy Regulatory Commission authority over the reliability of the grid, with the power to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). Currently, the North American Electric Reliability Corporation (NERC) serves as the ERO. NERC therefore proposes reliability standards for critical infrastructure protection (CIP) which are updated considering the status of reliability and cybersecurity concerns for the grid. FERC recently added mandatory and enforceable physical security requirements to its critical infrastructure protection standards.[30]

The electric utility industry also conducts a biennial grid security and emergency response exercise (GridEx) in which electric power and other stakeholders respond to simulated cyber and physical attacks.

(...continued)

1988; amended the Disaster Relief Act of 1974, Public Law 93-288. It created the system in place today by which a presidential disaster declaration of an emergency triggers financial and physical assistance through the Federal Emergency Management Agency (FEMA). The Act gives FEMA the responsibility for coordinating government-wide relief efforts." See http://www.fema.gov/about-agency.

[24] Federal Emergency Management Agency, *FEMA*, FEMA B-653, July 2008, http://www.fema.gov/pdf/about/brochure.pdf.

[25] Edison Electric Institute, *Federal Disaster Assistance and Utilities*, 2014, http://www.eei.org/issuesandpolicy/RES/14Tab5.pdf.

[26] See CIBS, page 16.

[27] The Energy Critical Infrastructure sector includes the electricity, petroleum, and natural gas subsectors. Department of Homeland Security, *Critical Infrastructure Sectors*, 2015, https://www.dhs.gov/critical-infrastructure-sectors.

[28] Department of Homeland Security, *National Infrastructure Protection Plan*, October 27, 2015, https://www.dhs.gov/national-infrastructure-protection-plan.

[29] Edison Electric Institute, *Electric Subsector Coordinating Council*, March 2015, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/ESCC%20Brochure.pdf.

[30] However, these rules largely do not apply to distribution system utilities which are subject to mostly state regulation. FERC Order No. 773 establishes a "bright-line" threshold essentially considering all transmission facilities and related facilities operating at 100 kilovolts or above to be part of the bulk electric power system. As such, these facilities are subject to the applicable NERC reliability standards.

The most recent exercise, GridEx III took place on November 18-19, 2015, and involved 364 organizations from across North America.[31]

In the event of a wide-scale power outage caused by a major attack or a disaster, electric utility efforts to restore power would likely have to be augmented by state and federal resources. Given the potential for damage to the nation's economy from a major attack on the grid, some might suggest a greater focus on recovery is needed and should become as much a part of a grid security strategy as the efforts to secure the system. NERC has essentially agreed, saying in its GridEx III report that severe emergency situations may require greater coordination with states and the federal government to identify physical risks to electricity facilities, and to identify cyber risks in addressing malware on control systems before recovery efforts could begin.[32]

Congress included provisions to give the U.S. Department of Energy (DOE) new authority to order electric utilities and NERC to implement emergency security actions in the "Fixing America's Surface Transportation Act" (FAST; P.L. 114-94).[33] DOE is designated as the lead sector specific agency for cybersecurity for the Energy sector.[34] Section 61004 of FAST also requires DOE (in consultation with FERC, NERC, and electrical infrastructure operators) to develop a plan for storing spare large power transformers and emergency mobile substations which can be quickly deployed to replace damaged large power transformers and substations which serve grid-critical functions.[35]

Areas for Further Congressional Consideration

In any discussion of extended power outages, two prominent themes emerge—preparation and recovery. If utilities are aware of an impending storm or weather-related event which may cause outages, they are expected to make preparations for restoration of services in as timely a manner as possible. Recovery from any such event will depend on the severity of the storm and the resulting damage. Recovery can be hastened, and the amount of damage to electric power infrastructure can be minimized, if good maintenance, restoration, organization, and communications strategies are followed on an ongoing basis.

However, a coordinated, major cyber and physical attack on the electric grid would severely test the ability of the nation to recover, especially as plans for such a recovery are currently in progress. The electric utility industry generally bases its response to the potential for such events based on the perceived

[31] "The electricity industry participants included chief executives from investor and publicly owned utilities, cooperatives, and independent system operators from the U.S. and Canada. The U.S. federal and state governments were represented by senior officials from various departments and agencies. In addition, approximately 70 individuals associated with the participants attended the tabletop as observers to provide feedback." Observers included the White House; National Security Council; Department of Energy; Department of Homeland Security, including Federal Emergency Management Agency; Department of Defense, including U.S. Cyber Command, U.S. Northern Command, North American Aerospace Defense Command; National Security Agency; Federal Bureau of Investigation; and the National Guard. North American Electric Reliability Corporation, *Grid Security Exercise - GridEx III*, March 2016, http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf. (Hereinafter, GridExIII).

[32] Ibid. Page 15.

[33] Section 61003 of FAST creates a new section 215A of the Federal Power Act, that following a written determination by the President, authorizes DOE to order utilities, the North American Electric Reliability Corporation (NERC), and Regional Entities to implement emergency security measures for up to 15 days at a time.

[34] The energy sector is one of 16 critical infrastructure sectors identified in Presidential Policy Directive-21 (PPD-21), Critical Infrastructure Security and Resilience. Sector specific agencies are designated with specialized expertise in those critical infrastructure sectors that are tasked with various roles and responsibilities for their respective sectors, as specified in PPD-21 (i.e., development of sector-specific plans, coordination with the Department of Homeland Security, and incident management responsibilities).

[35] Paul Parfomak, *Electric Grid Physical Security: Recent Legislation*, CRS Insight IN10425, 2016.

risks. The industry relies on the federal government to share relevant, real-time intelligence on risks from terrorism or cybersecurity threats, communicating the quality of threat information in a timely manner so it can respond appropriately. Improvements in threat/risk assessment would aid this process.

A focus on recovery would have to consider the mutual dependence and implications to other critical infrastructure (especially communications systems)[36] of an electric grid failure, and how quickly such impacts could proliferate if not planned for in advance. Congress may consider how the grid of the future will address cyber and physical security concerns, as more distributed generation is incorporated. The U.S. electric grid is evolving. Incorporating elements to increase system resiliency as it develops will aid in reducing the vulnerability of the system.

NERC itself concluded in its report on GridEx III that, after a major grid disruption, restarting generation and energizing transmission and distribution systems would be a first priority. Restoring service to communications systems, oil and gas, water supply/treatment and hospital customers would be a secondary priority. Electric power systems may be operating at reduced levels of service and reliability for an extended period at such a time. Congress may consider how planning for subsequent restoration of services would proceed to ensure that all civilian communities are kept informed, and treated as equitably as possible in disaster recovery efforts.

[36] "[PPD-21] identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors." The White House, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*, Presidential Policy Directive / PPD-21, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Testimony of Gerry Cauley, President and Chief Executive Officer,
North American Electric Reliability Corporation

House Transportation and Infrastructure Committee
Subcommittee on Economic Development, Public Buildings, and Emergency Management

April 14, 2016

Introduction

Good morning Chairman Barletta, Ranking Member Carson, members of the subcommittee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am pleased to speak with you today about the responsibilities that Congress has vested in NERC to assure reliability of the bulk-power system (BPS) in North America.

The North American BPS is among the nation's most critical infrastructures. Virtually every critical sector depends upon electricity. The BPS is also one of the largest, most complex systems ever created. It is robust and highly reliable. Nevertheless, conventional and non-conventional factors do present risks to the BPS. Therefore, assuring reliability, mitigating risks and preparing for recovery and restoration of the BPS following a loss of service is a vital concern.

My testimony discusses how NERC uses a range of tools to address key reliability challenges facing the BPS today. Given the subcommittee's interest in recovery efforts following a grid emergency, I will also discuss our biennial grid security exercise – a forward-looking initiative which helps industry and other stakeholders prepare for managing BPS security events. I welcome this opportunity to discuss these topics with the subcommittee.

About NERC

NERC is a private non-profit corporation that was founded in 1968 to develop voluntary operating and planning standards for the users, owners and operators of the North American BPS. Pursuant to Section 215 of the Federal Power Act (FPA) (16 U.S.C. §824o) and the criteria included in Order No. 672 for designating an Electric Reliability Organization, FERC certified NERC as the Electric Reliability Organization on July 20, 2006. On March 16, 2007, FERC issued Order No. 693 which approved the initial set of Reliability Standards. These Reliability Standards became mandatory in the United States on June 18, 2007.

NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

industry personnel. Through the Electricity Information Sharing and Analysis Center (E-ISAC), NERC performs a critical role in real-time situational awareness and information sharing to protect the electricity industry's critical infrastructure against vulnerabilities. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. Our jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

Reliability & Security Challenges

To assure the reliability and security of the North American grid, we must remain focused on emerging trends and the changing risk landscape, which ranges from conventional risks, such as extreme weather and equipment failures, to new and emerging risks in the security arena.

Physical Security Threats – Among other events, an April 2013 attack against a substation in California raised concerns about physical attacks on critical electric infrastructure. It is important to note the attack did not result in a power outage; in fact, no customer lost service. Nevertheless, the incident is a reminder of the vulnerabilities of our BPS and while rare, demonstrates that attacks are possible and have the potential to cause significant damage to assets and disrupt customer service. NERC's physical security standard – CIP-014-1 – requires users, owners and operators of bulk power system facilities to conduct a risk assessment to identify critical facilities and then develop and implement security plans to protect against attacks on those facilities. [1]

Cybersecurity Threats – In the Energy Policy Act of 2005, Congress anticipated the emerging cybersecurity threat by defining reliability standards to be developed by the ERO to include cybersecurity protection.[2] Since 2007, NERC has updated its standards to reflect the changing cybersecurity landscape. The fifth version of NERC's Critical Infrastructure Protection (CIP) cybersecurity standards will become effective on July 1 of this year. CIP Version 5 requires that all cyber assets must now be categorized as Low, Medium, or High Impact assets. The revised standards also include new requirements with new cybersecurity controls to address emerging cyber threats. In addition, CIP Version 5 uses a risk-based approach to implementing appropriate and changing technologies. That is, rather than specifying how to implement a requirement, the revised requirements specify the risk-based result that must be achieved, which enables industry to implement new and emerging technologies to address the risk. NERC is working with industry on the transition to this new standard, which is one of the most comprehensive, risk-based standards ever mandated. Today, the electric sector (along with nuclear) remains the only critical infrastructure sector subject to mandatory, enforceable cybersecurity standards.

Cyber attacks on three distribution utilities in Ukraine on December 23, 2015 has garnered significant attention. The Ukrainian incidents affected up to 225,000 customers in three distribution-level service territories and lasted for several hours.[3] A team from the United States, which included experts

[1] Federal Power Act, Sec. 215(a)(3).
[2] Federal Power Act, Sec. 215(a)(3).
[3] "Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case," SANS Industrial Control Systems and E-ISAC, March 18, 2016.

from the Department of Energy (DOE), the Department of Homeland Security (DHS), the FBI and NERC, assisted the government of Ukraine in gaining more insight into the event.[4] The events in Ukraine are a reminder that cyber threats are real and that constant vigilance is needed to protect the reliability of the North American grid. At the same time, it is important to note that the operational and technical aspects of the North American bulk power system are different from those of the Ukrainian system. Other differences include the U.S. industry's mandatory and enforceable cyber security standards, including security management controls and authorized personnel and training controls; network segmentation; and the use of licensed anti-virus software, among other things.

The Changing Resource Mix/Essential Reliability Services – NERC must anticipate risks before they manifest as threats to reliability. For example, NERC is working with industry, regulators, and policymakers to assure reliability during a period of rapid transformation in the sources of energy used to produce electricity. Part of this effort includes two recent reports detailing the need to maintain essential reliability services.[5] ERS include frequency response, ramping capability, and voltage support, all of which are needed to assure that the grid remains balanced and able to respond and deliver electricity where it is needed when it is needed. The BPS is undergoing a broad transformation with retirements of coal units and some nuclear units, and additions of resources fueled by natural gas, wind, and solar. Distributed generation, energy efficiency, and demand response are also changing the way in which the grid is called upon to meet electricity demand. Regulations such as the Environmental Protection Agency's Clean Power Plan have the potential to hasten the transformation of the electric system. As this trend continues, it is critical for new resources to provide ERS. For more information on ERS, NERC has developed three videos designed to inform a general audience about the importance of these resources.[6]

FERC/NERC/Regional Entity Joint Review of Restoration and Recovery Plans – In January 2016, NERC published a joint report with FERC and NERC Regional Entities reviewing restoration and recovery plans of nine entities with significant bulk power grid responsibilities.[7] The objective of the review was to assess and verify the electric utility industry's bulk power system recovery and restoration planning, and to test the efficacy of related Reliability Standards in maintaining and advancing reliability in that respect. Overall, the joint staff review team found that the participants have system restoration plans to be thorough and highly-detailed. The reviewed plans require identification and testing of blackstart resources, identification of primary and alternate cranking paths, and periodic training and drilling on the restoration process under a variety of outage scenarios. Likewise, the joint staff review team found that participants had extensive cyber security incident response and recovery plans for critical cyber assets covering the majority of the response and recovery stages. In addition, the team observed that each participant has full time personnel dedicated to the roles and responsibilities defined in their respective

[4] See ICS-CERT report at https://ics-cert.us-cert.gov/alerts/IR-ALERT-N-16-056-01.
[5] "Essential Reliability Services Task Force Measures Framework Report," NERC, November 2015.
See also "Reliability Considerations for Clean Power Plan Development," NERC, January 2016.
[6] See NERC ERS videos at https://vimeopro.com/nerclearning/ersttf 1.
[7] "Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans," FERC/NERC/Regional Entities, January 2016. http://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf

response and recovery plans. The joint staff review team identified several opportunities for improving system restoration and cyber incident response and recovery planning and readiness and further work will be done to follow up on the reports recommendations.

Electricity Information Sharing and Analysis Center

Mandatory and enforceable Reliability Standards are an important foundation of the complex endeavor to assure grid reliability. NERC employs other tools to help address new and emerging threats. Information-sharing through the NERC-operated E-ISAC[8] is one such tool.

The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange. The E-ISAC, in collaboration with DOE and the Electricity Sector Coordinating Council (ESCC),[9] serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

The E-ISAC:

- Identifies, prioritizes, and coordinates the protection of critical power services, infrastructure service, and key resources;
- Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices;
- Provides rapid response through the ability to effectively contact and coordinate with member companies, as required;
- Issues alerts to industry ranging from advisory notices to essential actions requiring recipients to respond as defined in the alert;[10]
- Provides and shares campaign analysis, which includes capturing, correlating, trending data for historical analysis, and sharing that information within the sector;
- Receives incident data from private and public entities;
- Assists DOE, FERC, and DHS in analyzing event data to determine threats, vulnerabilities, trends and impacts for the sector, as well as interdependencies with other critical infrastructures (this includes integration with the DHS National Cybersecurity and Communications Integration Center (NCCIC));
- Analyzes incident data and prepares reports based on subject matter expertise in security and the bulk power system;
- Shares threat alerts, warnings, advisories, notices, and vulnerability assessments with the industry;
- Works with other ISACs to share information and provide assistance during actual or potential sector disruptions whether caused by intentional, accidental, or natural events;

[8] https://www.esisac.com/.
[9] See ESCC website at http://www.electricitysubsector.org/.
[10] http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx.

- Develops and maintains an awareness of private and governmental infrastructure interdependencies;
- Provides an electronic, secure capability for the E-ISAC participants to exchange and share information on all threats to defend critical infrastructure;
- Participates in government critical infrastructure exercises; and
- Conducts outreach to educate and inform the electricity sector.

GridEx III

Led by the E-ISAC, NERC conducted its third biennial grid security and emergency response exercise, GridEx III, on November 18–19, 2015.[11] GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise (a simulated cyber and physical attack) and a separate executive tabletop session featuring 32 industry executives and senior officials from federal and state governments. All told, more than 4,400 individuals from 364 industry, law enforcement and government organizations across North America participated in GridEx III.

The objectives of GridEx III were to:

- Exercise crisis response and recovery;
- Improve communication;
- Identify lessons learned; and
- Engage senior leadership.

GridEx III provided participants with the opportunity to exercise their incident response procedures during large-scale security events affecting North America's electricity system. The large-scale cyber and physical attack scenario was designed to overwhelm even the most prepared organizations.

Distributed Play Results

Participating organizations were encouraged to identify their own lessons learned and share them with NERC. NERC used this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS, including:

- *Coordinated Response and Communication.* GridEx III highlighted the importance of well-coordinated communications. NERC recommended that organizations should review documentation that describes their internal information sharing processes in the context of a large-scale event and exercise these communication capabilities.

- *Reporting Mechanisms.* GridEx III participants observed that some aspects of the industry's information sharing and reporting tools are redundant, time-consuming to use, and provide no feedback mechanism to those who most need the information. NERC recommended that

[11] For more information on GridEx III, see "Grid Security Exercise, GridEx III Report," March 2016, at: http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf.

organizations should review the tools and reporting processes in use to identify opportunities to improve the efficiency and efficacy of the information-sharing process.

- *Active Participation of Operations Management, Support Staff, and System Operators.* GridEx III succeeded in providing exercise scenarios that linked the physical and cyber attacks with how system operators would respond to mitigate the impact of these attacks on bulk power system reliability. NERC recommended that future GridEx exercises should continue to include scenarios that prompt operations management, support staff, and field operations to interact with cyber and physical security personnel. NERC also identified the essential role of reliability coordinators in designing future GridEx exercises to reflect local conditions and provide for effective coordination of generation, transmission and system operations in the context of cyber and physical security events.

- *E-ISAC Information Sharing.* Participants observed that the E-ISAC portal should be enhanced for real-time urgent communication with portal members. Participants observed that information was quickly buried within the portal, making it become difficult to highlight important information. NERC recommended that the E-ISAC should continue to enhance the E-ISAC portal to support real-time, searchable, urgent communication and collaboration with portal members.

- *Introduction of New Exercise Tools.* While new exercise tools enhanced the exercise, there is room for continued improvement. Prior to the next exercise, functionality and volume/capacity tests should be performed.

- *Advance Exercise Planning Timelines.* Planning for the next GridEx exercise should begin earlier than GridEx III to provide organizations with more time to conduct their own planning and training activities. NERC should develop a firm delivery schedule with stakeholders, including major planning milestones, and tool development and testing at the outset of exercise planning. Future GridEx exercises should continue to provide opportunities for organizations to customize their scenario injects provided they are consistent with and support the overall NERC scenario as coordinated with their Reliability Coordinator.

- *After-Action Survey and Lessons Learned.* During the early stages of the GridEx III planning process, NERC developed a set of metrics to assess the success of the exercise that included the questions in the after action survey. Lessons learned reports that were submitted to NERC by participating organizations provided valuable input, but a greater number of reports would provide a more complete and representative set of lessons learned. The NERC planning team should consult with participating active organizations to understand any reluctance to share lessons learned and identify ways to increase the response rate.

Executive Tabletop Results

The executive tabletop engaged senior leaders in a robust discussion of the policy issues, decisions, and actions needed to respond to a major grid disruption caused by simulated physical and cyber attacks. Participants identified security and reliability challenges and opportunities to improve prevention, response, and recovery strategies. The discussion centered on three key areas: unity of messaging, unity of effort, and extraordinary measures.

Unity of Messaging. Participants explored how industry and government assess a crisis event, and receive and share information with each other and the public. Managing the challenges and opportunities related to social media was of particular interest.

Unity of Effort. While both industry and government have considerable resources at the ready to respond to crisis events, participants considered how to improve coordination during severe emergency situations. Industry needs to coordinate with local law enforcement to identify and assess the physical risks to electricity facilities and workers. Unlike how industry responds to major storms through mutual assistance, industry's capability to analyze malware is limited and would require expertise likely available from software suppliers, control system vendors, or government resources.

Extraordinary Measures. The industry operates within a regulatory framework designed within normal planning and operating criteria. Participants considered regulatory and legislative needs, as well as extraordinary government support, that could enhance timely and effective recovery under extreme circumstances that clearly exceed normal criteria.

The following summarizes additional key findings from the executive tabletop:

- *Establish Priorities for Restoring Electricity Service*. When restoring power following a large-scale outage, utilities' first priorities focus on supplying electricity to re-start generation and energize transmission and distribution lines and equipment. Second priorities include "lifeline" customers such as communications, oil and gas, water supply/treatment and hospitals.

- *Simplify Electricity System Operation Under Emergency Conditions*. North America's electricity system is operated by highly trained staff using sophisticated technology systems to forecast load, monitor electricity flows, dispatch generation, remotely operate equipment, and administer markets. In the event that these normal processes are disrupted, it may be possible to simplify how the electricity system is operated to provide basic service but at reduced levels of reliability and less economically.

- *Consider Mechanisms to Prevent Financial Defaults*. Utilities will need unprecedented levels of financial resources in order to restore their facilities and eventually resume normal operations.

- *Manage Personal and Corporate Liability Risks*. North America's bulk power system is designed and operated to meet extensive legal and regulatory requirements (e.g., environmental, safety, financial, labor, commercial). Some of these requirements may delay or prevent restoration during a large-scale event.

Conclusion

As our economy becomes increasingly electrified, and as we become ever more dependent upon electric infrastructure, the reliability of the BPS becomes ever more important. The North American BPS is reliable and resilient. A strong and effective regime is in place to assure reliability. However, given the evolving threats to the BPS, we must remain vigilant. Grid Ex III showed that there is more that we can and should do to be better positioned to plan for and respond to a disruption of service upon which we all depend. This is a big job that involves everyone at the table today and many more.

I appreciate the opportunity to discuss NERC's role in assuring reliability and protecting the grid from physical and cyber threats, and would be pleased to answer any questions.

STATEMENT OF WILLIAM H. SPENCE
CHAIRMAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER
PPL CORPORATION

BEFORE THE HOUSE COMMITTEE ON TRANSPORTATION & INFRASTRUCTURE
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS
AND EMERGENCY MANAGEMENT

"PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER AND PHYSICAL THREATS"

APRIL 14, 2016

Introduction

Good morning Chairman Barletta, Ranking Member Carson and Members of the Subcommittee. My name is Bill Spence, and I am the Chairman, President and Chief Executive Officer of PPL Corporation.

Headquartered in Allentown, Pennsylvania, PPL Corporation is one of the largest companies in the U.S. utility sector. Our seven utility subsidiaries serve 10 million customers in the U.S. and the United Kingdom. We deliver electricity to customers in the U.K., Pennsylvania, Kentucky, Virginia and Tennessee. We deliver natural gas in Kentucky. In addition, we own and operate about 8,000 megawatts of generation capacity in Kentucky.

In addition to overseeing PPL's domestic and international operations, I am a member of the Executive Committee of the Edison Electric Institute (EEI) and co-chairman of EEI's CEO Policy Committee on Reliability and Business Continuity. I am also a member of the Electricity Sub-Sector Coordinating Council (ESCC), which serves as the principal liaison between the federal government and the electric power sector to address national security threats to the nation's power grid.

Thank you for providing PPL Corporation with an opportunity to testify on the important topic of the reliability and resiliency of the power grid in the face of continuing cyber, physical and natural threats.

As I hope to convey in my testimony, PPL and the broader electric power industry are committed to protecting the nation's power grid from threats of all types. This commitment did not arise in the face of new, modern threats; it is a shared commitment that is deeply rooted in the fabric of the industry. We have made, and continue to make, significant investments in tools, technology and people to strengthen our defensive capabilities and ensure grid reliability and resiliency.

In particular, we recognize that cyber threats are persistent and evolving. Even as we enhance our responses to meet the rising threats, there is no way to fully guarantee a breach will not occur. As such, we plan and drill regularly to ensure we can respond and recover quickly and effectively should an emergency arise.

Overview of Industry Efforts

Protecting the nation's electric power grid and ensuring a reliable and affordable supply of energy are top priorities for the electric power industry.

As owners and operators of critical infrastructure, the electric power industry's top priority is to ensure the reliability and resiliency of the North American electric grid. With cyber and physical security a key focus of our reliability assurance strategy, the industry has a strong record of working together and with government partners to identify, assess, and respond to all threats.

The electric sector takes a "defense-in-depth" approach to protecting grid assets. This includes: rigorous, mandatory, enforceable and regularly audited reliability standards; close coordination among industry and with government partners at all levels; and efforts to prepare, respond and recover should power grid operations be affected in any way.

Security standards and regulations are an important part of the industry's security posture.

The electric power and nuclear sectors are subject to North American Electric Reliability Corporation (NERC) mandatory, enforceable and monitored Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties of up to $1 million per violation per day. In fact, our industry is the only one subject to mandatory, federally enforceable cyber and physical standards.

These mandatory standards continue to evolve with input from subject matter experts across the industry and government. Currently, the electric power sector must comply with Version 3 of the cybersecurity standards, while Versions 5 and 6 become enforceable on July 1, 2016. These new versions are more rigorous than the past versions and not only increase the scope of the standards, but also add several new cybersecurity requirements that mirror cybersecurity best practices.

In addition to implementing Versions 5 and 6 of the cybersecurity requirements, the industry is implementing requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry is also using voluntary standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as the Department of Energy's Cybersecurity Capability Maturity Model (C2M2).

PPL and others throughout the industry are assessing their cybersecurity capabilities against this framework and capability maturity model and, based on results, prioritizing their investments to strengthen cybersecurity.

While regulations and standards provide a solid foundation for strengthening the industry's security posture, they alone are not sufficient. As the threat environment evolves, so must the industry's security efforts.

In addition to regulations and standards, close coordination and the sharing of threat information between government and industry help to protect the power grid.

Protecting the grid is a responsibility shared by both industry and government. The industry owns and operates most of the grid, while the government has law enforcement and intelligence gathering capabilities and is responsible for national security. That's why industry and government must work together to protect infrastructure critical to the life, health and safety of Americans.

According to the National Infrastructure Advisory Council, the electric power sector is viewed as a model for how critical infrastructure sectors can more effectively partner with the government. Our intent is to keep it that way.

The Electricity Sub-Sector Coordinating Council (ESCC), which I referenced earlier in my remarks, brings senior electric power industry executives like myself together with senior Administration officials from the White House; Departments of Energy, Homeland Security, and Defense; the Federal Energy Regulatory Commission; and the Federal Bureau of Investigation, to improve sector-wide resilience against all hazards and potential threats.

The ESCC is focused on several key areas, including planning and exercising coordinated responses to attacks or major disruptions to the power grid; making sure that information about threats is communicated quickly among government and industry stakeholders; deploying government-held technologies on electric power systems that improve situational awareness of threats to the power grid; and cross-sector coordination with the interdependent critical infrastructure sectors.

The ESCC has developed a playbook that provides a framework for senior industry and government executives to coordinate in support of response and recovery efforts. This playbook already has been used during exercises, including NERC's GridEx III exercise this past November, which I will address later in my testimony.

In addition, the ESCC recently established several industry-government working groups on key initiatives. These initiatives include:

- Developing a cyber mutual assistance framework to coordinate responses to significant cyber incidents;

- Partnering with the Electric Power Research Institute to address threats posed by electromagnetic pulses;
- Reviewing threats to the supply chain;
- Accessing enhanced background checks for critical employees;
- Instituting a Member Executive Committee, which I chair, that is providing strategic guidance to the Electricity Information Sharing and Analysis Center (E-ISAC).

The Member Executive Committee is working directly with the E-ISAC to ensure the electric power sector has the very best information-sharing and analysis capabilities and an organization that responds to the needs of industry operators. This endeavor is an extraordinary example of the partnership that can lead to improved outcomes for security of the industry and, by extension, the nation.

The federal government plays a crucial role in strengthening the security of the power grid through information sharing.

In the fight against cyber and physical threats, industry-government information sharing, as well as close coordination among grid operators and government partners, is critical. The E-ISAC gathers industry information on security-related events for sharing with its government partners and shares government information on threats with industry.

The sharing of threat information and data analysis is taking place between the E-ISAC and the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). The coordination between the E-ISAC and NCCIC is improving the security posture, situational awareness, and preparedness and response capabilities of federal, state and local governments; intelligence and law enforcement communities; and the private sector when it comes to cyber and physical events that might impact the electric power sector.

One example of the industry-government information-sharing efforts worth highlighting is the implementation of the Cyber Risk Information Sharing Program (CRISP), which is bolstering the sector's and the government's situational awareness. CRISP is a public-private partnership that enables sharing of cyber threat data among the government, the National Labs, the E-ISAC, and industry stakeholders. Cyber threat information shared through CRISP is helping to inform important security decisions not just among participating electric power companies, but all

sector participants through the E-ISAC. When one company experiences a cyber event, that information is immediately shared with all companies that deploy CRISP. This sharing of information allows industry members to deploy the best resources to identify and deflect incoming threats. By the end of 2015, more than 100 million households, or about 75 percent of U.S. electricity customers, were covered by companies, including PPL, that had deployed CRISP.

However, more actionable threat information sharing is needed, which is why the industry and PPL fully supported Congress passing cybersecurity information-sharing legislation, including liability protections for businesses, to provide a framework for more voluntary information sharing. The industry looks forward to working with the government to fully implement the Cybersecurity Information Sharing Act of 2015, commonly referred to as CISA.

Congress also has passed legislation that granted the Secretary of Energy limited-duration authority to address declared grid security emergencies, and directed DOE to submit a plan to Congress evaluating the feasibility of establishing a Strategic Transformer Reserve.

We appreciate the efforts of Congress to work with our industry to further protect our nation's power grid. And, because cyber threats are always evolving, we hope Congress will support more investment in research and development focused on strengthening existing efforts and developing new technologies, including those that will improve the speed, integration and analysis of threat information while protecting sensitive information.

The electric power sector is focusing even more on incident response and recovery efforts.

The third major element of the industry's "defense-in-depth" strategy is incident response. Power grid operators manage risk, but do not eliminate it, which is why a sound approach to security must include contingency planning.

Electric power companies, including PPL, continuously plan and exercise for a range of potential threats to the power grid, as well as the possibility of a widespread incident.

Electric power companies are constantly managing risk by understanding that something could go wrong and planning for the worst-case scenario. If you look at the power grid, it is one big, interconnected machine with thousands of owners and operators; everyone has to work together.

Through storm preparation and mutual assistance networks, the electric power sector has decades of experience working together in response to major incidents. For example, the electric power sector's response to Superstorm Sandy had companies from as far away as California, Texas and Canada sending equipment and crews into the affected regions to restore power. More than 80 companies and tens of thousands of mutual assistance crews responded. Following Hurricanes Katrina and Rita, PPL sent crews as far as the Gulf Coast states to support recovery efforts. In short, mutual assistance is not just a program, it is in our DNA.

Just as electric power companies share crews as part of the industry's voluntary mutual assistance programs to restore power, they also regularly share transformers and other equipment. The electric power sector is expanding equipment-sharing programs – like the Spare Transformer Equipment Program (STEP), *SpareConnect*, and the newly announced Grid Assurance program – to improve grid resilience no matter the threat.

The electric power sector's success regarding these transformer sharing programs depends upon the industry's ability to move large spare equipment, such as transformers, quickly over our rails, roadways and waterways. That is why the industry is working with other critical infrastructure sectors and the government to improve the coordination and preparation involved in moving large transformers during an emergency. For example, electric power companies, Class I railroads, and the heavy hauler and rigging industries developed a new Transformer Transportation Emergency Support Guide to expedite the deployment of equipment and services that would be needed to move these critical assets rapidly in an emergency.

With respect to exercises, this past November, NERC conducted the third industry-wide grid security and incident response exercise, known as GridEx III. GridEx III brought together more than 364 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico to participate. PPL's U.S. distribution and transmission subsidiaries participated fully in the exercise, which was a rigorous and comprehensive two-day drill that simulated coordinated cyber and physical attacks on the power grid.

GridEx III also included an executive tabletop exercise that brought together 32 electric power sector executives and senior U.S. government officials to work through incident response protocols to address widespread outages. GridEx III was a continuation of industry-government efforts to participate in exercises that strengthen the security and resiliency of the power grid.

On March 31, NERC released its GridEx III After-Action Report to the public. Overall, NERC found that since GridEx II, industry and government responses to a significant cyber / physical attack continue to improve. The After-Action Report identified a number of recommendations for industry and government to continue to strengthen their coordination, preparation and response capabilities. As was the case with GridEx I and II, these recommendations will provide a road map for how the ESCC, with input from NERC, and the government will address security issues over the next two years.

Following GridEx III, the ESCC and our government partners agreed that more work is needed to help coordinate sector-wide response and recovery efforts, especially at the state and local level. Also, the ESCC established the Cyber Mutual Assistance Task Force to convene industry experts in an effort to inform and establish a cyber mutual assistance framework to aid electric power companies in rebuilding and recovering necessary computer systems in the event of a regional or national cyber incident. This program will build on the electric power sector's culture and tradition of mutual assistance to develop resource-sharing relationships that provide "surge capacity" should a cyber incident exceed the capacity for an individual company to respond.

PPL's Commitment to Protecting Critical Infrastructure

PPL is actively engaged in the industry efforts I have highlighted and takes an aggressive, defense in-depth approach to protect the power grid.

We strive at all times to comply with the industry's rigorous, mandatory and enforceable cyber and physical security standards.

We coordinate closely with industry partners and federal government agencies to share best practices and to prepare for and respond to potential threats. As I highlighted earlier, I am a member of the ESCC. PPL was an early participant in E-ISAC. We also participate in the CRISP

program. Through that program, we have received threat notifications and taken proactive security measures.

In addition, we continue to work to maintain and strengthen our ties to state agencies, state and local law enforcement, and state Fusion Centers that receive, analyze, gather and share threat-information.

As part of our broader efforts to modernize and reinforce the power grid — efforts that included infrastructure investments of more than $3.5 billion in 2015 and will include additional investment of more than $16 billion over the next five years — PPL is taking steps to better protect critical infrastructure. This includes improved system designs and redundancy that make the power grid more resilient and secure.

We conduct education and training for employees to improve threat awareness and prevent attacks. Further, we exercise and prepare regularly for grid emergencies, be they the result of an attack or severe weather. We have robust crisis management plans in place to guide our efforts in responding to threats and restoring power quickly if issues arise. As we have demonstrated in recent years during major storms, we are also committed to keeping federal, state and local officials, along with the general public, well informed of our efforts when service to customers is affected. This includes holding conference calls for elected officials and community leaders. It also includes keeping the public aware of the status of our restoration efforts via the Web, social media, news releases and direct communication to customers through text, email and other means.

Conclusion

In conclusion, PPL and the electric power industry are united in our commitment to protecting the nation's critical energy infrastructure.

Providing safe, reliable and affordable electricity is our top priority. Our industry invested more than $103 billion in energy infrastructure in 2015 alone — investments that included modernizing and better securing the nation's power grid. In addition, the industry made significant investments in preparedness, including training and exercises, to ensure we can respond quickly and effectively should a physical or cyber attack affect grid operations.

These sustained investments are making the grid more resilient and more secure every day.

Thank you again for the opportunity to present testimony on this important issue. I look forward to answering any questions you may have.

Testimony of Ms. Bobbi Kilmer

President and CEO of the Claverack Rural Electric Cooperative

to the

Committee on Transportation and Infrastructure Subcommittee on Economic Development, Public Buildings and Emergency Management

U.S. House of Representatives

April 14, 2016

Introduction

Chairman Barletta, Ranking Member Carson, and members of the Committee, thank you for inviting me to testify today on how electric cooperatives manage the consequences of a power outage. Regardless of the cause, getting power restored as quickly and as safely as possible requires advance thinking and planning well before the actual event. My name is Bobbi Kilmer and I am testifying today on behalf of the Claverack Rural Electric Cooperative and the National Rural Electric Cooperative Association.

Electric cooperatives prioritize preparing and planning for recovery efforts so that when disaster does strike, the impacts are minimized for our member owners and the local communities in which they reside. Knowing what to do, who to call and how to proceed is imperative and requires coordinated efforts in the public and the private sectors.

Claverack Rural Electric Cooperative delivers electricity to member owners in northeastern Pennsylvania. Our primary service territory includes Bradford, Susquehanna and Wyoming counties, with additional members in the bordering counties of Lackawanna, Luzerne Sullivan, Tioga and Lycoming. We provide electric service to 18,693 active accounts. Incorporated in 1936, Claverack is headquartered in Wysox, PA, and maintains district offices in Susquehanna and Wyoming counties. We serve primarily residential members and average less than six consumers per mile of line. Our electric distribution system includes 20 substations and 2,784 miles of electric distribution lines. We receive service from Penelec's (a First Energy company) sub-transmission system at 34.5 KV and distribute electricity to our consumer members via our 12.47 KV distribution system.

Claverack is governed by a board of 9 directors who are elected by the membership of the cooperative. Electric cooperatives are private, independent electric utilities, owned by the members they serve. Democratically governed businesses, electric cooperatives are organized under the International Co-operative Alliance or Rochdale Principles, anchoring them firmly in the communities they serve and ensuring that they are closely regulated by their consumers. Cooperatives are governed by a board of directors, which sets policies and procedures that are implemented by the cooperatives' professional staff.

Claverack is a member of the National Rural Electric Cooperative Association (NRECA), the service organization dedicated to representing the national interests of cooperative electric utilities and the consumers they serve. NRECA represents more than 900 not-for-profit consumer-owned rural electric utilities that provide electric energy to over 42 million people in 47 states or 12 percent of electric customers. Electric cooperative service territory makes up 75 percent of the nation's land mass.

Because we are owned by the members we serve, electric cooperatives reflect the values of our membership, and are uniquely focused on providing reliable energy at the lowest reasonable cost. We are accountable to our owners and those same owners are the customers who depend on us to provide power in rural areas.

National Versus Local Events

Prior to discussing how our industry prepares for or responds to a loss of power, it is important to note there are differences between an event that impacts the nation or a large region

versus a local event. The North American power grid is a huge, complex machine with built in redundancy that spans the entirety of the United States, Canada and even parts of Mexico. Its function can be impacted at different levels by many different types of events or threats, from natural events like Geomagnetic Disturbances (GMDs) caused by solar or severe earth weather to man-made malicious threats like physical attacks, including electromagnetic pulses (EMPs), or cyber attacks.

Due to the expanse of the system as well as the threat environment, the electric sector addresses risk management through a defense-in-depth approach. This includes preparing for and preventing what we can, while at the same time planning for response and recovery.

Most events impacting electric power supply tend to impact a community or a region – not the bulk power system as a whole. However, planning for recovery at a national level for widespread destructive events is necessary in a world where terrorists and nation states have an eye toward harming our critical infrastructure. Existing industry efforts to enhance resiliency, such as spare and recovery transformer programs, leveraging government resources and mutual assistance networks can be applied to national or local recovery events. Efforts aimed at bolstering reserves of strategic transformers, such as the plan the Department of Energy (DOE) was instructed to draft when the FAST act (P.L. 114-94) was signed into law at the end of 2015, will be complimentary to industry-led efforts already underway to establish spare equipment programs to help in the event of a national catastrophe or an act of war against the homeland. Importantly with a national level event, while our society depends on electricity to function, our systems are reliant on other systems including transportation systems for our fuel, water systems for cooling, and telecommunications for operations. When dealing with events coordination with all these systems is imperative.

Mutual Assistance Agreements

Electric cooperatives have a unique and effective approach to emergency management and disaster recovery - following a disaster, cooperatives will rapidly deploy support staff and equipment to emergency and recovery zones to assist sister cooperatives. The national network of transmission and distribution infrastructure owned by electric cooperatives has been built to federal standards enabling line crews from any electric cooperative in America to provide emergency support, secure in their knowledge of the system's engineering.

In Pennsylvania, our cooperative statewide organization, the Pennsylvania Rural Electric Association (PREA), and the 13 Pennsylvania cooperatives coordinate mutual assistance amongst themselves first, ensuring a shared situational awareness. Mutual Assistance Agreements are a formalization of arrangements that have historically been made informally among cooperatives to help each other when disaster strikes. NRECA maintains a database where a listing of cooperatives and municipally owned systems that have signed mutual assistance agreements can be found. The vast majority of NRECA member electric cooperatives have signed the agreement.

PREA member cooperatives also have mutual assistance agreements in place with a number of municipal and investor-owned utilities. The most important of these agreements is one with the FirstEnergy companies of Jersey Central Power &Light, Metropolitan-Edison, Penelec,

and West Penn Power. Electric cooperative crews in Pennsylvania have provided assistance to the First Energy companies on several occasions.

PREA is also involved with a national emergency work plan group. This group was started by statewide cooperative organizations in Louisiana and Mississippi. Participation in this group provides Pennsylvania cooperatives direct access to representatives of cooperatives in over 20 states. PREA requests out-of-state mutual assistance and coordinates the response from Pennsylvania member cooperatives to an out-of state request for help through this group. Mutual assistance coordination calls are organized prior to and during weather events. This national network is extremely helpful during large scale events. For example, in preparation for Hurricane Sandy in 2012, electric cooperatives in Pennsylvania secured crews from Florida to assist in restoration efforts. These crews were headed north even before the storm had passed and they remained in Pennsylvania assisting with power restoration efforts. Over the years, crews from Claverack and other Pennsylvania member cooperatives have travelled to other states such as Louisiana and Ohio to provide assistance.

Public Private Partnerships/Unity of Effort

Critical infrastructure protection is a responsibility shared by the electric industry and government. The federal government, in conjunction with local and state agencies, has a law enforcement responsibility and a national security mandate. Moreover, the federal government is privy to threat information that can help industry protect critical infrastructure assets. The industry owns and operates the critical infrastructure, is expected to maintain reliable operation of that infrastructure, and has the operational expertise to do so. Receiving threat information, both classified and unclassified, enhances our ability to protect critical infrastructure.

Electric utilities have spent decades creating redundancies to enhance the security measures they have adopted, but threats to both physical and cyber security are evolving. Given these evolving threats, industry continues to work together along with federal, state, and local security and law enforcement agencies to enhance the physical security of its critical infrastructure.

At the national level, the Electricity Sub-Sector Coordinating Council (ESCC) was formed to serve as the principal policy-level liaison between the electric industry leadership and government. The ESCC is composed of 30 utility CEO's and trade association leaders representing all segments of the electricity industry – including NRECA. The ESCC works at the highest levels of the federal government to coordinate policy-level efforts to prevent, prepare for, and respond to, national-level incidents affecting critical infrastructure. These efforts include planning and exercising coordinated responses, ensuring threat information is communicated quickly to government and industry stakeholders, and deploying government technologies on utility systems that improve situational awareness of threats. The ESCC also serves an advisory role with the Electricity Information Sharing and Analysis Center (E-ISAC)

Additionally, at the local level, our statewide organization participates in annual meetings of the Pennsylvania Public Utility Commission (PA PUC) Critical Infrastructure Interdependency Working Group. This group consists of all utilities and services that would be affected should a major event occur within Pennsylvania including the Department of Homeland Security and disaster response services. The PA PUC and the Pennsylvania Emergency

Management Agency (PEMA) provide Pennsylvania cooperatives access to all state departmental group services that may be needed during a major event, such as the Pennsylvania Department of Transportation for assistance such as snow plowing and road closure information. Our Statewide also interfaces with the Pennsylvania Department of Revenue to secure travel waivers for non-IFTA (International Fuel Tax Agreement) tagged cooperative vehicles to enable their passage across state lines during certain events. This facilitates cross state mutual assistance.

Crisis Communication Lines

Electric cooperatives take the protection and security of their consumer-members' assets very seriously. One challenge has been ensuring appropriate information sharing among government and the industry prior to and during an incident.

In Pennsylvania, our statewide association's mutual assistance coordinator communicates with Pennsylvania State Agencies, such as PEMA and the PUC. During major events, the statewide requests information such as outage counts and locations from the distribution cooperatives and provides this information to the PEMA/PUC. This data, along with information from the jurisdictional Pennsylvania power companies gives the PEMA/PUC situational knowledge of a storm's impact and enables them to coordinate activities for public safety. This information is then shared by PEMA with the government as necessary and appropriate. The information that is requested from individual cooperatives includes: outage reports for PEMA use; crew counts, outage locations and estimated restoration schedules; and the need for mutual assistance as well as the availability of crews to provide assistance to other utilities.

Knowing your community

At Claverack, we work closely with our county Emergency Management coordinators. In addition to participating in events such as "table-top" emergency exercises, we remain in contact with these offices during events. We provide a map on our website that provides information about outages which is often utilized by emergency management personnel in evaluating the need for services such as emergency shelters and ice distribution within local communities. In the event the internet is unavailable for any reason we have back up plans to manually engage by phone as we did prior to the internet. We also work with local chapters of the American Red Cross, and other local human service agencies to assist our members. Social media is utilized to provide updates on outages and to issue safety reminders. We also have contacts with local radio and television stations in the event we need to broadcast information.

During Hurricane Irene and Tropical Storm Lee which swept through Pennsylvania in 2011, we were reminded of the importance of redundancy and preparedness in our 21st century communication systems. Major flooding in parts of our service territory resulted in thousands of power outages. Our headquarters building also experienced an outage in our telephone and internet service due to the loss of a river crossing by the local telephone company. We were able to use cell phones and cellular hot spots for internet connectivity. Many roads were inaccessible which would have made travel difficult or impossible for our employees to get to work. Fortunately, we have dedicated employees who remained at the cooperative in advance of the storms and many who remained at the cooperative during the course of outage restoration.

Following that event we took steps to further strengthen our communications systems. Discussions with our local phone carrier helped them to identify an alternate path to provide phone service. We have also strengthened our internet service and continue to look for back-up systems in addition to the cellular network.

Our communication systems are important in our operations. While we still use traditional radio and telephone systems, the internet and cellular networks are of increasing importance. We use traditional low band radio systems to reach our crews in the field and we use the internet to manage much of our outage coordination. The internet is also important in our flow of information to and from our members, emergency management agencies, and the general public. Though we do have back up plans in place to manage outage events without the internet, when it is functioning we utilize it to enhance our reach to the public and inform the government.

Electric cooperatives know their communities. We live and work in the neighborhoods where we serve. Our board members and our employees are personally acquainted with the fire chiefs, the township supervisors, the county commissioners and community volunteers. We leverage these relationships and our local knowledge to better serve our members. While a rural electric cooperative such as Claverack may not have the resources of a large utility, you can be sure that this sense of community and accountability along with the strength of our cooperative network will serve our rural residents well in the event of an emergency.

Planning for events

We test our business continuity and disaster recovery plans annually. Components of the plan include confirming communication channels for key contacts, reviewing our methodology for assessing the situation and determining appropriate courses of action. Our business information system vendor maintains a copy of our data which is updated every 24 hours. A copy of our database can be delivered to any site with secure internet access so that if our buildings or servers were destroyed or unavailable, we could serve our members at a remote location. We understand that cybersecurity challenges are growing daily so we must remain vigilant in order to protect our data and networks.

Staff from our information technology department have participated in Pennsylvania's Department of Homeland Security Task Force since its inception. We prioritize the protection of our cyber assets. Claverack is a small distribution utility and we are not connected to the bulk power system. Nonetheless, we follow industry best practices in protecting our operational data as well as our business and member information. Some examples include the use of technological barriers such as network firewalls and the segregation of operational and business networks. We also utilize proactive scanning, intrusion and detection programs, and network monitoring to identify security vulnerabilities. We recognize the human risk in keeping our systems safe so we require all employees to complete cyber training on an annual basis.

Utilizing the planning

Our cooperative has experienced many situations where advance planning and coordination resulted in a shorter power restoration time and a safer environment for both our crews and members. While we pride ourselves on always being prepared, because we know that emergencies can happen at any time, predicted weather events help us to put our plans into

action and learn how to improve. We saw this just a few weeks ago with a weather bulletin issued by our statewide emergency response center on a Friday afternoon advising us of the potential for high winds over the course of the weekend. Upon receipt, we doubled checked crew availability, ensured that trucks were stocked, and that we had adequate staffing at our on-call center. We also confirmed the availability of crews from our tree removal contractor and our line construction contractor who routinely perform work on systems throughout the year. These relationships are important not only to perform work in a cost effective manner but in having these additional resources available for emergency outage events. On Sunday morning, our outage map reflected over 3,000 outages spread across our entire system after a night of fierce wind. Our statewide emergency response center was already engaged, requesting outage and crew availability information from all cooperatives. At the time, we had all hands on deck assisting in the restoration and had activated our outage management team in the office to oversee the storm response. Our website outage map was continuously updated in order to keep emergency management agencies informed of our situation. With one phone call we were also able to secure additional crews from our neighboring electric cooperative.

Annually, the cooperatives in Pennsylvania are provided with an Emergency Resource guide that contains important operational information about each cooperative. This guide contains contact information, radio frequencies, information regarding system voltages, conductor types and sizes, special working conditions, special equipment & tools and spare substation transformers and moving substations. Having this information readily available helps foreign crews in understanding the characteristics of the system they are assisting plus it gives us information in the event we need to quickly secure additional equipment or transformers.

In this particular case, we were able to predict restoration within 24 hours. Therefore, there were elements of our emergency plans that we did not have to implement such as securing sleeping accommodations for outside crews, coordinating with local emergency management officials for warming shelters, or reaching out to suppliers for extra materials. Following every major event we review what worked and what we could do to improve our readiness and response in the future.

Conclusion

In closing, I thank you again for inviting me to testify. Electric cooperatives across the country learn from each experience, we learn how to protect our systems better, how to become more resilient. Serving our member-consumers we have learned how to restore power in extremely difficult circumstances. I hope that my comments have helped the Committee to understand the types of preparations that the rural electric cooperatives take in order to protect our members from power outages. I look forward to your questions.