S. HRG. 115–284

THE THREAT POSED BY ELECTROMAGNETIC PULSE AND POLICY OPTIONS TO PROTECT ENERGY INFRASTRUCTURE AND TO IMPROVE CAPABILITIES FOR ADEQUATE SYSTEM RESTORATION

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MAY 4, 2017

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
26–072 WASHINGTON : 2018

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

JOHN BARRASSO, Wyoming	MARIA CANTWELL, Washington
JAMES E. RISCH, Idaho	RON WYDEN, Oregon
MIKE LEE, Utah	BERNARD SANDERS, Vermont
JEFF FLAKE, Arizona	DEBBIE STABENOW, Michigan
STEVE DAINES, Montana	AL FRANKEN, Minnesota
CORY GARDNER, Colorado	JOE MANCHIN III, West Virginia
LAMAR ALEXANDER, Tennessee	MARTIN HEINRICH, New Mexico
JOHN HOEVEN, North Dakota	MAZIE K. HIRONO, Hawaii
BILL CASSIDY, Louisiana	ANGUS S. KING, JR., Maine
ROB PORTMAN, Ohio	TAMMY DUCKWORTH, Illinois
LUTHER STRANGE, Alabama	CATHERINE CORTEZ MASTO, Nevada

COLIN HAYES, *Staff Director*
PATRICK J. MCCORMICK III, *Chief Counsel*
ISAAC EDWARDS, *Senior Counsel*
ANGELA BECKER-DIPPMANN, *Democratic Staff Director*
SAM E. FOWLER, *Democratic Chief Counsel*
DAVID GILLERS, *Democratic Senior Council*
RICH GLICK, *Democratic General Counsel*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

THE THREAT POSED BY ELECTROMAGNETIC PULSE AND POLICY OPTIONS TO PROTECT ENERGY INFRASTRUCTURE AND TO IMPROVE CAPABILITIES FOR ADEQUATE SYSTEM RESTORATION

THURSDAY, MAY 4, 2017

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

The Committee met, pursuant to notice, at 10:09 a.m. in Room SD–366, Dirksen Senate Office Building, Hon. Lisa Murkowski, Chairman of the Committee, presiding.

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

The CHAIRMAN. Good morning. The Committee will come to order.

I would like to welcome everyone to the Energy hearing this morning. We are here to examine the threat that is posed by electromagnetic pulse, that is known as EMP, as well as policy options to protect energy infrastructure and provide for system restoration in the event of an EMP attack. The United States has recognized a potential EMP attack as a national security threat for decades and our efforts to understand a potential EMP burst are certainly not new.

The Department of Defense (DoD) and our national labs have been grappling with these issues to one degree or another since we first started testing nuclear weapons. Extensive tests in the 1950s and 60s examined the potential impact of an EMP burst on both military and civilian infrastructure. Today, however, there is a renewed focus on understanding the effects of such an attack and an increase of efforts directed at mitigating and recovering from such an event should it occur. This issue is, perhaps, more salient now than ever for several compelling reasons.

First is the proliferation of nuclear technology which is no longer limited to the U.S., Russia, China, the U.K. and France. Other nations have tested nuclear weapons and missiles to deliver them. Rogue nations, such as North Korea, may already have or be close to obtaining these capabilities. We must also be mindful of the potential for a non-state actor to obtain a nuclear device. While their ability to use a missile as a delivery vehicle for a high altitude EMP attack would likely be more limited, we know that it cannot be ruled out.

Second is the proliferation of electronics in today's society. Just about everyone in this room, I would venture to say, has a smartphone. That is just the start of the devices that we rely on, and that, in turn, rely on electricity and electronics to function. This has magnified the impact as compared to the potential impact in the 1960s that an EMP burst could now have on the electric grid, the technologies that rely on electronics and on our daily lives.

We must recognize from the start of today's discussion that the threat posed by an EMP attack is a matter of national defense. Defending our nation from a missile carrying a nuclear warhead is clearly beyond the scope of the owners and operators of energy infrastructure and their regulators. Nevertheless, these institutions do have a role in protecting critical energy infrastructure and providing for its restoration. As the owners and operators of critical energy assets, our utilities must assist government EMP experts in understanding how the electric grid works.

For its part, government must prudently share its knowledge and expertise with industry on a timely basis and approve or direct prudent, reliability standards as warranted. There really is no way around this.

On the one hand, we have defense and national security personnel who are very familiar with the effects of a nuclear detonation but who are not responsible for the complexities of keeping the lights on. And on the other hand, you have professionals in the power sector who know the grid but are not familiar with the characteristics of a nuclear detonation.

It is critical that the electric industry and government improve upon their mutual understanding and trust because it is essential to the productive relationships that are necessary to improve our ability to respond to EMP and other potential, high impact, but low frequency events.

Both camps must work together to share information and expertise. Our engineering schools and other conduits for professional expertise must embrace a new paradigm for considering and addressing security threats in the design and operation of electric systems.

Improving our ability to respond to an EMP threat is also an area where, like cybersecurity, the subject of another recent hearing that we just had, stronger public/private partnerships are needed and today's capabilities must be improved. This hearing will consider as a policy matter whether the appropriate federal agencies have the authority they need to address this potential threat and whether additional authority or direction is needed.

Back in 2005, we established authority for the North American Electric Reliability Corporation, now NERC, through an informed stakeholder process to establish, subject to the Federal Energy Regulatory Commission's (FERC) approval, mandatory, physical and cybersecurity standards for the industry. More recently, in 2015, Congress codified the Department of Energy (DOE) as the sector-specific agency for energy critical infrastructure and provided the Secretary with emergency authority to address a host of threats: cyber, physical, geomagnetic disturbances and EMP. So we have taken some steps, but many argue and believe that those steps are

not sufficient and that we still have a great deal of work in this area.

Our task today is to consider the distinct points of view about EMP brought to us this morning by our very distinguished panel. I am looking forward to the testimony we will receive from each of you.

I now turn to my Ranking Member, Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Madam Chair.

I welcome the witnesses here today and thank you for scheduling this hearing.

The electric grid is essential to our lives and also the lifeblood of our economy. With the fate of our economy dependent on access to reliable electricity, it is our responsibility to ensure that the grid is prepared to withstand many threats including natural disasters, including those caused by changes in climate, extreme weather, physical attacks of terrorism, cyberattacks, geomagnetic disturbances, electromagnetic pulse, or EMP. We must continue to identify and evaluate the threats to the system as well as appropriate investments in technology to reduce these threats.

Threats to the grid are measured both by probability and severity of impact. We must prepare and protect against all these hazards, but we must prioritize based on the likelihood of occurrence and severity of impact.

Electromagnetic pulse attacks are considered a high-impact, low-probability threat, as I think, Mr. Manning, in his testimony, indicates. We do not yet have the concrete science-based analysis necessary to understand the threat and identify effective solutions.

As a result, in 2001 Congress established a commission to assess the threat from high-altitude electromagnetic pulse, known as HEMP. In 2014, the Department of Homeland Security (DHS) developed guidelines to help federal agencies identify those options to protect critical equipment and facilities and communication and data centers from these attacks.

The Department of Energy and the Electric Power Research Institute (EPRI) are both engaged in studying the EMP threat and releasing action plans for both government and private industry.

The Departments of Homeland Security, Defense and Energy, including our national labs, are actively engaged in studying the effects of EMP and identifying proactive measures that can help mitigate against these threats.

As Mr. Manning has noted, solutions to EMP threats to the grid are not well understood. Much of the available information is not specifically applied to utilities, making it difficult for utilities and regulators to identify the options for protecting that infrastructure. So I am pleased the work is currently underway by both industry and the government to identify our options.

I also want to say that threats to our grid are measured by the likelihood of occurrence and severity and warming climate has increased physical threats to our infrastructure with rising sea levels, storm surge and extreme weather events. According to NOAA, high sea surface temperatures have contributed to a substantial in-

crease in hurricane activity in the Atlantic and the severity of those strong threats on our grid.

In 2012, Hurricane Sandy tore through the East Coast leaving a path of wreckage, rainfall, and knocked down power lines, leaving 88.5 million homes and businesses in 16 states without power.

In the State of Washington, we have seen extreme weather changes. We have had landslides, flooding and sea level rise, as well as drought, that has induced forest fires threatening our grid. In 2014, large fires in Central Washington substantially impacted the electric infrastructure with over 3,000 customers without power. I should say that the cost is how much was actually burnt up in the fire, substantive investments that had just been made by utilities in that region.

Finally, I would like to talk about the issue of cybersecurity that the Chair mentioned. While we have never experienced a high-altitude EMP attack, the severity of successful cyberattacks on our grid is growing and it is significantly more likely that our grid is being tested for cyber vulnerabilities every day by our adversaries. In fact, Russia is believed to have deployed a cyber weapon to shut down Ukraine's grid in both 2015 and 2016.

On March 14th of this year I asked the Trump Administration to protect the growing grid vulnerabilities from cyberattacks and make sure that we zero in on the appropriate assets. I sent a letter to the Administration and to the Department of Energy asking that they assess the capabilities of some of these nations, of Russians, particularly, to hack into our energy infrastructure, and I am looking forward to getting a response since it has been several weeks since we sent that letter.

It is widely known the United States is under constant threat from cyberattacks, and many cyber experts have come to the same conclusion. It is not an if, but a when, a massive attack on our grid will occur. In fact, the former Director of National Intelligence, General Clapper, stated in 2015 that cybersecurity is now more a significant threat to our national security than terrorism.

So I am glad we are holding this hearing on the risks to our grid, and EMP being one of them, but I hope that we will also make sure that we continue to focus on cybersecurity. I know we have had a hearing, and three other committees that I serve on have also had cybersecurity hearings.

I think everybody is waking up to the fact that cyber is a big issue. Obviously, Madam Chair, we passed the Energy Policy Modernization Act out of the Senate, that the House failed to act on, which had a major cybersecurity provision. So I hope our colleagues over there will wake up to the importance of that.

I look forward to hearing from our witnesses. And thank you, Madam Chair, for the hearing.

The CHAIRMAN. Thank you, Senator Cantwell.

We are joined this morning by a very distinguished panel. I welcome you all.

The panel will be led off this morning by the Honorable Cheryl LaFleur, who is the Chairman of the Federal Energy Regulatory Commission. She has been a member of the FERC since 2010. We appreciate all that you do on that very important commission. We

would like to get you a quorum so that you can be working every day, but we are pleased that you are here this morning.

Chairman LaFleur will be followed by a man who is well known up here on Capitol Hill. It is a pleasure to welcome you to the Committee. Chairman of the Board of Gingrich Productions and former Speaker of the House, Speaker Gingrich has been a leading voice on the issues and the dangers of an EMP attack. We are very pleased to have you provide your insight this morning.

Following Speaker Gingrich is Ambassador Henry Cooper. He is the former Director of the Strategic Defense Initiative Organization, and he was President Reagan's Chief Negotiator at the Geneva Defense and Space talks. It is nice to have you at the Committee this morning. Welcome.

Caitlin Durkovich is the Director at Toffler Associates. Prior to joining Toffler, she served as the Assistant Secretary for Infrastructure Protection with the Department of Homeland Security under President Obama. It is nice to have you here.

Mr. Robin Manning currently serves as the Vice President of Transmission and Distribution at the Electric Power Research Institute, EPRI, where he oversees research and development activities. We thank you for your leadership there.

The panel will be rounded out by Mr. Kevin Wailes, who serves as the CEO and Administrator of Lincoln Electric System. Mr. Wailes is also the Vice Chair of the Electricity Subsector Coordinating Council.

We are pleased to have you all here. We would ask that you try to limit your comments to five minutes. Your full statements will be included as part of the record. Commissioner LaFleur, if you would like to lead off, please.

STATEMENT OF HON. CHERYL LAFLEUR, ACTING CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION

Ms. LAFLEUR. Good morning and thank you, Chairman Murkowski, Ranking Member Cantwell and members of the Committee. I appreciate the opportunity to appear before you today to discuss electromagnetic pulse, EMP, threats to the electric grid in the United States. I very much appreciate your attention to this important issue.

The Federal Energy Regulatory Commission, FERC, plays a key role in the oversight of grid reliability. In 2005, Congress entrusted FERC with the responsibility to approve and enforce mandatory reliability standards for the nation's bulk power system. Under the statute, FERC oversees the North American Electric Reliability Corporation, NERC, in developing standards to protect the reliability and security of the grid.

In addition to our work on mandatory standards, FERC has also supported grid security through collaborative efforts with federal agencies, states, industry and stakeholders. This work is particularly well suited to revolving threats that require action more quickly than a standard can be written. And as Senator Murkowski noted, public/private communication on those threats is critical.

FERC, NERC and industry have, over the last decade, put in place a robust set of baseline standards to address a wide range of reliability issues. In recent years, we've been particularly focused

on emerging threats to grid security, including cybersecurity, physical security and the risk associated with geomagnetic disturbances.

Geomagnetic disturbances to the bulk power system can be caused in two different ways: naturally occurring geomagnetic disturbances (GMDs) from solar activity and man-made EMP events.

EMPs can be generated by devices that range from small, portable suitcase units all the way through detonation of nuclear weapons in the upper atmosphere. EMP devices can generate three distinct effects: a short, high energy burst, called E1, that can destroy electronics; a slightly longer burst that is similar to lightning termed E2; and a third effect, E3, that generates electric currents in power lines and equipment which can then damage equipment such as transformers.

In the case of GMDs, naturally occurring solar magnetic disturbances periodically disrupt the Earth's magnetic field which in turn can induce currents on the electric grid that may cause voltage instability or destroy key transformers over a large geographic area. GMD events are similar in character and effect to the final phase of EMP, E3.

I'll briefly touch this morning on some of the work FERC has done that can help address EMP.

First, FERC developed the directed, excuse me, FERC directed the development of standards on GMD that can help to mitigate the E3 effective EMP based on a 1 in 100 years' solar storm benchmark event. Second, FERC directed the development of a physical security standard, like the GMD standard now effective and in place, that can help protect against attack from small, portable EMP devices which require proximity to their intended targets. Third, FERC has supported efforts to protect the grid, the resilience of the grid, against all risks which improves its ability to respond and recover from major outage events whatever the cause.

For example, mandatory reliability standards require backup capabilities for the loss of critical assets which reduces the potential for cascading outages. FERC has also issued orders concerning grid assurance and EEIs, spare transformer equipment program, which are efforts to protect customers from prolonged outages by providing electric utilities timely access to emergency transmission equipment that otherwise would take months or longer to acquire.

As I expect we will discuss today, FERC has not to date directed NERC to develop a specific standard specifically targeting EMP. To be clear, I believe this is the result of recent consideration of the issue, not a lack of attention or willingness by FERC to address EMP threats. Although much work has been done, there remains a significant amount of scientific research and debate underway about how EMP, particularly the E1 component, affects the electric grid.

I particularly want to highlight the work being done by DOE, Los Alamos National Lab, Idaho National Lab, an amazing place I visited a couple years ago, DHS and the Electric Power Research Institute, which I believe will help improve our understanding of EMP impacts on the electric grid and more importantly, how best to target our actions to mitigate them.

FERC is closely engaged in all these efforts to understand and address the EMP threat as more fully detailed in my written testimony. Those efforts will and must continue, and I'm confident that should FERC determine that a reliability standard is warranted, it will exercise its authority to require one as it has with other threats, like GMD and physical security.

Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Ms. LaFleur follows:]

Testimony of Cheryl LaFleur
Acting Chairman, Federal Energy Regulatory Commission
Before the Committee on Energy and Natural Resources
United States Senate
May 4, 2017

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

Thank you for the opportunity to appear before you today to discuss electromagnetic pulse (EMP) threats to the electric grid in the United States. I appreciate the Committee's attention to this important issue.

The Federal Energy Regulatory Commission (FERC) plays a central role in protecting the reliability of the Nation's electric grid against a range of threats, both naturally-occurring and manmade. Our work generally takes the form of both mandatory reliability standards and voluntary, collaborative efforts with our federal and state colleagues, industry, and other stakeholders. Before turning to EMP specifically, I would like to provide an overview of the evolution of FERC's reliability work, which I believe will help inform that discussion.

FERC's Oversight of Grid Reliability

In the Energy Policy Act of 2005, Congress entrusted FERC with a new responsibility to approve and enforce mandatory reliability standards for the Nation's bulk-power system. This authority is found in section 215 of the Federal Power Act (FPA), and is limited to the "bulk-power system," as defined in the statute, which excludes Alaska and Hawaii, as well as local distribution systems.

Under FPA section 215, FERC cannot directly write or modify reliability standards but must rely on the Electric Reliability Organization (ERO) that FERC certifies to perform this task. In 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the ERO. Under the section 215 construct, NERC develops and proposes for FERC's review new or modified reliability standards. In addition, as I will discuss in more detail below, FERC may direct NERC to develop or modify a standard and has done so when FERC determines that new or modified standards are needed. Once NERC develops a standard, it is filed with FERC, at which time FERC can either approve or remand the standard. If FERC approves a proposed standard, it becomes mandatory and enforceable in the continental United States and is applicable to the users, owners and operators of the bulk-power system. If FERC remands a proposed reliability standard, it is sent back to NERC for further consideration.

In addition to its formal standards work, FERC has also supported grid security through voluntary and collaborative efforts. Largely conducted by FERC's Office of Energy Infrastructure Security, FERC has worked closely with other federal agencies, states, industry, and other stakeholders to improve coordination and knowledge-sharing regarding threats to the grid. This work includes, among other activities, the development, identification, and dissemination of best practices; participation in grid reliability exercises; and providing briefings to state colleagues.

FERC, NERC, and industry have made significant progress over the last decade to put in place a robust set of baseline standards to address basic day-to-day grid reliability issues, like tree trimming and relay setting. Reaching a steady state on those standards has allowed us to increasingly shift our attention to cutting edge or emerging threats, like cyber and physical security of critical grid infrastructure, and the risks associated with geomagnetic disturbances (GMD) from solar storms and EMP attacks. Going forward, I expect that our collective attention to these issues and the risks posed by high-impact, low-frequency events will only increase. Later in my testimony I will explain some of the work we have done to date on these issues and how it helps to provide protection against potential EMP threats.

EMP Threats

I will now turn to EMP, as well as a related discussion about the threats posed by GMD. The bulk-power system may be impacted by electromagnetic events, such as naturally-occurring GMD or man-made EMP. In the case of EMPs, equipment is available that can generate localized high-energy bursts designed to disrupt, damage or destroy electronics such as those found in control systems on the electric grid. EMPs can be generated by devices that range from small, portable, easily concealed battery-powered units all the way through missiles equipped with nuclear warheads. As described, for example, in a recent report from the Los Alamos National Laboratory, depending on the yield of the device and the altitude of its detonation, EMP devices can generate three distinct effects of varying magnitude, each impacting different types of equipment: a short, high energy Radio Frequency-type burst called E1 that can destroy electronics; a slightly longer burst that is similar to lightning, termed E2; and a final effect, termed E3, that generates electric currents in power lines and equipment, which can then damage or destroy equipment such as transformers.

In the case of GMDs, naturally occurring solar magnetic disturbances periodically disrupt the earth's magnetic field, which, in turn, can induce currents on the electric grid that may simultaneously damage or destroy key transformers over a large geographic area. GMD events are similar in character and effect to the final phase of EMP, termed E3, as they can affect the same equipment including transformers. Any of these effects has the potential to cause voltage problems and instability on the electric grid, which could lead to wide-area blackouts.

The risks posed by EMP and GMD events have been the subject of significant scientific research and debate, as well as broad discussion among regulators, elected officials, industry, and other stakeholders about the appropriate steps to address these threats. FERC has been actively involved in these discussions, and the threats posed to the grid by electromagnetic events, particularly GMD, have been a particular priority of mine during my time at FERC. While the threats posed by GMD and EMP overlap in part, our understanding of those threats and how to effectively mitigate them has led to different approaches to address them.

With these issues and challenges in mind, FERC has used both regulatory and more informal collaborative approaches to address EMP threats.

FERC Regulatory Actions

First, with respect to regulatory actions, FERC has acted through both its reliability authority under FPA section 215 and its ratemaking authority under FPA section 205 to support grid reliability efforts that help protect against EMP threats.

Through its work on GMD, FERC has taken steps that help to mitigate one aspect of EMPs, i.e., the effect of the E3 component on high-voltage transformers and other equipment. In 2013, FERC directed NERC to develop GMD reliability standards in a two-stage process. The first stage GMD reliability standard, which has been in effect since 2015, requires responsible entities to develop and implement operational procedures to mitigate the effects of GMDs. The second stage GMD reliability standard, which FERC approved in 2016, requires responsible entities to conduct initial and on-going assessments of the potential impact of a benchmark GMD event on bulk-power system equipment and the bulk-power system as a whole and to mitigate any assessed vulnerabilities. With respect to the second stage GMD reliability standard, FERC also directed NERC to develop modifications and perform additional GMD research on specific issues to ensure that the protections against GMD evolve with our improving understanding of the science.

FERC has also taken other actions that provide a measure of protection against EMP threats, particularly through its efforts to protect the grid against physical threats. The nature of physical attacks – which, like EMP events, are intentional, manmade efforts to disrupt the electric grid – introduce additional complexities not present in events that have caused wide-spread blackouts and reliability failures in the past, such as vegetation-related events. Recognizing these risks, in 2014, FERC directed NERC to develop a reliability standard that addresses physical security threats. FERC approved NERC's proposed physical security reliability standard later that year. The physical security reliability standard requires responsible entities to

mitigate assessed vulnerabilities to critical transmission facilities through resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities. This standard, insofar as responsible entities harden their substations and improve perimeter security to address their assessed vulnerabilities, can help address the use of small, portable EMP devices that require close proximity to their intended targets.

FERC, NERC, and industry have also dedicated significant attention to improving grid resilience. Resilience efforts cover a range of actions that grid owners and operators can take to reduce the risks associated with the loss of individual or multiple assets and to improve recovery and restoration following such losses. FERC has supported efforts to improve the design, planning, maintenance, and operation of the grid through its standards and rate work, as well as through collaborative efforts. For example, some of these efforts stem from requirements in mandatory reliability standards to ensure backup capabilities for the loss of critical assets, or to de-risk critical assets, which reduces the potential for cascading outages.

One important element of grid resilience is ensuring adequate inventories of critical grid infrastructure, particularly long-lead time construction items like high-voltage transformers. Through its rate-making authority, FERC has issued orders to provide clarity on how it will address services provided by Grid Assurance, a company created by several electric utilities and energy companies, and Edison Electric Institute's (EEI) STEP program. Over the last two years, FERC issued orders addressing important cost recovery and rate design questions concerning Grid Assurance's service model, which is intended to support transmission owners in the procurement, maintenance, and delivery of transformers and related equipment in the event of a loss of a critical transformer. Similarly, EEI's STEP program, which FERC approved in 2006, provides a sharing service for backup or spare transformers among participating transmission owners. These programs are intended to enhance grid resilience and protect customers from prolonged outages by providing electric utilities with timely access to emergency spare transmission equipment that otherwise can take months or longer to acquire.

As noted above, the GMD and physical security standards help provide protection against particular aspects of the EMP threat. However, FERC has not directed NERC to develop a standard specifically targeting EMP. To be clear, I believe this is the result of reasoned consideration of the issue. FERC has repeatedly demonstrated a willingness to direct NERC to develop or modify a reliability standard where FERC identifies a gap in the protection of the bulk-power system; indeed, the physical security and GMD standards, as well as an ongoing effort to develop a standard to address supply chain threats, were the result of FERC directives. It is also worth noting that directives to develop new standards have been supported by FERC commissioners from both parties, demonstrating a strong bipartisan commitment to

grid reliability.

I recognize that some parties have challenged FERC's decision to proceed with a GMD standard that did not also include EMP threats more generally. I believe that FERC's approach has been prudent, given our understanding of those threats and potential mitigation to address them. With GMD, FERC was able to identify and direct a structured plan of monitoring, assessment, and mitigation that targets specific critical grid components (e.g., high voltage transformers) for protection against a GMD event. That plan was the result of years of FERC, NERC, and industry efforts to understand the GMD threat and determine how best to protect against it.

By comparison, large-scale EMP attacks pose a very different threat to the grid, and one that, to date, FERC has not determined is well-suited to a mandatory reliability standard at this time. Although much work has been done, there remains a significant amount of scientific research and debate underway about EMP threats. For example, in January 2017, DOE, in its role as the Sector-Specific Agency for the Energy Sector, issued its Electromagnetic Pulse Resilience Action Plan, which lays out a multi-year effort to improve our understanding of EMP threats, effects, and impacts; identify priority infrastructure; test and promote mitigation and protection approaches; enhance response and recovery capabilities; and share best practices. DOE, through the Los Alamos National Laboratory, is working with the Department of Homeland Security (DHS) to advance our understanding of EMP's effects on the electric power system. DOE's Idaho National Laboratory is also working to develop potential EMP strategies, protections, and mitigation for the electric grid. Similarly, the Electric Power Research Institute is currently conducting a multi-stage study of grid impacts associated with EMP threats, including evaluations of the impacts of E-1, E-2, and E-3 components.

In addition, last year, Congress directed DHS to conduct research and development on how to mitigate the consequences of threats of EMP and GMD, and report periodically over several years. A year earlier, Congress also re-authorized the EMP Commission, initially created in 2001, to continue to assess and report on the threats posed by EMP.

EMP threats present unique challenges as well. Unlike naturally-occurring GMD, which can be measured and subject to rigorous public scientific debate, EMP threats stem from hostile actors, particularly foreign nations, which introduces complexities regarding confidential national security information that are not readily adapted to FERC proceedings or the NERC standards development process. Any standard we may adopt in the future may need to differ from our usual standards, in order to avoid the security risk of announcing publicly the limits of our protective mitigation.

Furthermore, while there has been much written regarding the nature of the threat from EMP, consensus has not been reached regarding how best to protect against it. While the military has developed protocols to protect key assets, these protocols have been described by Los Alamos National Laboratory as "not widely implemented in civilian applications due to the expense," and by Idaho National Laboratory as "focused on load center protection for communication stations, control and mission critical facilities, not distribution, transmission and large generation assets for the electric power grid." Given the scope and potential cost of an effort to protect the entire grid against an EMP attack, I think it is prudent that FERC not launch a mandatory standard unless it concludes that the standard would effectively mitigate the threat at a justifiable cost. Ongoing research by DHS, DOE, and others eventually may support such a conclusion, but to date, FERC has not reached that conclusion.

That said, as described below, FERC remains actively engaged in efforts to understand and address the EMP threat. Those efforts will continue, and I am confident that, should FERC ultimately determine that a reliability standard is warranted, it will exercise its authority under FPA section 215 to require one.

Collaborative Efforts

FERC is also actively involved in efforts beyond its standards process. As noted above, FERC works closely with Federal agencies, state partners, and industry to identify key energy facilities; provide threat briefings, including on GMD and EMP threats; assist with the development and identification of best practices for mitigation; and cooperate with international partners to convey threat and mitigation information, as well as encourage adoption of best practices for mitigation. DOE, DHS, and the Department of Defense (DOD) have been particularly active on EMP issues, with DOE engaging the national labs to help support its efforts. In this regard, in 2015 I had the opportunity to visit the Idaho National Laboratory for a couple of days to learn about its work on cybersecurity and GMD issues.

Many of FERC's collaborative actions involve cross-sector, interagency, and public-private efforts to improve our collective understanding of GMD and EMP threats. For example, FERC participates in DOE's Electric Sector Coordinating Council, which is evaluating both EMP and GMD threats. In 2010 FERC, DHS, and DOE released a report conducted by the Oak Ridge National Laboratory that investigated and identified the effects of, and mitigation measures for, both GMD and EMP on the Nation's power grid. FERC is an active participant with the Energy Infrastructure Security Council, assisting with national and international collaboration. These efforts include the publication of resources in collaboration with DOE and participation in state and national table-top exercises simulating EMP attacks and coordinated responses as well as potential proactive protection measures.

FERC continues to monitor international efforts to address EMP and GMD, including collaborating on both foundational and best practices. In 2016, FERC exchanged information with Norway and expects to do so with both the UK and Israel later this year. On a national level, FERC briefed the EMP Commission earlier this year and has offered further collaboration to DHS, DOE, DOD, the national laboratories, and industry.

In addition, in November 2014, the National Science and Technology Council created the Space Weather Operations, Research, and Mitigation (SWORM) Task Force to develop high-level strategic goals for enhancing national preparedness for a severe space weather event. The SWORM Task Force is co-chaired by members from the Office of Science and Technology Policy, DHS, and the National Oceanic and Atmospheric Administration. FERC has participated in the SWORM Task Force's efforts from its inception. As a result of this work, FERC was an active participant with the development and release of both the National Space Weather Strategy and the National Space Weather Action Plan. FERC also assisted with the follow-up Executive Order released in October 2016 that, among other things, directed DOE and DHS to "develop a plan to test and evaluate available devices that mitigate the effects of geomagnetic disturbances on the electrical power grid through the development of a pilot program that deploys such devices." FERC has offered further assistance to DOE should this work proceed.

Most recently, FERC has assisted both DOE and DOD to identify defense-related critical electric infrastructure as directed under the FAST Act, thereby assisting with their decisions regarding EMP and GMD protection at these facilities. Further, in response to a directive of the FAST Act, DOE, after consulting with FERC and others, submitted a Strategic Transformer Reserve report to Congress in March 2017. This report described the importance of maintaining a strategic transformer reserve, as well as the current efforts underway by the industry and government to mitigate potential threats to the U.S. bulk-power system created by the vulnerabilities of these transformers. Specific to the subject of today's hearing, these threats include both EMP and GMD events. DOE recommends encouraging and supporting an industry strategic transformer reserve driven by voluntary industry actions and NERC's physical security reliability standard's requirements. DOE also recommends that it re-assess this approach in the future with FERC and electricity industry partners to determine whether sufficient progress has been made through this approach or if alternative actions by the government might be necessary. As noted above, FERC has encouraged these efforts through its collaborative outreach and ratemaking authority.

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

The CHAIRMAN. Thank you, Chairman LaFleur.
Speaker Gingrich, welcome.

STATEMENT OF HON. NEWT GINGRICH, CHAIRMAN OF THE BOARD, GINGRICH PRODUCTIONS

Mr. GINGRICH. Thank you very much for holding this hearing. I think it's very important and I commend the Chair and the members for putting time in on this.

I just want to focus backward from consequence.

A good friend of mine and co-author of several novels, Bill Forstchen, wrote a novel called, "One Second After," which is the study of a small town in North Carolina during the year after electricity was knocked out by an EMP attack. And it's really worth looking at because we take electricity for granted. Even in relatively short outages as we had in April in New York, San Francisco and Los Angeles, people are remarkably inconvenienced.

But it turns out, for example, all the drugs we rely on for a wide range of things require refrigeration. And the minute you start knocking out the system, there's a cascade of consequences.

We've known indirectly since 1859 with the Carrington event that something can happen that has an effect back then and knocked out telegraph lines but we weren't relying on everything that's electronic that we do today.

We've known since 1962 that there can be a manmade event at a high altitude which knocks out electricity because it knocked from Johnston Island, it knocked out lights in Honolulu.

The challenge we have with the electric grid is it's actually designed for efficiency and it's a remarkable achievement. The problem is efficiency, it leads to fragility. And so, from your perspective, you both have to look at notable points which could be knocked out physically or by a local EMP. You have to then look at cyberattacks, and then you have to look at EMP attacks.

The grid is vulnerable at all three layers. And if somebody were to methodically come in here, they would find, I think, there are as few as nine notable points you could knock out that would have a catastrophic effect because it would lead to a cascade of systems to shutting down.

If you then looked at the effect, potentially, of either the series of local EMP attacks or a high-altitude EMP attack, you're talking about a catastrophic event from which, conceivably, you couldn't recover for years.

So, I would—a couple of quick things. One, the Congress should look at EMP attacks as one of the three great threats to our survival. The other two being cyber warfare and nuclear weapons, and they should regard all three as catastrophic. For us to survive as a civilization we have to be able to defeat all three of those threats. Two, I think that the Congress should communicate a sense of urgency. There are a lot of people doing a lot of good things at a relatively leisurely pace and trying to be reasonable. If you work back from consequence, you rapidly become unreasonable because the consequences are so horrible. This is like 9/11 where we said, gee, we hadn't thought about an airplane hitting a building which is nonsense. Tom Clancy had written about it a decade earlier, but nobody wanted to cut through and say so, what would you have to

do to stop that from happening? After the event, we did all sorts of things to make it harder to take over an airplane. We're in the same boat right now except here we're gambling on our civilization. This is vastly bigger than 9/11.

I would suggest a couple things. One, that Homeland Security and Department of Energy should have some very rigorous war games thinking through all the permutations of what could happen and they should look for the key notable points where you could, in fact, begin to fix the system because there are a number of steps that are going to be taken to make the system more resilient and to make it more difficult to take out. Two, I would look at the new infrastructure bill to consider having a substantial part of the national security infrastructure component. Three, if you were to go through and cut out a lot of the red tape that the electric industry has to deal with, the time value of money you would save would probably more than pay for everything you're going to ask them to do on EMP.

And so, there are very practical things that can be done here but you need to somehow communicate to the Executive Branch, you need a sense of urgency. We need to understand that every morning we get up, we're a step away from catastrophe.

And let me just note that the NASA has estimated that the potential for the sun to hit us with a, it's different than a man-made, but nonetheless equally dangerous, the potential for the sun to hit us with the, effective of the Carrington effect is about 12 percent per decade. That we're now overdue for that happening. We apparently came within one week of it happening and happened to be out of position for the sun so the solar flare missed us. But that should give us a reminder.

I'll just close by saying there's a historium. Work back from the consequences. When you have a high likelihood that over the next 20 to 30 years something this consequential is going to happen, there has to be a sense of urgency by blocking it from occurring because if it does occur, it could literally end civilization as we know it.

[The prepared statement of Mr. Gingrich follows:]

Hearing to examine the threat posed by electromagnetic pulse and policy options to protect energy infrastructure and to improve capabilities for adequate system restoration

10 a.m., May 4, 2017
Dirksen Senate Office Building
Room 366

Speaker Gingrich:

Good morning, I'd like to thank Chairman Murkowski, Ranking Member Cantwell, and the committee members for inviting me to testify today about the very real danger that electromagnetic pulse poses to the United States.

I wrote about this danger in my book *To Save America* in 2011.

Then, I acknowledged that we have known about the threat of electromagnetic pulse (EMP) since the mid-twentieth century. We learned then that setting off a nuclear explosion in the right way, and at the right altitude could simulate an enormous lightning strike, which could damage electronic devices and render them inoperable. Writing that book, I learned that testing hydrogen bombs in the Pacific resulted in burning out lights in Honolulu, which was 1,200 miles away from the test site.

As I wrote in 2011, anyone who has ever had a household appliance ruined by a power surge can understand the danger of EMPs, but our military has not fully assessed how an EMP strike could impact people in cities across the United States – and especially along the East Coast.

In 2004, Congressman Roscoe Bartlett called together a panel of nuclear physicists to study this issue. And according to their report, one EMP weapon detonated over Omaha would cripple half the economy. Further, they found that Russia, China and North Korea were working to develop EMP weapons – and the United States was quite vulnerable to an EMP attack.

Bill Forstchen, a friend who has co-authored books with me, wrote a sobering and horrifying novel about an EMP attack on the United States. The book is called *One Second After*, and in it Forstchen described how a small North Carolina town would be affected over the course of a year after a successful EMP attack. The story really illustrates how terrible such an assault could be.

As I argued in *To Save America*, within the next decade, there is no question that the United State should take action to develop a hardened, more resilient electrical system that could better withstand an EMP attack. Frankly, it is a matter of national survival.

The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack reported in 2008 that, "the electromagnetic pulse generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences."

The report went on to say: "Because of the ubiquitous dependence of U.S. society on the electrical power system, its vulnerability to an EMP attack, coupled with the EMP's particular damage mechanisms, creates the possibility of long-term, catastrophic consequences. The implicit invitation to take advantage of this vulnerability, when coupled with increasing proliferation of nuclear weapons and their delivery systems, is a serious concern. A single EMP attack may seriously degrade or shut down a large part of the electric power grid in the geographic area of EMP exposure effectively instantaneously. There is also a possibility of functional collapse of grids beyond the exposed area, as electrical effects propagate from one region to another."

Just consider if one of these pulses were to be unleashed and disabled the power infrastructure on the East Coast. This is not simply about the lights going out. Consider the consequences of hospitals and

public safety agencies being without power, communication, or transportation for a significant amount of time.

This is a topic I am incredibly concerned – and passionate – about. I look forward to speaking with you about it today.

The CHAIRMAN. Speaker, thank you very much for your comments and reminding us of the imperative here.

Ambassador Cooper, welcome.

STATEMENT OF AMBASSADOR HENRY F. COOPER, FORMER DIRECTOR, STRATEGIC DEFENSE INITIATIVE ORGANIZATION

Ambassador COOPER. Madam Chairman, Ranking Member and members, I very much appreciate the opportunity to testify before you today on my views of this important issue.

Actually, Speaker Gingrich has covered a lot of my material which is a good thing because I wasn't sure I could get through even my abbreviated comments here.

I guess I would like to say that I add that we're living through the most dangerous period of my lifetime for a number of reasons, but the vulnerability of our national electric power grid is among the most important and we are collectively continuing to endure or to take ineffective countermeasures to deal with it.

Frankly, I've become so concerned about the dysfunctionality of the Federal Government, both the Executive and the Legislative branches, that I am now spending most of my time working with private citizens, local and state authorities and happily, some key people in the electric power industry to begin working this problem from the bottom up believing that if enough of our citizens gain a real understanding of the issues and how they can actually turn—must be addressed at the local level then Washington eventually will begin to do the right thing in addressing this urgent problem.

I went through another set of issues in my summary comments here that have largely been covered already that I want to skip over and turn to the comments written by the Chairman of the EMP Commission which was chartered, as you know, by the Congress to deal with these issues, in a letter April 20th, to Secretary of Energy Perry. The EMP Commission, and these are their comments, I want to make clear. I share their views for a lot of reasons, but these are their comments. They view the current efforts to address natural EMP threat are "producing grossly inadequate standards for protecting the grid," to quote its Chairman, Bill Graham, who is a colleague of mine for many years. He further noted the Commission's concern over misleading and erroneous studies by NERC and others that grossly underestimate the natural EMP threat from solar storms and dangerously have become the basis for grossly inadequate standards approved by FERC.

Perhaps more importantly he noted the Commission's concern that the 2014 Obama Administration Intelligence Community Assessment of the nuclear EMP threat is profoundly erroneous and perhaps the worst ever produced on EMP, and that has been used to thwart efforts to protect the nation against nuclear EMP by dismissing the threat, despite overwhelming evidence to the contrary.

He also noted that the nuclear EMP is the ultimate cyber weapon threat and its military—in the military plans of Russia, China, North Korea and Iran for combined arms cyber warfare that they will see decisive new revolution in military affairs as a consequence.

He indicated to Secretary Perez and Perry that the Commission is also very concerned over misleading and erroneous studies re-

cently completed by industries, Electric Power Research Institute and grossly underestimate the nuclear EMP threat.

These and other bureaucratic issues led me, a couple of years ago, to lose confidence that we were ever going to deal with this problem from the top down, and I decided to try to work it from the bottom up.

My written testimony goes into some detail discussing the work I am doing, along with Duke Energy engineers. Duke Energy, as you probably know, is among the largest, if not the largest, energy company in the nation. And we were working on a pilot study in York County and Gaston in South Carolina and Gaston County in North Carolina. And of course, Duke's corporate headquarters are in Mecklenburg County which is a neighbor to those two counties. We are engaging with local authorities, particularly the folks in Rock Hill which is a bedroom community for Charlotte as well as an important area of its own.

This is important because the nature of the grid is, I'm sure this Committee knows, a crazy quilt patchwork of co-ops and electric utility companies across the nation, some, I don't know, 2,000 or 3,000, I understand. Unless those folks are actively involved in working the problem and providing the loading conditions that they can and will need at Duke Energy to produce the power and get it to the local subscribers, then we're going to have the consequence that the Speaker referred to earlier.

Water and waste water is a key matter, for example. Duke Energy doesn't provide the electricity to the water and waste water operations in Rock Hill. That's provided by a different utility. And unless that utility is working hand-in-hand with Duke, then you're going to have hospitals running out of electricity very shortly and, as I understand it, without water those hospitals will be experiencing deaths within hours.

So this is an important issue. I urge you to have the EMP Commission which, in my view, is the nation's top authorities. Many of the engineers were involved in the DoD from the earliest of days dealing with this issue, and that is where the expertise originally has been. The DoD is not particularly helpful in working this problem today.

The Department of Energy, while I have great respect for the engineers at our laboratories, is reinventing lessons that were learned the better part of a half century ago. And it's absurd, in my judgment, that we find ourselves in this situation.

I hope the Committee can help deal with the communication problems within the Executive Branch as well as help us work this problem from the bottom up.

Thank you, Madam Chairman.

[The prepared statement of Ambassador Cooper follows:]

ON PROTECTING THE ELECTRIC POWER GRID

Testimony of Ambassador Henry F. Cooper

To

The U.S. Senate Committee on Energy and Natural Resources:

May 4, 2017 Hearing to examine the threat posed by electromagnetic pulse (EMP) and policy options to protect energy infrastructure and to improve capabilities for adequate system restoration.

Madam Chairman, thank you for this opportunity to share my views on the need to address the fragilities of the electric power grid and the means to do so. I view that the related current status and plans known to me leave the grid vulnerable to existential threats. And I believe we have the technical means to rectify these vulnerabilities—but are regrettably blocked from doing so, primarily because of political conditions that this Committee can, and hopefully will, address[1].

I consider that we are living in the most dangerous period of my lifetime for a number of reasons, but the vulnerability of our national electric power grid is among the most important ones. Moreover, I believe we have had clear warning of the nature of this threat for years, and are collectively continuing to ignore and/or take ineffective countermeasures to deal with it. Frankly, I have become so concerned about the dysfunctionality of the federal government in dealing with the threat that I am now spending whatever remaining time the Good Lord gives me to work with local and state authorities and private citizens to address the key issues from the "bottom up"—and I will address one of these important initiatives. If enough of our citizens gain an understanding of the issues and how they can—actually must—be addressed at the local level, then I believe Washington will eventually do its part in addressing this urgent problem.

The following sections briefly review some important lessons from recent events and their implications for understanding the various threats to the electric grid, including from natural and manmade EMP; the nature of this so far poorly addressed existential EMP threat; the maturing related threat posed by hostile adversaries and our thus far inept response; and recommended initiatives to counter that threat and protect the grid.

IMPORTANT LESSONS FROM RECENT EVENTS

To set the stage for discussing EMP issues, please consider the fragility/vulnerability of the electric grid illustrated by the events of Friday just three weeks ago (April 21st) when nearly concurrent grid outages occurred in New York City, in Los Angeles and particularly in San Francisco where, for hours, there was consequent jammed traffic, people stranded in elevators, hospitals on backup generators and other disruptions that continued for several hours before emergency management operations restored electric power[2].

---

[1] Please permit me to tell you why I believe you should consider my views on this important—and I believe—urgent matter. I am a PhD engineer, with very pertinent experience—from working on developing military and civilian systems at Bell Telephone Laboratories in the early 1960s, to over 20 years conducting research and developing simulators to test our strategic systems against nuclear weapons effects, to overseeing the Research, Development and Acquisition of U.S. Air Force Strategic and Space Systems under Presidents Carter and Reagan, to backstopping our bilateral negotiations with the Soviet Union while developing our national space arms control policy and serving as Chief U.S. Defense and Space Negotiator with the Soviet Union under President Reagan, as Strategic Defense Initiative (SDI) Director and Acquisition Executive for all our missile defense programs under President George H.W. Bush, and for 15 years as Chairman of the Board of Directors of a successful R&D company. In short, I've been around and solving technical and political problems of concern for essentially my entire professional career.

[2] See a Reuters review of these events at http://www.reuters.com/article/us-usa-sanfrancisco-power-idUSKBN17N27T

Joseph Weiss, an international authority on cybersecurity, control systems and system security regularly gives his views at http://www.controlglobal.com/blogs/unfettered/ . On April 24, he noted San Francisco's 7-hour outage was due to cascading effects triggered by a single breaker in one allegedly low-impact substation, the Larkin Street Substation. Weiss noted problems at this Larkin substation were identified years ago, but authorities have not taken remedial action. On April 28, he noted some root causes, like "thermally overloaded transmission lines" were well known years in advance and that this "home town" event should raise red flags at the Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) and the need for substantial improvements[3].

Indeed! This regulatory system is failing to protect the nation's electric grid from many threats, including EMP.

IMPORTANT IMPLICATIONS FOR THREATS TO THE GRID

From my perspective, Weiss' most important observation is that the major San Francisco grid failures cascaded from a single relatively "minor" event: A lowly breaker failure in a single substation, however caused[4]. This observation brings to mind conclusions by former FERC Chairman Jon Wellinghoff following the April 16, 2013 San Jose's Metcalf Substation attack that similar cascading failures from only nine identifiable substations could bring down the entire electric grid for an extended period[5]. But the Larkin Substation was enclosed in a structure that would have shown evidence of Metcalf kind of terrorist attack with rifle fire—not evidenced in San Francisco three weeks ago. Maybe terrorists with radio-frequency (RF) weapons could have triggered such a failure, but as Weiss pointedly wrote: "Given the walled enclosure, a physical attack such as the rifle attack against the PG&E Metcalf substation would not be possible."

Moreover, while simultaneous terrorist and cyberattacks could have been planned to occur across the nation[6], the concurrent events in cities on both the East and West Coasts more likely reflect the April 21 (updated on April 22) warning by *The Sun* (a United Kingdom News Company) that "a mega hole in the Sun could cause blackout mayhem" due to its "belching" of radioactive particles toward the Earth[7]. Thus, such "space weather" effects are understood and were anticipated.

NATURAL AND MANMADE EMP

Such "Solar Hole" events are longer lasting but much less damaging than would be a Coronal Mass Ejection (CME) like in the 1859 Carrington event that interacted with the earth's geomagnetic field

---

[3] For more information, see http://www.controlglobal.com/blogs/unfettered/additional-information-concerning-the-april-21st-san-francisco-outage/ for Weise's April 28 message which includes a link to his April 24 message.

[4] Notably, Weiss told me this breaker failure brought to mind the 2007Aurora cyberattack demonstration conducted by Idaho National Laboratories that caused catastrophic damage to a generator associated with a nuclear plant, by commanding breakers out of phase with the grid's operating frequency. I do not believe this vulnerability has been rectified at all our nuclear plants—a very significant possibility if true, given their importance as discussed later.

[5] See the *Wall Street Journal* reports on this important matter at https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879?tesla=y and https://www.wsj.com/articles/u-s-risks-national-blackout-from-small-scale-attack-1394664965?tesla=y .

[6] See http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf for a pertinent February 2017 Defense Science Board report, prefaced by the Chairman's conclusion: "The cyber threat to U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries."

[7] See https://www.thesun.co.uk/tech/3379806/solar-flare-spewing-from-mega-hole-in-the-sun-could-cause-blackout-mayhem-next-week/.

to produce a Geomagnetic Disturbance (GMD) that destroyed telegraph lines, with little impact on that low-tech agrarian society. Today, a Carrington-class CME/GMD would cause catastrophic damage to critical electronic infrastructure, particularly our unprotected electric power grid. We missed such an event by a week in 2012, as explained by NASA and other scientists[8] who study "Space Weather," or "natural" EMP. They project a 12-percent-per-decade likelihood for a Carrington CME/GMD.

While current efforts (however meritorious—see below) seek to protect the grid against such natural EMP events, little to nothing is being done to protect the grid against much more stressful "manmade" EMP, caused by nuclear weapons detonated high in or above the Earth's atmosphere.

Notably, if the grid is protected from manmade EMP attack, it will be protected from Natural EMP events—but the converse is not true, because of fundamental differences in the EMP pulses. Missing in the Natural EMP pulse are the high frequency components that threaten solid state electronics, like the supervisory control and data acquisition (SCADA) systems that control much of our critical infrastructure, including our electric grids and natural gas and petroleum pipelines.

OUR ENEMIES PLAN EMP ATTACKS—A RAPIDLY MATURING THREAT

Such manmade EMP attacks are known to be included in the doctrine and planning of Russia, China, North Korea and Iran. One particularly important report on Iranian doctrine and strategy was referenced by Rep. Trent Franks at the July 21, 2015 International Electric Infrastructure Security (EIS) Summit in Washington, DC[9]. He stated that the conclusion of this doctrine is that nuclear EMP is "an advanced and useful weapon in modern warfare."

These nations also have information on how to build low-yield "Super" EMP weapons. (It is a myth that high yield nuclear weapons are required to produce extensive and intensive EMP effects.) In 2004, the EMP Commission was advised by very senior Russian Generals, experts on nuclear EMP weapons, that this "Super" EMP knowledge had been transferred to North Korea, which would probably develop these weapons in a few years[10]. We should also assume that Iran knows whatever North Korea knows and has whatever the Mullahs wish to buy.

Thus, North Korea and Iran may now or in the foreseeable future actually have such low yield super EMP weapons—indeed, that possibility could explain North Korea's underground low-yield nuclear tests—and we should assume Iran also has that information. David Albright, an often quoted expert on these matters, estimates that North Korea already has 13-30 nuclear weapons and is capable of building 3-5 each year[11].

Both nations could deliver an EMP attack on the United States by simply detonating a nuclear weapon carried by one of their satellites as it passes over the United States—no hardened reentry vehicle or accurate guidance system is needed as would be the case for a conventional intercontinental ballistic missile (ICBM) targeted on a city or other surface target. Both nations

---

[8] See https://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm for a detailed discussion.
[9] Rep. Franks reported: "The National Intelligence University translated an Iranian military doctrine called *Passive Defense from 2010*, which emphasizes the importance of targeting critical infrastructure in warfare and references 22 times the use of EMP as a weapon to damage or disable the civilian electric grids of potential opponents. The Iranian doctrine states that nuclear and non-nuclear EMP weapons operate differently, but morally are the same.
[10] Personal Communication with Dr. William R. Graham, EMP Commission Chairman.
[11] See David Albright, "North Korea's Nuclear Capabilities: A Fresh Look," *Institute for Science and International Security*, April 28, 2017 at http://isis-online.org/isis-reports/detail/north-koreas-nuclear-capabilities-a-fresh-look

have launched such satellites—Iran successfully placed satellites in orbit in 2009, 2011, 2012 and 2015 but had a failure in 2016 and plans more attempts[12]; and North Korea, after several failed attempts, in 2012 and 2016[13].

These satellites were launched over the South Polar regions to approach the United States, from our mostly undefended South. The test launches generally are reported to be of concern because they could be a stepping stone to developing ICBMs—as is certainly the case. However, they also could be intended to develop a means to carry out an EMP attack on their first passage from the South over the United States[14]. And that is why that possibility should not continue to be ignored, especially since we have little if any defense against that possibility[15].

Moreover, the 2008 EMP Commission report[16] noted that Iran had in the late 1990s launched a ballistic missile from a barge in the Caspian Sea, and sent electronic signals that suggested it "triggered" a simulated a nuclear weapon detonation at altitudes up to 400 kilometers, to produce a potentially devastating EMP. To date, the United States has not deployed a ballistic missile defense (BMD) system to counter this identified threat that could originate on a vessel off our coasts—including from the Gulf of Mexico. We are essentially defenseless against this plausible threat[17].

MISSILE DEFENSE ROLE

Our Aegis BMD ships have demonstrated an ability to shoot down such threat missile/satellite attacks—if they operate with appropriately trained crews in response to the identified threat, especially when they are near our coasts.

Aegis BMD ships do not operate in the Gulf of Mexico, but the Aegis Ashore BMD system, now operational in Romania and slated to be operational in Poland by the end of this year, could be deployed on our military bases around the Gulf to protect us from such an attack[18].

---

[12] See https://spaceflightnow.com/2015/02/02/iranian-satellite-successfully-placed-in-orbit/ and http://presstv.ir/Detail/2016/10/04/487619/Iran-Space-Agency-Mohsen-Bahrami-Sharif-Sat-Amirkabir-Nahid-I-satellite

[13] The most recent satellite http://www.space.com/31860-north-korea-satellite-launch.html was successfully placed in orbit but was subsequently reported to be "tumbling" and not transmitting signals.

[14] In February 2016, I joined Former CIA Director R. James Woolsey, Former Reagan Science Advisor (and EMP Commission Chairman) Dr. William R. Graham, Former Chairman of the National Intelligence Council Fritz Ermarth and EMP Commission Staff Director Dr. Peter Vincent Pry) to challenge underestimates of North Korea's and Iran's threat. See http://www.nationalreview.com/article/431206/iran-north-korea-nuclear-threats-are-very-real.

[15] U.S. Commander of Pacific Command Admiral Harry Harris testified last week that all nations should take the North Korean threat seriously because "North Korea's missiles point in all directions." Furthermore, Secretary of State Rex Tillerson also referred to this same fact in his Fox News interview with Bret Bair last Thursday. It would be reassuring if U.S. authorities also recognized that such missiles headed south can also deliver a devastating EMP strike by carrying a nuclear weapon payload and detonating it over us in its first orbit, rather than reentering the atmosphere to attack a American city. North Korea could plausibly accomplish this potentially existential threat attack today.

[16] The 2004 and 2008 reports of the Congressional Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, or the EMP Commission, can be found its webpage at http://www.empcommission.org/.

[17] Note that in 2013, a North Korean vessel was caught smuggling from Cuba two SA-2 rocket launchers and nuclear capable rockets (without warheads) under tons of sugar. See http://www.nbcnews.com/news/other/north-korean-ship-carrying-hidden-missile-equipment-detained-after-leaving-f6C10647045 .

[18] The Aegis BMD system, which I am proud to have originated as SDI Director, is in my opinion our most cost-effective BMD system with a very impressive test record, now deployed on 35 ships around the world and soon to be at several sites in a land based mode, including in Hawaii. It should be built on military bases around the Gulf of Mexico, beginning on Tyndall AFB in Panama City, Florida—home of 1st Air Force which has the lead mission for air defense of the continental United States, the Dominican Republic and Puerto Rico. No additional R&D is needed to protect Americans at home, just build the same Aegis Ashore system now deployed to protect our allies and overseas troops.

Congress and the President also should give our Aegis BMD ships a homeland defense mission when they are near or in our coastal waters—including while in port, e.g., at Norfolk, Virginia[19].

These BMD capabilities are technically available in the near term. I also urge that we return to the development of the most cost-effective BMD systems of the Strategic Defense Initiative (SDI) era (March 1983-January 1993)—those based in space that can intercept threat ballistic missiles beginning in their boost phase, while their rockets are still burning. We referred to this most cost-effective BMD concept as "Brilliant Pebbles." That program was cancelled abruptly in 1993 by the Clinton administration and as yet has not been revived. With the needed funding and management skills, I believe such a cost-effective system could be deployed within five or so years, now even more capable and for less money because of more advanced technology developed since 1993[20].

HARDEN THE GRID

But no defense is perfect—so we should "harden" our critical civil infrastructure, especially the electric power grid, against the full complement of threats. And it should be understood that if any adversary mounts an EMP attack against us, he will employ a preemptive combination of cyber, physical, radiofrequency and other weapon attacks to confuse and devalue our response.

As already acknowledged by the Obama administration, the grid must be hardened to protect against a GMD event that will surely one day occur, only its timing is uncertain. But as noted above, even if this hardening effort is successful (currently an unlikely prospect, based on my understanding of progress toward that end), it will not protect the grid from the manmade nuclear EMP threat—or from other threats that might be posed by terrorists or rogue regimes. Rather, we should be addressing the manmade nuclear EMP threat, together with protection against natural geomagnetic disturbances, with competently executed, integrated efforts that work the problem from the bottom up—beginning at the local level. Such efforts should also include protection against physical, cyber and radiofrequency weapon attacks.

As a prelude to my recommendations on how best to deal with this threat—which focus on protecting the grid from the bottom-up (beginning at the local level in conjunction with cooperative electric power companies (CoOps)), consider the Chairman of the EMP Commission Dr. William R. Graham's observations in his April 20 letter to Secretary of Energy Rick Perry[21]:

---

[19] A few years ago, there were usually 4-6 Aegis ships near our East Coast or in port there. If coupled with one of our relatively inexpensive TPY-2 radars appropriately placed in New England, they could supplement our Ground Based Interceptors in Alaska—especially against ICBMs from Iran, long before an additional East Coast site can be built.

[20] See http://www.nationalreview.com/article/442532/ for a *National Review* article, "How Trump can Fulfill Reagan's Defense Vision" explaining the basis for a cost-effective "rapid startup" strategy, co-authored with Retired US Army Lt General Mal O'Neill, my Deputy SDI Director (and subsequently the BMD Acquisition Executive of the Clinton administration and Assistant Army Secretary for Acquisition, Logistics and Technology); Dr. Robert L. Pfaltzgraff Jr. president of the Institute for Foreign Policy Analysis (IFPA), Inc., and Shelby Cullom Davis Professor of International Security Studies at The Fletcher School, Tufts University, and chairman of the Independent Working Group on Missile Defense, and Retired USAF Colonel Rhip Worrell who was the SDI Brilliant Pebbles Program Manager.

[21] In introducing the following list, Dr. Graham indicated the context for these observations was to explore with the Secretary of Energy how the Energy Department was going to support to the Critical Infrastructure Protection Act (FY 2017 National Defense Authorization Act, Section 1913, "EMP and GMD Planning, Research and Development, and Protection and Preparedness" p. 1762), which directed the Department of Homeland Security: to develop plans to protect the electric grid and other critical infrastructures from EMP; to educate and train federal, state and local emergency planners and first responders on the EMP threat; and to conduct research and development to mitigate EMP.

1. Nuclear EMP is the ultimate cyber weapon in the military doctrines and plans of Russia, China, North Korea and Iran for Combined Arms Cyber Warfare that they see as a decisive new Revolution in Military Affairs.
2. Protecting the grid from the worst threat—nuclear EMP attack—can also mitigate lesser threats, including from natural EMP from solar storms, non-nuclear EMP from radiofrequency weapons, cyber-attacks, physical sabotage and severe weather.
3. State electric grids can be "islanded" by installation of surge arrestors, blocking devices, Faraday cages, and other devices to protect individual states, even though they may be part of a larger regional electric grid, from a prolonged catastrophic blackout. For example, Texas State Senator Bob Hall has introduced legislation to harden the Texas Electric Grid.
4. The Commission is profoundly concerned that the 2014 Obama administration intelligence community assessment of nuclear EMP is profoundly erroneous, and perhaps the worst ever produced on EMP, and that has been used to thwart efforts to protect the nation against nuclear EMP by dismissing the threat, despite overwhelming evidence to the contrary.
5. The Commission is very concerned over misleading and erroneous studies by the NERC and others that grossly underestimate the natural EMP threat from solar storms, and dangerously, have become the basis for grossly inadequate standards for EMP/GMD protection approved by the Obama administrations' FERC.
6. The Commission is also concerned over misleading and erroneous studies recently completed by industry's Electric Power Research Institute (EPRI), in cooperation with Obama administration holdovers in the Department of Energy, that grossly underestimate the nuclear EMP threat.

Dr. Graham's observations provide a sound basis for assessing and responding to the current vulnerabilities in the management and execution of efforts to provide a viable electric power grid. The EMP Commission is the most competent and technically credible source of such advice.

Below, I will elaborate on how I am actively seeking in South and North Carolina a stepping stone to achieve his third observation, by taking Texas State Senator Bob Hall's "islanding" approach to a more fundamental level.

It is interesting that when Dr. Graham and I were junior USAF officers at the Air Force Weapons Laboratory (AFWL) at Kirtland AFB, NM conducting research on nuclear weapons effects and developing simulators to test the nation's strategic systems and their essential command, control and communications (C3) systems to assure their viability under nuclear attack, Senator Hall was also a USAF junior officer at the Space and Missile Systems Organization (SAMSO) at Norton AFB, CA—helping to harden the Minuteman ICBM system, specifically to EMP effects. Our efforts were highly classified because all our systems were vulnerable to EMP—as then recently discovered on atmospheric nuclear tests. Our EMP knowledge base remained highly classified until most were downgraded and published in the 2008 EMP Commission report—see Footnote 16.

Now we have the opportunity again to cooperate on hardening the electric power grid (and other related critical infrastructure)—and to exploit the urgency of effecting change that I believe we all feel. This includes overcoming political challenges, which are in fact more daunting than the costs of making needed improvements or technical challenges, which were solved a half century ago by the Department of Defense (DoD) and its contractors expert in protecting military systems from the effects of nuclear weapons.

POLITICAL/BUREAUCRATIC CHALLENGES

Not the least of the political challenges is associated with ineptness in the responsible DoD agencies that have blocked progress—e.g., by stalling the initial startup of the Congressionally re-established EMP Commission by almost a year and, as I understand it, continuing to inhibit its effective operation. Moreover, DoD is withholding information it learned many years ago in establishing threat EMP environmental information standards to protect our strategic systems that our nation's power companies now need to develop, deploy and maintain effective hardening designs.

So, DOE laboratories and other agencies are conducting studies to learn again, under the best of conditions, lessons mastered by DoD nearly a half century ago. Under less desirable conditions on several fronts—and without the knowledge that comes from a half century of practical experience, the current efforts can easily—perhaps predictably—run amok.

In the decades when nuclear testing was conducted, the DOE had so little interest in EMP and other nuclear weapon effects that the DoD had to pay the DOE to calculate the necessary weapon gamma ray and other outputs to allow accurate EMP analyses to be performed by the DoD. Now that the DOE and its national laboratories are searching for relevant missions, both government and private monies are going to replicate what the DoD accomplished years ago at considerable taxpayer expense. See Dr. Graham's Items 5 and 6, above.

Moreover, political/bureaucratic problems come from mission conflicts between DoD and other government departments and agencies—particularly the Department of Homeland Security (DHS). Evidence of these difficulties was graphically illustrated a couple of years ago when then Commander of Northern Command (NORTHCOM) Admiral William Gortney made clear he understood the significance of the EMP threat (See Dr. Graham's Items 1 and 4.) by supporting a major program to improve the viability of his mission to provide warning to our strategic forces and the President (costing almost a billion dollars) to harden and move key equipment from Peterson AFB to his Cheyenne Mountain command center to assure viability of that mission against EMP.

At the same time, little has been done to assure the NORTHCOM's Homeland Defense mission is viable in the face of the same EMP attack—not NORTHCOM's job to protect the nation's critical civil infrastructure except in commanding our BMD systems. Admiral Gortney indicated his was a supporting role to DHS and the Justice Department. I again call your attention to Footnote 9 and note that to my knowledge DHS has not even listed EMP among the strategic disaster scenarios against which all emergency managers (federal, state and local) are supposed to prepare[22]. See Footnote 21 that explains Dr. Graham's purpose in his letter to Secretary Perry. Unlike the previous DHS Secretary, Secretary Kelley has stated his support for addressing such EMP and related issues.

Senator Hall certainly understands many of these political challenges, since this is his second try at getting the full Texas Senate to pass needed legislation to harden the Texas Grid—and the Texas legislature meets only every other year. Other states have tried and are trying to pass legislation in various formats to protect their citizens. But so far, most of their efforts have been blocked by a lethargic regulatory, self-supervising regime and lack of leadership at the federal level—in both the legislature and executive branches. And I would add, a lack of knowledge of what needs to be done.

[22] I'd also note that NORTHCOM has refused at least two attempts known to me by the SC Adjutant General's office to permit the National Guard to include EMP in its annual Vigilant Guard exercises. So the National Guard upon which we all depend in major emergencies is unprepared to deal with EMP threats.

In 2013, the first state legislation was initiated by State Representative Andrea Boland and passed in Maine, and I understand the subsequent response has been helpful but limited—inhibited by pushback from the private sector and a lethargic response by Maine's Public Utility Commission. That public record is pertinent for others to exploit. A successful legislative example is Virginia's, which I understand is being effectively supported by Dominion Power—perhaps because Virginia's major military presence has a collective background that appreciates the EMP threat. A number of other states are also considering initiatives, and there are combined positive efforts, such as are being pursued by Ohio's American Electric Power, involving 11 states.

WHAT TO DO?

Given these political/bureaucratic difficulties (and others), I concluded several years ago that I would never see major progress in dealing with the EMP existential threat in my lifetime, especially if the current conditions remain. And I could see no prospect for meaningful improvement. So, I decided to try a different approach and work the problem from the "bottom up" . . . literally.

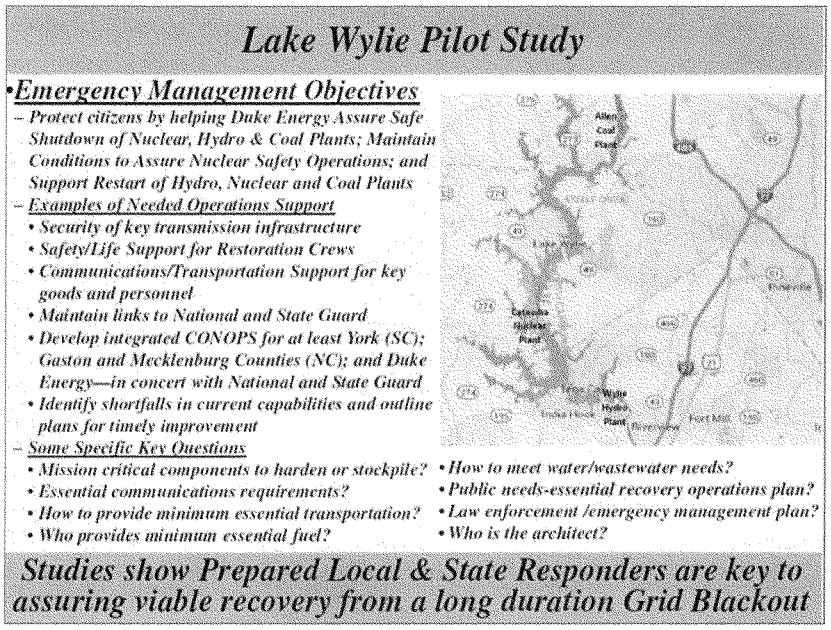
I entered this phase with several biases, based on a lifetime of pertinent experiences, which have survived to this day and which guide my assessments and recommendations.

- I have no confidence that we will ever harden the entire grid, so I believe we have to establish priorities—I give top priority to assuring the safety and viability of our ~100 nuclear power plants that produce about 20-percent of the nation's electricity, and half the electricity of my home state South Carolina. Thus, I believe our top priority is to build protected "islands" around our nuclear power plants[23].
- To assure the viability of the nuclear power plants, we must first assure their cooling water systems are viable in an indefinite grid shutdown to avoid Fukushima-like disasters.
- We must assure that sufficient generating and loading conditions provided by the surrounding "island" in the grid—and linked with other critically important elements of the grid—are available to restart the nuclear power plants—and other power plants, which will shut down to protect themselves if the grid goes down.
- I don't believe anything that isn't regularly tested and subjected to independent critical review—effective design and deployment is not enough; truly effective testing and maintenance are major challenges.
- Accomplishing these objectives requires considerable emergency management cooperation at the local level—without which there is little hope for most citizens who today depend on electricity for life-line services in our "just-in-time" economy.

I approached the Electrical Engineering Department Chairman at my alma mater, Clemson University, and requested information on faculty who might be interested in my concerns and graduates who were employed by Duke Energy—one of the nation's largest companies, if not its largest, with whom I could begin working to address the EMP threat to the grid. I want to make clear I was not selling anything to or for Duke and would not take money from them if they offered it. I just want to cut through the morass described above, and provide hope that my grandkids can survive if we experience an EMP attack. I know that all our citizens want this objective met.

[23] This "Islanding" approach to prioritizing what to harden first is similar to the approach adopted by the DoD in giving top priority to protecting our strategic systems and their supporting command, control and communications systems. This objective was central to our "deterrent" policies of the Cold War. And we hardened little military infrastructure and essentially no critical civil infrastructure beyond assuring that we could meet that objective.

To make a long story short, I developed an excellent relationship with a key professor and several Duke engineers who also are concerned about this threat—and we agreed on how we could proceed with a meaningful "bottoms-up" program to assure the viability of three Duke Energy power plants on Lake Wylie, on the Catawba River that runs between North and South Carolina—and of course key transmission infrastructure that interconnects those power plants and others to their customers. We refer to this project as the "Lake Wylie Pilot Study," briefly summarized in the following chart.



I have now been working for nearly two years with Duke Energy engineers to address how best to assure we can restart the grid after a major blackout—while giving top priority to assuring the safety and viability of our Nuclear Power Plants[24]. Duke Energy's senior management has agreed to share broadly the lessons learned from the Lake Wylie Pilot Study.

In particular, we are working with local and state authorities and citizens to help Duke engineers exploit the most resilient electric power source, the Wylie Hydroelectric Power Plant, to assure availability of electricity to the cooling water pumps at the Catawba Nuclear Power Plant, if its diesel generator fuel is exhausted and can't be replaced. (See the list of "Needed Operations

[24] Along the way, I discovered that Duke Energy was funding related research at several universities and in cooperation with other energy companies. While that research is primarily focused on the cyber threat, EMP concerns will no doubt also receive attention. Recently I learned that Duke plans to invest significant funds to modernize and protect their power systems over the next 10 years, $13 billion in North Carolina (http://www.utilitydive.com/news/duke-energy-to-harden-north-carolinas-power-system-with-13b-initiative/440524/) and $25 billion in the several states in which they have infrastructure http://www.charlotteobserver.com/news/business/article133059044.html .

Support" and "Key Questions" in the above chart.) The Allen Coal Plant in Gaston County, NC also should be available relatively quickly and has a major supply of coal to support operations.

So, at a top level, the key operations of the Duke infrastructure are being considered and with no question Duke Energy intends to assure its power plants are functional after an EMP attack. From my perspective, there would likely be problems with SCADAs, especially those that control natural gas and petroleum pipeline operations, so that is a remaining concern—at least to me.

We are working to assure that electricity gets restored to subscribers around the Lake Wylie "Island" in the grid, especially high priority subscribers like the water-wastewater operations that are not served directly by Duke Energy infrastructure[25]. That service is provided by other utility companies and Electric Cooperatives (CoOps) that maintain important grid infrastructure between Duke Energy, from whom they purchase electricity, and their subscribers. Moreover, Duke Energy engineers need information from these utility companies and CoOps if they are to exploit that set of loading conditions to enable rapid restart of their power plant operations serving the general public throughout York County and beyond.

We are progressing well toward this end—engaging with city, county and state officials to assure (at least in York County, SC and Gaston and Mecklenburg Counties, NC) that the utility companies and CoOps who buy electricity from Duke and distribute it through their own grid infrastructure to their customers/subscribers are prepared to deal with a major grid outage. We seek to assure that Duke Energy's nuclear, hydroelectric and coal power plants serve the local interests—and that the lessons learned are exploited throughout South and North Carolina—and beyond. Our effort should serve as a pattern that can be followed in integrating the activities of the several thousand electric utilities and CoOps that are key to delivering electricity to their subscribers throughout the nation.

We plan to engage with others as we progress—as previously noted, I intend to join forces with Texas Senator Bob Hall and other friends in Texas as they progress with their legislative initiative and related efforts to harden the Texas Grid and especially related to nuclear power plants and associated islands in the overall grid. I also intend to engage other states, particularly Pennsylvania and Illinois. Like South and North Carolina, they rely heavily on electricity from nuclear plants.

I also intend to work closely with the National Guard and the Adjutants General of the United States because of their key roles in disaster emergency management activities[26].

Before we began our Lake Wylie Pilot Study in earnest, my Duke Energy partner engineers got approval from their front office that the lessons learned would not be treated as "Duke Proprietary"—but could be shared with others in the electric power and related sectors. We are working with local and county officials and associated utility companies and other CoOps to

---

[25] Water-wastewater operations are perhaps the top priority, especially for urban operations. The June 2016 report by the National Infrastructure Advisory Council (NIAC) http://highfrontier.org/wp-content/uploads/2016/08/NIAC-Water-Sector-Resilience-Final-Report-Recommendations-July-2016.pdf indicates how key services are rapidly lost without water-wastewater services. For example, casualties in hospitals are expected within hours following a loss of water-wastewater support.

[26] While our SC Adjutant General—a Georgia Tech electrical engineering graduate—is on board with our Lake Wylie project, we have not yet engaged our state legislators to seek a supportive legislative initiative. However, SC State Senators and Legislators have indicated to me during the past two years that they would help sponsor such legislation when we are ready. The Duke engineers with whom I am working have cleared our project with their front office and lessons learned will be shared with all when we are ready. I understand from my Duke partners that they are fully engaged in a related NC initiative by their Lt. Governor.

understand how best to assure infrastructure connectivity to enable a Black Start following a major grid shutdown, beginning with the Lake Wylie "Island" in the grid.

South Carolina is one of the few states (joined only by Wisconsin when last I checked) focusing a statewide effort associated with NERC's November GRIDEX-IV national exercise on responding to cyber and physical attack threats. I believe the lessons learned will be helpful in extending, again from the bottom up, our Lake Wylie efforts. Therefore, we are also engaging with several other counties in this national exercise to build the relationships to share our lessons learned.

Note, there are several thousand utility companies and CoOps in the United States—so solving this important problem for that integrated "crazy quilt" distribution system is very complicated.

I have serious doubts that I will see a solution result in my lifetime from a "top-down" federal or state initiative. This is not to argue against such initiatives—which are important at least for consciousness-raising purposes. But I do worry that at best they have been proven to be very inefficient in producing serious progress in actually dealing with a truly existential threat.

I'm excited about our progress in working the problem from the bottom-up thus far—with a particular focus on assuring viable water-wastewater services to local citizens, and will be sharing more information in the future, especially with the lessons learned on how best to deal with the political issues that have for more than a decade confounded our collective progress.

My final comment is a lesson I have learned from my entire career: Effectively designing, deploying and operating any complex system requires a competent "Red Team" with access to all design, deployment and operations information, and which can challenge at the top level all efforts and report findings to the top management[27].

In my opinion, the EMP Commission should be chartered to play that role—indefinitely, and it should report directly to the President through an appropriate White House office hosting secretariat services.

Thank you for your interest and attention.

[27] During my watch as SDI Director (1990-93), I voluntarily sent several hundred million dollars from my five year budget to the Defense Special Weapons Agency (now the Defense Threat Reduction Agency) with no strings attached, except that the funds be spent to develop an independent competent assessment capability that could provide needed independent "Red Team" inputs to me (and my boss, the Secretary of Defense) on our BMD acquisition efforts. My distinct impression is that DTRA's capability and interest is a pale shadow of the DSWA's in that era a quarter century ago. I have no idea whether the key BMD systems developed under acquisition programs that I began (our ground-based interceptors in Alaska and California, our Aegis BMD system, our Patriot System or the THAAD system now being deployed in South Korea—and their associated command, control and communications systems) are confidently hardened against EMP, but without question, they certainly should be.

The CHAIRMAN. Thank you, Ambassador.
Ms. Durkovich, welcome.

STATEMENT OF CAITLIN DURKOVICH, DIRECTOR, TOFFLER ASSOCIATES

Ms. DURKOVICH. Thank you.

Good morning, Madam Chair and members of the Committee. Thank you for inviting me to testify today on protecting our energy infrastructure from the threat posed by electromagnetic pulse.

My name is Caitlin Durkovich. I had the honor of serving eight years in the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security, first as the Chief of Staff and from May of 2012 to January of 2017 as the Assistant Secretary of Infrastructure Protection. NPPD leads the national effort to protect and enhance the resilience of our nation's physical and cyber infrastructure. I transitioned from government to Toffler Associates, a future-focused strategic advisory firm that architects better futures for public and private sector clients.

Over my nearly 20-year career in homeland security, I have seen critical infrastructure public-private risk management redefined to address emerging, complex issues from violent extremism to complex mass attacks, cybersecurity grid and GPS resilience, extreme weather and electro and geomagnetic disturbances.

I have co-chaired interagency task forces that have integrated the private sector into government strategies, including those that are most relevant here today—the Joint U.S.-Canada Electric Grid Security and Resilience Strategy and the National Space Weather Strategy.

There is no doubt that we live in a dangerous world. State and non-state actors, insiders and promulgators of disinformation are growing in kind and consequence. Borders no longer protect us whether our shores or the fences and walls of our organizations. We have built a complex ecosystem where disruption in one node can ripple across the system and where threats are not bounded to one sector or one industry nor can we protect against every threat and secure every building system and network. Our country is too big; our infrastructure too interdependent; the cost too expensive; and, the outcome would alter our way of life.

This is why we are in the business of risk management. Think of a matrix where the x and y axes are increasing likelihood in consequence, respectively. A denial of service attack is highly probable, but the impact to a company and its operations is minimal.

Most natural disasters are high likelihood and low consequence. Superstorm Sandy or a 9.0 Cascadia Subduction Zone event are exceptions and flip, low likelihood, high consequence. A cyberattack against industrial control systems like the December 2015 attack on the Ukrainian power grid, lower probability than denial of service, but certainly more consequential. In 1859 Carrington Light GMD event. As Speaker Gingrich said, we are long overdue. And so, I would say it is more likely and certainly high consequence. There are half a dozen more risks on that matrix, including a high-altitude electromagnetic pulse, and we place it at a very low probability but high consequence.

All of the risks on this matrix must be managed. Since critical infrastructure is largely owned and operated by the private sector there are finite resources in a world where you have a business to operate, shareholder obligations, regulatory costs and rate recovery, just to name a few.

I want to be clear. We have not ignored the threat of an EMP. Industry and government are working hand-in-hand to better understand the impacts of EMP. The work that EPRI is doing is critical to understanding how the systems and its parts would be affected. This critical modeling can help inform where investments and shielding will have the maximum value and what operational procedures can mitigate voltage collapse. And much of this effort can be applied to mitigating the consequences of a GMD where we will have time to put measures in place and manage flow thanks to improved space weather forecasting and alerting.

Equally important is the fact that we understand an EMP, like many threats and hazards, is sector agnostic. Disruption to communications during incidents hampers response and restoration efforts. Malicious actors understand this, and Mother Nature is undiscerning.

There is debate about the sophistication of the attack on the Metcalf Substation that supplies power to Silicon Valley, but the perpetrators knew enough to cut the fiber lines that controlled 911 and downstream communications. A telephone denial of service attack hampered the ability of customers to call and utility operators to talk to each other in the Ukrainian incident.

An EMP or GMD will impact communication systems and data centers and, therefore, command and control. To industry's credit, they are looking beyond prioritized calling services as a contingency plan but it illustrates why we cannot take a silent approach and must understand the vulnerabilities caused by the intersections of these sectors.

This complex risk environment is what has given way to the public/private partnership. While government brings important capabilities to the table, information sharing, private sector clearances, research and modeling, war gaming, industry is heavily invested in ensuring its reliability and resilience. Disruptions impact their bottom line, their brand and their industry.

It is why the Joint U.S.-Canada Electric Grid Security and Resilience Strategy, the National Space Weather Strategy and the Joint Electromagnetic Pulse Resilience Strategy and corresponding action plans are critical. They lay out high-level goals for government and industry to guide action and investment, to enhance resilience and accelerate recovery from these types of events.

In conclusion, we are managing a complex risk environment and cannot protect against every threat and secure every asset. There is no one-size-fits-all approach. The solution requires a whole of community risk-based approach focused on mitigation planning and investment in a modern and secure infrastructure that is resilient to the threats of today and tomorrow.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Durkovich follows:]

Testimony of

CAITLIN DURKOVICH

Director, Toffler Associates

Former Assistant Secretary, Infrastructure Protection,
National Programs and Protection Directorate
Department of Homeland Security

Submitted to the

SENATE ENERGY & NATURAL RESOURCES COMMITTEE

For the May 4, 2017 Hearing

"To Examine the Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure"

Chairman Murkowski, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify at the hearing today, "To examine the threat posed by electromagnetic pulse and policy options to protect energy infrastructure and to improve capabilities for adequate system restoration."

My name is Caitlin Durkovich. I had the honor of serving eight years in the National Protection and Programs Directorate at the Department of Homeland Security (DHS), first as the Chief of Staff and from May of 2012 to January 2017, as the Assistant Secretary of Infrastructure Protection. NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

I have transitioned from government to Toffler Associates, a future-focused strategic advisory firm that architects better futures for public and private sector clients around the globe with an unwavering commitment to be the catalyst for change.

Over my nearly twenty-year career in homeland security, I have seen critical infrastructure public-private risk management redefined to address emerging, complex issues from lone offenders to complex mass attacks, cybersecurity grid and GPS resilience, interdependencies, electromagnetic pulse (EMP) and severe geomagnetic disturbances (GMDs), and security-by-design. I have co-chaired several interagency task forces that have integrated the private sector into government strategies, including those that are most relevant today – the *Joint US-Canada*

Strategy for Electric Grid Security and Resilience (December 2016) and *The National Space Weather Strategy* (October 2015).

There is no doubt we live in a dangerous world. State and non-state actors, cyber threats, unbounded disasters, lone offenders, insiders, and promulgators of disinformation are growing in kind and consequence. These threats – and our vulnerabilities to them – transcend political treaties, geographic borders, and corporate lines of business, blurring the lines between public and private accountability and responsibility. It is the private sector, which owns and operates most of our critical infrastructure, that must invest in and manage the risks and often intertwined consequences posed by an increasingly dynamic threat environment.

The energy sector in particular faces a variety of threats and hazards, largely driven by the increasing sophisticated threat actors with intent and capability as well as the interdependencies of the infrastructure systems, including the increasing reliance on digital infrastructure as the electric grid transitions from an analog system to a digital system to improve efficiency. The bottom line is the risk to digital and physical infrastructures has grown and our critical infrastructure is more vulnerable than it was a few decades ago.

My colleagues in government have testified before other committees about how the public-private partnership views EMP, and my time out of government has not changed my understanding of the threat or my perspective; therefore, I will leverage the work of DHS and my colleagues within the DHS Office of Cyber and infrastructure Analysis.

Background on EMP

An EMP is the burst of electromagnetic radiation created, for instance, when a nuclear weapon is detonated or when a non-nuclear EMP weapon is used. EMPs can be high frequency, similar to a flash of lightning, or low frequency, similar to an aurora-induced phenomenon. The consequences of an EMP can range from permanent physical damage to temporary system disruptions, and can result in fires, electric shocks to people and equipment, and critical service outages.

There are two general classes of EMP of concern: (1) Nuclear sources of EMP, such as High altitude EMP (HEMP), and (2) Non-Nuclear sources of EMP (NNEP). HEMP results from a nuclear detonation typically occurring 15 or more miles above the Earth's surface. The extent of HEMP effects depends on several factors including the altitude of the detonation, the weapon yield, and whether it was designed for EMP effects. On the ground, effects may be diminished by the electromagnetic shielding, or "hardening," of assets. A high-altitude burst could blanket

the entire continental United States and cause widespread impacts to multiple sectors, including to lifeline sectors, such as the energy and communications. HEMP threat vectors can originate from a missile, such as a sea-launched ballistic missile; a satellite asset; or a relatively low-cost balloon-borne vehicle.

Non-Nuclear EMP (NNEP) can be created by sources, such as Radio Frequency Weapons or Intentional Electromagnetic Interference devices, which are designed to produce sufficient electromagnetic energy to burn out or disrupt electronic components, systems, and networks. NNEP devices can be either electrically-driven, where they create narrowband or wideband microwaves, or explosively-driven, where an explosive is used to compress a magnetic field to generate the pulse. The range of an NNEP is short (typically less than 1 kilometer) and Faraday casings with line filters and surge arresters can mitigate much of the EMP effects.

Potential Impacts to Critical Infrastructure from EMP

We do not fully understand how an EMP event would impact electrical infrastructure, and it is the subject of ongoing analysis. In some of its forms, EMP could cause widespread disruption and serious damage to electronic devices and networks, including those upon which many critical infrastructures rely. There is uncertainty over the magnitude and duration of an electric power outage that may result from an EMP event due to ambiguity regarding the actual damage to electric power assets from an event. Any electric power outage resulting from an EMP event would ultimately depend upon several unknown factors and effects to assets that are challenging to accurately model, making it difficult to provide high-specificity information to electric system planners and system operators. These variables include characteristics such as the EMP device type, the location of the blast, the height of the blast, the yield of the blast, and design and operating parameters of the electric power system subject to the blast. Secondary effects of EMP may harm people through induced fires, electric shocks, and disruptions of transportation and critical support systems, such as those at hospitals or sites like nuclear power plants and chemical facilities.

In the development of *The National Space Weather Strategy*, we recognized that the growing interdependencies of critical infrastructure systems have increased potential vulnerabilities to EMPs and GMDs. Cross sector protection and mitigation efforts to eliminate or reduce EMP and GMD vulnerabilities are essential components of national preparedness. Protection focuses on capabilities and actions to eliminate vulnerabilities to EMP, and mitigation focuses on long-term vulnerability reduction and enhancing resilience to disasters. Together, these preparedness

missions frame a national effort to reduce vulnerabilities and manage risks associated with EMPs, GMDs, and other unbounded events.

Government and Industry and Collaboration

More than two decades of critical infrastructure programs and policies has fostered unprecedented collaboration between government and industry to mitigate the consequences of low probability, high consequence events, including EMP.

DHS continues to devote resources to address EMP risks, largely in three areas (1) risk assessment and analysis, (2) communication and coordination of threat information, and (3) research and development to mitigate EMP risks. NPPD, the Federal Emergency Management Agency, and the Science and Technology Directorate are working with the critical infrastructure community to ensure it has information to make critical decisions, and can respond to, assist recovery and mitigate the consequences of a potential EMP attack.

My fellow witnesses will testify to the scope of efforts industry is undertaking to continue to improve grid resilience to all-hazards. They range from continued research and development, mutual assistance and spare parts programs, supplemental operating strategies, and full-scale cross sector exercises.

Critical Infrastructure Risk Management

It is important to emphasize, however, that critical infrastructure, including the electric sector, takes a holistic approach to assessing and mitigating risks from not only EMP, but from cyber attacks, physical sabotage, and natural disasters, all of which can result in disruptions to their operations. The partnership between industry and government, which includes information sharing, capability development, training and exercises, and interoperable plans, is even more essential as our Nation continues to face an increasingly complex threat environment.

Conclusion and Recommendations

EMP is one of many threats to the functions, systems, and networks that underpin our national security, economic prosperity, and American way of life. From cyber espionage and sabotage, to the convergence of cyber and physical systems, to insider threats, and to EMPs and GMDs, owners and operators of critical infrastructure have an obligation to manage these persistent threats. However, the solution requires a whole of community effort that is focused not on one threat but on a broad range of threats. These challenges demand industry and government work

together to both develop mitigation plans and to invest in a modern and secure infrastructure that is resilient to the threats of today and tomorrow.

You can help by continuing to support national programs that strengthen public-private collaboration and enable the critical infrastructure community to efficiently and effectively manage the complex risk environment, and by continuing to advocate for a secure and resilient critical infrastructure.

Chairman Murkowski, Ranking Member Cantwell, and members of the Committee, thank you again for the opportunity to appear before you today. I look forward to your questions.

The CHAIRMAN. Thank you, Ms. Durkovich.
Mr. Manning, welcome.

STATEMENT OF ROBIN E. MANNING, VICE PRESIDENT, TRANSMISSION AND DISTRIBUTION, ELECTRIC POWER RESEARCH INSTITUTE

Mr. MANNING. Thank you, Madam Chairman, members of the Committee. Good morning.

I want to share with you a bit of history, if I can. I am a Vice President of Transmission and Distribution for the Electric Power Research Institute, but also spent 30 years at Duke Energy and another six at the Tennessee Valley Authority (TVA). And through this time my responsibility was leading construction, operation and maintenance of energy infrastructure.

So, as the Chairman put it so well earlier, I kept the lights on across the United States. As the leader of TVA's transmission organization in the 2008–2009 timeframe as I read the EMP Commission report, I struggled to understand how I could take the plethora of information that was available on EMP and practically apply it to create some sort of a plausible approach for risk management associated with TVA's system.

And that's exactly what EPRI is attempting to do as we are now one year into a three-year research project, began in April of 2016. Our project objective is to develop cost-effective mitigation tools, to develop recovery options for utilities and to form a basis for decision-making that provides utilities, like the TVA, the information that is necessary to effectively protect their customers from the EMP threat.

This project now has financial support from 57 U.S. utilities, making this project one of the most widely-supported collaboratives ever at EPRI. We're also collaborating very closely with the U.S. Department of Energy with national labs and the U.S. Department of Defense.

We have seven tasks on this project. Many of these tasks are being completed in parallel with various expected completion dates over the remaining two years of the project. We are seeking greater characterization of the HEMP threat as it relates to electric infrastructure; we're investigating specifically how EMP propagates and how it couples to power systems; we're testing that equipment to understand at what level do we begin to see damage from EMP events; and then we're combining the threats and the vulnerabilities to understand a more complete picture, a holistic picture of EMP impacts to infrastructure. But together this information provides methodologies and tools to support risk-informed decision, and of course, it's our intention to communicate our research findings to public policymakers and other stakeholders throughout the process.

For example, in February we released publicly a report assessing the impacts of a HEMP-generated, E3 energy wave on bulk power transformers. We advanced a series of a test nuclear blast across the United States, 11 different locations and assessed the value of each of those. We used advanced modeling assessment techniques as well as conservative assessment criteria and conservative engineering judgments throughout.

The results of this study indicated that damage to a large number of bulk power transformers from E3 is unlikely. Even so, the results of the assessment should not be interpreted to mean that HEMP or even the E3 would not adversely affect bulk power system reliability. The potential for widespread outages due to voltage collapse or the combined effects of E1, E2 and E3 are still being investigated.

Certainly impacts from HEMP are real; however, evaluating the effects of such events on complex systems like our electric power grid requires concrete, scientifically-based analysis from people who understand the power system. With greater understanding, cost-effective mitigation and/or recovery options can be developed and deployed.

The utility industry is poised to take further action, and more scientific research enables these actions to be both appropriate and cost effective for consumers.

At EPRI we are committed to providing sound science-based solutions to these complex problems and will continue to offer technical leadership and support to the electricity sector to public policymakers and other stakeholders to enable safe, affordable, reliable and environmentally responsible electricity to the people of the United States.

Thank you for your time. That concludes my testimony. I look forward to your questions.

[The prepared statement of Mr. Manning follows:]

Written Testimony

Hearing of the U.S. Senate Energy and Natural Resources Committee

Robin E. Manning
Vice President, Transmission and Distribution
Electric Power Research Institute

"Hearing to examine the threat posed by electromagnetic pulse and policy options to protect energy infrastructure and to improve capabilities for adequate system restoration"

May 4, 2017

The Electric Power Research Institute (EPRI) conducts research and development relating to the generation, delivery, and use of electricity for the benefit of the public. An independent, non-profit organization, EPRI brings together its scientists and engineers, as well as experts from academia and industry, to help address challenges in electricity, including reliability, efficiency, affordability, health, safety, and the environment. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries.

The subject of today's testimony is EPRI's research efforts related to electromagnetic pulse (EMP) events, including naturally occurring geomagnetic disturbances (GMD) as well as electromagnetic pulse (EMP) events, specifically high altitude EMP, or HEMP. EPRI has been researching GMD for many years with significant applications now implemented across the electric industry. Implications and solutions for EMP and HEMP are less understood. Much of the available information is not specifically applied to electric utilities, making it very difficult for utilities and regulators to understand effective options for protecting energy infrastructure. This testimony provides an overview of EPRI's research activities related to GMD, and a more detailed description of our EMP research efforts as we seek to better inform the issue with a firm technical basis for decision making.

GMD Research

During geomagnetic disturbance (GMD) events, magnetic field variations at the earth's surface drive low-frequency electric currents along transmission lines and through transformer windings to ground. These geomagnetically induced currents (GIC) cause half-cycle saturation of transformers leading to harmonic generation, increased reactive power losses, and heating of transformer windings and structural components. These effects are real, and have been observed in the past. For example, during the March 1989 geomagnetic storm, Hydro-Quebec experienced a blackout resulting from the effects of GMD-related harmonics, and a generator step-up unit (GSU) at Salem Nuclear Power Plant in New Jersey was damaged from resulting hotspot

heating. Several other effects were observed in the United States and Canada, for example tripping of capacitor banks, but these did not result in any significant reliability impacts[1].

EPRI recognizes the potential impacts of severe GMD events, and has been involved in GMD-related research for nearly four decades[2]. Some of EPRI's research activities in this area include:

- developing sensors and a support network for measuring GIC;
- developing software tools, models and guidelines to assess the impacts of severe GMD events on the bulk-power system;
- improving the fidelity of existing models (e.g. earth conductivity);
- improving understanding of potential impacts of GMD events on bulk-power system components;
- evaluating mitigation options and their application; and
- supporting the development of benchmark GMD events used in assessments.

Because EPRI's research in the GMD area is expansive, only current activities will be addressed.

Geomagnetic Field Monitoring

EPRI currently has a research project underway to install three axis magnetometer sensors between existing magnetic observatories operated by the U.S. Geological Survey (USGS) to improve magnetic field resolution throughout the United States. Measurement data will be used to validate deep earth conductivity models, and improve understanding of local geological factors that can affect the geoelectric field induction process.

SUNBURST Network

The EPRI SUNBURST network is both an organized method for measuring geomagnetically induced currents (GICs) and a source of data for continuing research studying the cause, effects and mitigation of GIC impacts on electrical power systems. While the primary focus of this research is operating the monitoring network, the data collected in this project will be used for feedback into new prediction models that will serve as advance warnings, that is, the NASA Solar Shield project. The SUNBURST project also supports an annual event where relevant scientists from the field of solar phenomena/space weather come together to discuss common issues and concerns related to GICs.

The SUNBURST network consists of a consortium of member utilities where near-real-time continuous monitoring of the GIC flowing in the neutral of large power transformers is performed. Over the last decade, EPRI has accumulated a body of data and experience about correlations between space weather and GIC flows in the grid.

---

[1] North American Electric Reliability Corporation (NERC), March 13, 1989 Geomagnetic Disturbance: www.nerc.com/files/1989-quebec-disturbance.pdf

[2] *Investigation of Geomagnetically Induced Currents in the Proposed Winnipeg-Dulluth-Twin Cities 500 kV Transmission Line.* EPRI, Palo Alto, CA: 1981. EL-1949

New GIC Sensor

One of the limitations of measuring GIC using current technology (e.g. SUNBURST) is that the monitoring location must be the neutral of the transformer. Depending on the type of transformer, e.g. an autotransformer, a neutral connected GIC node may not provide the observability necessary to determine the GIC flows that could affect power system operation. To fill this gap, EPRI has recently developed a sensor that is capable of measuring GIC flows in energized conductors. Measurement of GIC in energized AC (alternating current) transmission lines and transformer windings improves observability of the behavior and effects of GIC on the bulk-power system. In addition, GIC flows through interconnections and in some cases, remote transformers can be measured directly. This will lead to developing more effective network boundary models, and closer representation of actual GIC conditions when assessing impact to transformers.

Current Research in Grid Operations & Planning Area

Harmonics studies are an integral part of any GMD vulnerability assessment, and as such, are a key component of related reliability and planning assessments and associated regulatory requirements, e.g. NERC TPL-007-1 standard. However, commercially-available software tools or industry guidelines necessary to perform such assessments are limited. To fill this gap, EPRI is developing an open source software tool that can be used to perform GMD-related harmonics studies. Additionally, guidelines for performing assessments to determine the potential impacts of GMD-related harmonics on the bulk-power system are being developed.

EMP Research

Electromagnetic pulse (EMP) attacks and geomagnetic disturbance (GMD) events are often discussed together when evaluating potential impacts on the bulk-power system and approaches for improving system resiliency. While both events are considered high-impact low-frequency (HILF) events (along with physical attacks, severe storms, earthquakes, and other similar events), there are very important differences that should be considered when evaluating resiliency improvement priorities and investment decisions.

The high-altitude detonation of a nuclear weapon can generate a large electromagnetic pulse (referred to as a high-altitude EMP or HEMP) that is comprised of three components: E1, E2 and E3. Depending on weapon yield and height of burst the resulting EMP can impact large geographical areas such as the size of an electrical interconnection. The early-time pulse, E1, refers to a nearly instantaneous (rise times are on the order of 2.5 nanoseconds or 2.5 billionths of a second) – large magnitude (50 kV/m) pulse that can result in damage to electronic components and electric infrastructure. The intermediate-time pulse or E2, refers to the short duration pulse which has characteristics similar to lightning although the magnitude of E2 is much lower (~ 0.1 kV/m) and the way in which it couples into electric infrastructure is different. The latter component, magnetohydrodynamic electromagnetic pulse (MHD-EMP) or simply E3 is similar to a severe GMD event, and can drive low frequency, geomagnetically-induced currents (GIC) in transmission lines and power transformers. However, there are two key

differences between E3 and GMD. First, E3 from a single high-altitude detonation would not generate planetary-scale effects like a severe GMD event can. Secondly, the magnitude and duration of E3 are significantly different. The magnitude of E3 can be much higher than that of a severe GMD event; however, the duration of E3 is much shorter lasting only a few minutes as compared with days in the case of a severe GMD event. As with severe GMD events, potential impacts from E3 range from voltage collapse to increased hotspot heating in bulk-power transformers.

EMP Research Project Description

HEMP events are a growing concern in the energy business. While the industry has worked to develop effective responses to GMD, little definitive work has centered on the effects of a HEMP attack. Numerous constituencies are pressing to ensure the electric power system is more resilient to a large HEMP event, but technical information is inconsistent and options to increase resilience through hardening and recovery are not well-defined. Some proposed approaches are high-cost and lack the technical basis to substantiate their viability. To fill this gap, EPRI initiated a three-year research project in April 2016, currently with financial support from fifty-six electric utilities, to improve understanding of the potential impacts of HEMP on the bulk-power system and develop cost-effective mitigation options. The financial support of EPRI's members demonstrates the importance to them of providing scientific and technical analysis of this issue for the benefit of the public.

As a part of this research project EPRI is collaborating closely with the U.S. Department of Energy (DOE), national laboratories, and the U.S. Department of Defense (DoD).

The EPRI EMP project is comprised of 7 tasks which are as follows.

Task 1 –HEMP Threat Characterization

As a part of the threat characterization task, we are:

- identifying the state of knowledge of unclassified HEMP research,
- identifying conservative (bounding) HEMP waveforms (magnitude, spatial and time dependent characteristics, etc.) that can be used to assess the potential impacts on bulk-power system components, and
- investigating the physics of HEMP propagation and coupling to power system infrastructure.

As a part of this research, all three components of the HEMP environment are being evaluated, i.e., E1, E2, and E3.

In September 2016, EPRI released its first report[3] associated with this task which is a compendium describing the state of knowledge of HEMP research that is relevant to the electric

[3] *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs.* EPRI, Palo Alto, CA: 2016. 3002008999.

power industry as well as a suite of unclassified HEMP environments that can be used in power system assessments.

We are currently developing models to simulate coupling of E1/E2 into transmission infrastructure (substation bus work, control cables, control houses, etc.) and are performing an analysis of a transmission substation to determine impacts of E1/E2 on equipment. Modeling results will also be used to inform equipment testing and mitigation efforts. Simulation work has begun and will continue into 2018. EPRI is currently working with Lawrence Livermore National Laboratory (LLNL) to further research in this area.

Additionally, an important component of this research is to develop tools that utilities can use to perform their own assessments. To that end, EPRI is developing software tools and modeling guidelines that can be used by utilities to simulate the coupling of an E1 pulse into overhead and underground conductors and/or control cables. The beta version of the overhead conductor coupling tool is expected to be finished by the fourth quarter of 2017.

Task 2 – Electric Infrastructure EMP Vulnerability

This task is identifying the vulnerability of transmission systems and support assets (protection and control systems, communications, SCADA, cables, transformers, insulators, etc.) exposed to the HEMP threat defined in Task 1 – HEMP Threat Characterization by performing laboratory tests. To facilitate high-volume EMP testing of components, EPRI is building two EMP test labs and updating our high-voltage test lab in Lenox, MA to test systems and components by subjecting them to synthetic EMP pulses (E1). Equipment testing will include both radiated and conducted transients. Testing of protection and control (P&C) systems to determine impacts of E1 is initial priority. Testing is expected to begin by the second quarter of 2017 with initial results possible by the end of the year.

In addition to performing tests internally, EPRI is also partnering with Sandia National Laboratory and Little Mountain Test Facility to perform additional E1 testing of P&C equipment.

Task 3 – Electric Infrastructure Impacts

This task is assessing the potential impacts of a HEMP attack on the bulk-power system by combining the modeling results of Task 1 with the equipment testing results of Task 2. Assessment techniques, models and tools for assessing the impacts of a HEMP attack are also being developed.

The first of many studies has been completed, and will be described in more detail later in this testimony. A report[4] assessing the potential effects of E3 on U.S. bulk-power transformers was released in February 2017. A companion report assessing the potential impacts of E3 on the stability of the bulk-power system is expected to be finished by the third quarter of 2017.

---

[4] *Magnetohydrodynamic Electromagnetic Pulse Assessment of the Continental U.S. Electric Grid: Geomagnetically Induced Current and Transformer Thermal Analysis.* EPRI, Palo Alto, CA:2017. 3002009001

The results of the first E1 threat assessment are expected by the end of the year.

Task 4 – Mitigation, Hardening and Recovery

This task is assessing various mitigation and hardening approaches that can be employed to reduce the impacts of HEMP on bulk-power system reliability. Potential unintended consequences of various mitigation and hardening strategies are being evaluated. Enhanced recovery procedures/plans are being developed.

As an initial step, EPRI is developing interim guidance on hardening substations using information provided in relevant IEC[5] and military standards. This is only a first step, and EPRI is not recommending utilities harden to these standards. Future research efforts aim to develop cost-effective hardening and mitigation solutions that are relevant to electric power infrastructure. Interim guidance is expected to be completed and made available to project members by the third quarter of 2017.

Task 5 – Risk-based Decision Support

This task is developing methodologies and tools to support risk-informed decisions regarding the implementation of HEMP hardening and mitigation measures. A framework for assessing the relative benefits of various hardening and mitigation approaches will be developed. Support tools designed to aid in decision making will be developed as a part of this task.

Task 6 – Trial Implementation

Once hardening measures have been identified, supporting member utilities will have the opportunity to evaluate implementation on aspects of their systems. This task will develop a collection of leading industry practices with regards to HEMP mitigation and hardening. Applications of various assessment techniques and mitigation options will be catalogued, and the effectiveness and lessons learned will be communicated.

Task 7 – Project Member and Stakeholder Communication

An important aspect of this research project is communicating the results to our supporting members and stakeholders as appropriate. This task is developing communications to inform of the background and potential impacts of HEMP, and appropriately share new learning in a timely manner.

February, 2017 Report: E3 Assessment of the Continental U.S. Electric Grid

GIC generated by E3 resulting from a HEMP attack can cause additional hotspot heating in windings and structural parts of bulk-power transformers. If heating is severe enough, it can cause damage to the transformer. The loss of hundreds of bulk-power transformers could create an environment where system recovery is not possible in a timely manner resulting in long-term

[5] IEC is the International Electrotechnology Commission – an international standards organization

blackout. Thus, one of the first steps in this three-year research project was to evaluate the potential impacts of E3 on bulk-power transformers.

Past research performed by Oak Ridge National Laboratories (ORNL) during the mid-late 1980's through early 1990's and late 2000's evaluated the potential impacts of E3 on bulk-power transformers; however, the results of the ORNL research had conflicting conclusions. Earlier ORNL research[6] concluded that E3 would not result in significant damage to bulk-power transformers while a later research report[7] concluded that transformer damage was likely, and that up to 100 transformers could be damaged depending on the target location.

The purpose of the EPRI study was to determine, using advanced transformer models that were not available at the time of the ORNL research, whether or not a significant number (hundreds) of bulk-power transformers would experience thermal damage from a single E3 event. More simply, the study sought to answer the question, "if a HEMP attack occurred, would there be enough bulk-power transformers left to facilitate system recovery?"

The fundamental approach to the EPRI study was similar to that adopted by the North American Electric Reliability Corporation (NERC) to assess the potential impacts of severe geomagnetic disturbance (GMD) events on bulk-power transformers. First, the electric field environment necessary for calculating GIC flows was identified and a direct current model of the interconnection-wide system was assembled. For this study, a publicly available E3 environment along with a model of the United States bulk electric system was used to calculate the GIC flows in the transmission system that would result from a single, high-altitude detonation over the continental United States (CONUS). GIC calculations were then performed assuming weapon detonation over 11 separate locations in the CONUS. The resulting time-series GIC flows were then used to compute the time-series hotspot temperature of each bulk-power system transformer included in the interconnection-wide assessment using physically-based transformer models. The maximum instantaneous hotspot temperatures were then evaluated against conservative temperature limits that were based on an assumed condition-based GIC susceptibility category of the entire transformer fleet. The number of transformers that were identified as exceeding the specified temperature limits were then combined with the probabilities of a given transformer being in one of the three specified categories to estimate the expected number of bulk-power transformers to be at potential risk of thermal damage. Additionally, the potential for thermal damage caused by circulating harmonic currents in the tertiary windings of large autotransformers was also evaluated.

The EPRI study found that although a significant number of transformers (hundreds to thousands) could experience GIC flows greater than the 75 amps/phase screening criteria adopted from NERC TPL-007-1, only a small number (3 to 14 depending on the target location evaluated) of these transformers were found to be at potential risk of thermal damage. In addition, the at-risk transformers were found to be geographically dispersed.

---

[6] Electromagnetic Pulse Research on Electric Power Systems: Program Summary and Recommendations. Oak Ridge National Laboratories, Oak Ridge, TN: 1993. ORNL-6708.

[7] Meta-R-321, The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid. Metatech Corporation, January 2010.

The results of this study agree with earlier work performed by ORNL which indicate that the failure of a large number (hundreds) of bulk-power transformers from E3 is unlikely. The assessment results can be used to help quantify the overall risk of E3 impacting the bulk-power system (interconnection-level assessment), but they should not be interpreted to indicate E3 will not affect bulk-power reliability since the potential for widespread outages due to voltage collapse or the synergistic effects of E1, E2 and E3 are still being investigated. Additionally, because of the number of conservative assumptions that were required due to the lack of asset specific data, the results should not be used to inform investment decisions at individual utilities.

A companion study to the GIC and transformer thermal assessment, an analysis determining the potential for voltage collapse resulting from E3, is expected to be completed by the third quarter of 2017. Future research will be aimed at improving the assessment process to include the synergistic effects of E1, E2 and E3.

Concluding Remarks

The potential impacts of GMD and HEMP are real; however, evaluating the effects of such events on existing and future power grid infrastructure requires concrete, scientifically-based analysis. Once the true impacts are known, including the potential unintended consequences of mitigation options, cost effective mitigation and/or recovery options can be developed and employed.

The recent E3 assessment of the US bulk-power transformer fleet is merely a first step in a series of studies aimed at informing the electric utility industry of the potential impacts of HEMP on the bulk-power system. Although the results of this assessment indicate that E3 from a single high-altitude detonation would have marginal effect on bulk-power transformers, the results should not be interpreted as indicating that HEMP will not affect bulk-power system reliability. More research is needed to determine the impacts of E1 on bulk-power system assets, and more importantly, the ability to accurately capture, through modeling and analysis, the synergistic effects of E1, E2 and E3 is needed to assess the true impact of HEMP on the grid and develop cost-effective mitigation options.

EPRI is committed to developing science-based solutions to these difficult problems, and offers technical leadership and support to the electricity sector, public policymakers, and other stakeholders to enable safe, reliable, affordable, and environmentally responsible electricity to the people of the United States.

The CHAIRMAN. Thank you, Mr. Manning.
Mr. Wailes, welcome.

STATEMENT OF KEVIN WAILES, CHIEF EXECUTIVE OFFICER, LINCOLN ELECTRIC SYSTEM, AND MEMBER OF THE BOARD OF DIRECTORS, AMERICAN PUBLIC POWER ASSOCIATION

Mr. WAILES. Chairman Murkowski, Ranking Member Cantwell, members of the Committee, thank you for giving me the opportunity to testify today.

My name is Kevin Wailes. I'm the CEO of the Lincoln Electric System (LES) in Lincoln, Nebraska. I'm testifying on behalf of the American Public Power Association (APPA) on whose Board of Directors I serve. APPA is the voice for not-for-profit, community-owned utilities that serve 49 million people nationwide.

I also serve as the Co-Chair of the Electric Subsector Coordinating Council which is made up of 30 utility and trade association CEOs and serves as the electric sector's principle liaison with the Federal Government on policy level security issues.

The electric sector takes very seriously the threat of electromagnetic pulse, or EMP, events and certainly, if you consider reliability, it's what we do. That's the primary objective for electric utilities in the first place.

Chairman LaFleur provided a good description of the various types of EMP events. I want to emphasize, consistent with Senator Murkowski's, Chair Murkowski's, opening comments, that in effect a HEMP attack is an event that would be an act of war or terrorism, and in fact, is the responsibility of the Federal Government to prevent, as a matter of national security. But that doesn't mean that we don't take it very serious in trying to develop how we might mitigate that.

The technical impact of a HEMP event on the electric infrastructure is uncertain. Though through a collaborative effort, as mentioned by Rob, with the Electric Power Research Institute and the Federal Government were conducting research to gain more information to be able to provide that mitigation.

Some proposed the electric industry should install a particular protected device or fully gold-plate the entire grid so that it could survive a HEMP event. However, there's really no consensus on what measures should be taken at this point. The potential unintended effects of that type of protection on the grid or how successful the efforts would be if we, in fact, tried to do that at this time.

Cost is a significant factor. As a community-owned, not-for-profit utility, all additional costs borne by LES, for example, would have to be passed directly on to our customers.

Assuming EMP blocking devices could be installed to protect the entire grid, power supply would still likely be disrupted by a HEMP event due to the collateral impacts on other critical infrastructures, as mentioned by Ms. Durkovich, the utilities rely on to provide services.

EMP are one of many threats the electric sector must confront, as other witnesses identified, including severe weather events, geomagnetic disturbances, cyber and physical attacks. Given this broad threat landscape, our industry understands that we cannot

protect all assets from all threats and instead we must manage that risk.

To do this, the electric sector follows a multilayered risk management approach to grid protection. A HEMP event is a high-impact, low-probability threat. We take EMP event threats seriously, but we must consider them within the context, a broader context of all threats. A cyberattack aimed at disrupting electric service would be a relatively cheaper and easier weapon to deploy and finding the needed nuclear materials and delivery vehicle to deploy that type of weapon. So clearly, we must place more effort on mitigating the highest and most profitable risk, probable risk.

Given industry cannot protect the electric grid from all potential threats, we focus on all hazard recovery, that is, regardless of the cause of damage to the electric system, preparations to ensure mitigation, response and restoration are substantially the same. Grid operators must prioritize critical asset protection, engineer redundancy on to the system and stockpile spare equipment and as also mentioned, there are several programs that are ongoing with respect to enhance that capability given these new threats.

In conclusion, electric utilities are working on multiple fronts to increase the scientific understanding of the potential impacts of EMP. As policymakers, there are several ways that you all can support that effort.

First, the EMP Commission should be directed to work with owners and operators of critical infrastructure, EPRI, the North American Electric Reliability Corporation, and help assist the Electric Subsector Coordinating Council (ESCC), I'm sorry, and assess the vulnerability to the electric grid to EMPs. Collaboration between experts on EMP and experts in the utility industry will end up with the best product.

Second, we need to ensure that the classified reports and research produced by both DoD and DOE are available and that can accurately reflect the threat we're trying to evaluate so we can come up with the best solution.

Finally, this is an extremely complex issue that cannot be solved with a one-size-fits-all solution, as previously identified. Prescriptive legislative directives could have unintended consequences and saddle ratepayers with increased cost with no associated value.

Similarly, protecting the current successful standards in process put into place by the Energy Policy Act of 2005 is critical. This structure produces standards based upon expert input and necessity when it comes to vast and complex bulk electric system.

Thank you for the opportunity to testify, and I look forward to answering any questions as part of the panel.

[The prepared statement of Mr. Wailes follows:]

Testimony of

KEVIN WAILES

Chief Executive Officer, Lincoln Electric System

On Behalf of the American Public Power Association

Submitted to the

SENATE ENERGY & NATURAL RESOURCES COMMITTEE

For the May 4, 2017, Hearing

"To Examine the Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure"

Chairman Murkowski, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify at the hearing today, "To examine the threat posed by electromagnetic pulse and policy options to protect energy infrastructure and to improve capabilities for adequate system restoration."

My name is Kevin Wailes. I am the Chief Executive Officer at Lincoln Electric System (LES), headquartered in Lincoln, Nebraska. LES provides electricity to approximately 135,000 residential, commercial and industrial customers in Lincoln and the surrounding communities. Today, I am testifying on behalf of the American Public Power Association (APPA), on whose board of directors I serve. APPA is the voice of not-for-profit, community-owned utilities that serve 49 million people in 2,000 towns and cities nationwide.

I also serve as a co-chair of the Electricity Subsector Coordinating Council (ESCC), a public/private partnership as outlined in the National Infrastructure Protection Plan (NIPP) for critical infrastructure owners and operators, which serves as the electricity sector's principal entity with the government on policy-level security issues. The ESCC is composed of 30 utility and trade association CEOs, representing a cross-section of the electricity industry. It engages regularly with its federal government counterparts, including senior Administration officials from the White House, Department of Energy (DOE), Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the Federal Bureau of Investigation (FBI), and others as needed.

Introduction

Protecting the nation's electric power grid and ensuring a reliable and affordable supply of energy are of utmost importance to APPA, its utility members, and the electric power industry. The power grid is a complex, interconnected network of generation, transmission, distribution, control, and communication technologies that can be impacted by a range of threats—from natural events like hurricanes, earthquakes, and geomagnetic disturbances (GMDs) caused by

solar flares, to malicious events such as cyber, physical, and electromagnetic pulse (EMP) attacks. Given this broad threat landscape, our industry understands that we cannot protect all assets completely from all threats, and instead must manage risk. To do this, the electric sector follows a multi-layered risk management approach to grid protection. The key to this strategy involves setting priorities to protect the most critical power grid components against the most likely threats. By framing risk as a function of likelihood and consequence, we can allocate resources more effectively.

Electromagnetic Pulses (EMPs)

The threat we are here to discuss today are electromagnetic pulses or "EMPs." An EMP is a blast of electromagnetic energy that can potentially disrupt or destroy electronic devices within an affected area. Manmade EMPs are produced by nuclear weapons or other devices designed to create intentional electromagnetic interference. The electricity sector is not the only sector that would be impacted by an EMP—any activity that relies upon devices containing integrated circuitry, such as industrial process control systems, hospital equipment, transportation, and telecommunication systems — may be affected by an EMP attack. As such, the responsibility for protecting the United States from a national-level event like an EMP attack is that of the country's defense intelligence and military services, not individual critical infrastructure providers.

There are two types of EMP events of primary concern to the electric industry. The first is a "high-altitude electromagnetic pulse" ("HEMP") caused by the detonation of a nuclear weapon in the atmosphere. A HEMP attack would have a potentially catastrophic impact on society; it is what the industry terms a "high impact, low probability" threat. An attack of this magnitude would be an act of war or terrorism, and thus the federal government has primary responsibility for preventing high altitude EMPs as a matter of national security.

The second type of EMP results from the use of a smaller directed energy weapon against a single facility or piece of equipment. Mitigation strategies for this type of EMP threat include physical protection measures, including limiting proximity and controlling access, while also relying on system redundancy. To cause significant damage to the electricity grid, dozens of directed energy weapons would need to be built, deployed, and detonated in a coordinated attack without being detected or stopped by law enforcement.

Protecting Infrastructure

How exactly an EMP event would impact electrical infrastructure remains uncertain and is the subject of ongoing analysis. A recent study published by Schweitzer Engineering labs concludes, by testing and analysis, that commercially-available intelligent electronic devices designed to meet IEC (International Electrotechnical Commission) requirements are resilient to High-Altitude Electromagnetic Pulse (HEMP) events. The Schweitzer study also concludes that existing IEEE (Institute of Electrical and Electronics Engineers) substation design standards are

sufficient to protect intelligent electronic devices from HEMP. [1] Unfortunately, the Schweitzer report was prepared based on public-source EMP waveform data; access to classified information on EMP waveforms would better inform the study and allow industry to better prepare for cost-effective mitigation.

Some propose that to address EMP events, the electric industry install their particular "protective device" or fully "gold plate" the entire grid so that it could, theoretically, at least partially survive a high altitude nuclear event. However, there is no consensus on precisely what measures should be taken, the unintended effects they might have on the system, how much such an effort would cost, or how successful such efforts would be in actually limiting impacts to the bulk power system. For example, due to non-uniform designs and complexity, substation solutions (e.g., Faraday cages) would have to be individually customized, which would not come at a standardized rate. Additionally, there are concerns that installing "protective devices" in some areas of the bulk power system could unintentionally cause problems in other areas. Further research and testing of these devices is needed.

Even assuming that every conceivable blocking device were installed to protect every inch of the electric grid and caused no problems, power supplies still would likely be subject to disruption from other collateral impacts due to a HEMP event. That is because other critical infrastructures that utilities rely upon to function—such as transportation systems for generation fuel, water systems for cooling, and telecommunications for operations—may also be adversely impacted.

To better understand the potential impact of EMP and effective mitigation techniques, the Electric Power Research Institute (EPRI), an independent research organization funded by industry, has embarked on an ambitious, three-year research project. This project is in partnership with government entities to determine the specific nature of the HEMP threat, based on objective evidence, and to develop cost-effective strategies for mitigation. On February 21, 2017, EPRI released the first in a series of assessments on how an EMP caused by the detonation of a high altitude nuclear weapon above the U.S. would affect the electric grid.[2] This first study found that a small number of large power transformers (3 to 14 of 37,000 analyzed) would be at risk for thermal damage. Its findings represent only one piece of a complex puzzle. More work is needed to fully investigate other potential impacts to the entire bulk-power system and will be pursued in subsequent phases of the project.

Enhancing Capability for Adequate System Restoration

Government-industry coordination on national security issues such as EMPs is critical to preparing an effective response to these national security threats. One such effort is the Electric Subsector Coordinating Council (ESCC), which serves as the principal liaison between the federal government and the electric power industry. The ESCC is a forum for electric sector CEOs and top-level government executives from DOE, DHS, the FBI, and other organizations to engage on current and emerging threats like EMP that would have cross-sector and national

[1] *Understanding Design, Installation, and Testing Methods That Promote Substation IED Resiliency for High-Altitude Electromagnetic Pulse Events*, Tim Minteer, Travis Mooney, Sharla Artz, and David E. Whitehead, Schweitzer Engineering Laboratories, Inc., February 2017.
[2] https://www.epri.com/#/pages/product/000000003002009001/

security implications. The ESCC works across the electric power industry, with the government and other interdependent critical infrastructure sectors to improve planning for, and response to, major incidents. The ESCC formed a R&D task force to address several issues including EMP and is supporting EPRI's EMP Project.

Regardless of the cause of damage to the electric system, preparations to ensure mitigation, response and restoration are the same: grid operators prioritize risk to enhance protection around critical assets, engineer redundancy to avoid single points of failure, stockpile spare equipment for hard-to-replace components, and develop other contingencies to minimize impacts. The ESCC is involved in all aspects of these preparations.

- **Exercises:** Electric utilities plan and regularly exercise for a variety of emergency situations that could impact our ability to provide electricity. The industry participates in many incident response exercises, including five national-level exercises since November 2015. One such exercise, GridEx III, involved more than 360 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico. Managed by the North American Energy Reliability Council (NERC) and the Electricity Information and Analysis Center (E-ISAC), GridEX III also included an executive tabletop exercise where 32 electric sector executives and senior U.S. government officials worked through incident response protocols to address widespread outages.[3] GridEx events are conducted every two years; GridEx IV is planned for November 2017.

- **Mutual Assistance Programs:** The three segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after emergencies. The years of experience industry has had in deploying these resources is a valuable tool. In fact, the ESCC has led efforts to create a Cyber Mutual Assistance (CMA) program that will allow utilities to share critical personnel and equipment in the event of cyber-related emergencies. To date, 100 utilities are participants, covering about 80 percent of the country's electricity customers—or 118 million.

- **Spare Equipment Programs:** Electric companies regularly share transformers and other equipment through long existing bi- and multi-lateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program (STEP), SpareConnect, and the newly formed Grid Assurance program—to improve grid resiliency.

- **Transformer Transportation Emergency Support Guide:** The ESCC, in coordination with other critical infrastructure sectors and the government, has developed a Transformer Transportation Emergency Support Guide to expedite the deployment of large spare equipment, such as transformers, quickly over rail, roadways, and waterways in an emergency.

[3] NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC); it develops and enforces reliability standards for the bulk power system. The E-ISAC serves as the primary security communications channel for the electricity sector.

- **Supplemental Operating Strategies:** Following GridEx III and the cyber incident affecting Ukrainian distribution electric companies, the industry focused on electric grid operations under sub-optimal circumstances. The ESCC has asked grid experts to explore "extraordinary measures" that can be anticipated, planned for, and practiced so they are not contemplated for the first time during an incident that disables significant technology used to operate the grid. These "extraordinary measures" include, but are not limited to, operating systems in "manual" configuration where systems are not allowed to automatically re-energize, engaging in planned separations or "islanding" of portions of the grid to avoid cascading outages, leveraging secondary and tertiary back-up systems, or operating in other degraded states.

- **Research & Development:** The ESCC R&D strategic committee is overseeing the industry's collaboration efforts with the government, including the national labs, on resilience and infrastructure investments for grid security R&D. In July 2016, DOE and EPRI announced the *Joint Electromagnetic Pulse Resilience Strategy* to "...enhance coordination...and to guide future efforts to help meet the growing demands for EMP guidance."[4] DOE and EPRI committed to developing separate, but coordinated, Action Plans to implement the goals outlined in the Joint Strategy; DOE released its Action Plan in January 2017.[5]

Conclusion and Recommendations

As I hope I have conveyed, the electric utility industry takes the threat of EMPs seriously and we are working on multiple fronts to increase the scientific understanding of the potential impacts, including mitigation and response options. As policymakers, there are several ways in which you can support our efforts. First, we recommend that the reconstituted EMP Commission be directed to work with owners and operators of critical infrastructure, EPRI, ESCC, NERC, and the E-ISAC as the Commission executes its mission to assess the vulnerability of the electric grid to EMPs and to develop recommended policy actions. Combining the unique backgrounds of the EMP Commission with the knowledge of experts in grid engineering and operations would produce a more meaningful and informed product. Allowing industry representatives with appropriate security clearances to access classified EMP reports produced by the Departments of Energy and Defense would also be immensely helpful. The more information we have on the potential threat, the better we can mount an effective response. Finally, I want to reiterate that this is an extremely complex issue that cannot be solved with a "one-size-fits-all" solution. Prescriptive legislative directives could have unintended consequences and saddle ratepayers with increased costs for which they receive little or no additional benefits. Similarly, protecting the current successful NERC/FERC standards-setting process that this committee developed in the Energy Policy Act of 2005 is critical. This structure produces standards based upon expert input, a necessity when it comes to the vast and complex bulk electric system.

Thank you for the opportunity to testify. I look forward to answering any questions you may have.

---

[4] https://www.energy.gov/sites/prod/files/2016/07/f33/DOE_EMPStrategy_July2016_0.pdf
[5] https://www.energy.gov/oe/downloads/doe-electromagnetic-pulse-resilience-action-plan

Supplemental Document to the Testimony of

KEVIN WAILES

Chief Executive Officer, Lincoln Electric System

On Behalf of the American Public Power Association

Submitted to the

SENATE ENERGY & NATURAL RESOURCES COMMITTEE

For the May 4, 2017, Hearing

"To Examine the Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure"

Exercises

The electric sector plans and regularly exercises for a variety of emergency situations that could impact their ability to provide electricity. The industry participates in many incident response exercises, including five national-level exercises since November 2015.

I. **GridEx III** *(NERC, November 2015)* gathered more than 360 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico. GridEX III also included an executive tabletop exercise where 32 electric sector executives and senior U.S. government officials worked through incident response protocols to address widespread outages.

II. **Clear Path IV** *(DOE, April 2016)* convened 200 participants from the oil and gas and electric power industries and federal and state officials to test response and restoration protocols to a catastrophic simulated earthquake and tsunami in the Pacific Northwest.

III. **Cascadia Rising** *(FEMA, June 2016)* was a three-day exercise that tested first responders and government emergency personnel responders and government emergency personnel responses in the immediate aftermath of a significant earthquake.

IV. **Cyber Guard** *(DOD/NSA, June 2016)* was a two-week exercise that tested the response capabilities of 1,000 energy, IT, transportation, and government experts to a major cyber-attack.

V. **Joint Financial Services – Electric Sector Cyber Exercise** *(Treasury, August 2016)* examined incident response capabilities and interdependencies between the two sectors.

Spare Equipment Programs

Electric companies regularly share transformers and other equipment to improve grid resilience from a range of threats. There are multiple spare transformer initiatives:

I. **Spare Transformer Equipment Program (STEP)** - In 2006, federal energy regulators approved the Spare Transformer Equipment Program (STEP), an electric industry program that strengthens the sector's ability to restore the nation's transmission system more quickly in the event of a terrorist attack. STEP represents a coordinated approach to increasing the electric power industry's inventory of spare transformers and streamlining the process of transferring those transformers to affected utilities in the event of a transmission outage caused by a terrorist attack.

Under the program, each participating electric utility is required to maintain and, if necessary, acquire a specific number of transformers. STEP requires each participating utility to sell its spare transformers to any other participating utility that suffers a "triggering event," defined as an act of terrorism that destroys or disables one or more substations and results in the declared state of emergency by the President of the United States.

Any investor-owned, government-owned, or rural electric cooperative utility in the United States or Canada may participate in the program. Currently over 50 utilities are members.

II. **SpareConnect** - The SpareConnect program provides an additional mechanism for Bulk Power System (BPS) asset owners and operators to network with other SpareConnect participants concerning the possible sharing of transmission and generation step-up (GSU) transformers and related equipment, including bushings, fans and auxiliary components. SpareConnect establishes a confidential, unified platform for the entire electric industry to communicate equipment needs in the event of an emergency or other non-routine failure.

SpareConnect complements existing programs, such as the Spare Transformer Equipment Program (STEP) and voluntary mutual assistance programs, by establishing an additional, trusted network of participants who are uniquely capable of providing assistance concerning equipment availability and technical resources. SpareConnect does not create or manage a central database of spare equipment. Instead, SpareConnect provides decentralized access to points of contact at power companies so that, in the event of an emergency, SpareConnect participants are able to connect quickly with other participants in affected voltage classes. SpareConnect does not impose any obligation on participants to provide any information or to make any particular piece of equipment available. Once connected, those SpareConnect participants who are interested in providing additional information or sharing equipment work directly and privately with each other on the specific terms and conditions of any potential equipment sale or other transaction.

As of March 27, 2017, SpareConnect has 129 member utilities. Seven of the municipal utility members are joint action agencies that participate on behalf of themselves and their 176 municipally-owned utilities. Generation & Transmission (G&T) cooperatives within SpareConnect participate on behalf of 180 distribution

cooperative systems.

III. **Grid Assurance** – Launched in 2016 by six large electric utility companies, Grid Assurance is an independent company created to enhance grid resiliency by giving electric transmission owners faster access to long-lead time critical equipment necessary to recover from catastrophic events that could impact the nation's electric grid. More information is available at http://www.gridassurance.com/#IndustryDriven

The CHAIRMAN. Thank you, Mr. Wailes. Thank you, all, for your comments here this morning.

Let me start with just a broad question to you all. Is it fair to say that you would all agree that an EMP attack is, in the first instance, a threat to national defense? Do we agree that is what we are dealing with?

Ms. LAFLEUR. Yes, Senator.

The CHAIRMAN. Chairman?

Mr. GINGRICH. Yes.

Ambassador COOPER. Yes.

Ms. DURKOVICH. Yes.

Mr. MANNING. Yes.

Mr. WAILES. Yes.

The CHAIRMAN. Okay, we have agreement here.

Now the question is what we do with this?

I do appreciate the various suggestions that have been presented here and how we can work to protect, how we can become more resilient.

Speaker Gingrich, you mentioned the prospects for a broad infrastructure package and what we might be able to do in the context of national security. It begs the question, though, and you have indicated, Mr. Wailes and I think others have said, this is a tough order. There is really not a one-size-fits-all here. But is there commercialized technology the industry could use to protect against EMP attacks, and if not, what are the barriers to deploying the technology?

Cost has been mentioned, most specifically, but how prepared are we, if we were to get this infrastructure package? Do we have something that we could actually lay down there that could be constructive? I will let anybody jump on this one.

Mr. GINGRICH. Let me, if I can for a second, I want to make, sort of, a deeper point about where we're at.

We've done an extraordinarily elegant job operating off of a paradigm of efficiency to create an electric system for North America. It's really extraordinary.

You now have to shift from that model to a model that says you want resistance, redundancy and resilience. Then you have to create, first of all, just the model and that's why I said—part one of this is, at least in part, the Department of Energy and the Department of Homeland Security modeling what would that system look like.

It's not a situation where you get a choice, where you get to say, you know, I'm going to take the risk of being destroyed by cyber because I'm really going to focus on EMP. You've got to look at all the major threats, figure out what the notable points of defense are against all of them and then design a policy to fit that. And this will be the more expensive system. Then you've got to figure out what part of that more expensive system is a national defense requirement in which case it ought to be borne directly by the government. What part can you legitimately say we can find offsetting savings, as I mentioned earlier, just in cutting the red tape and the time, value and money you could save an enormous amount of resources that the industry would, I think, be happy to swap and put that money back into a more resilient system.

But I think you've also got to ask the question, I think there ought to be real urgency and cutting through all of this and setting very tight deadlines for implementation because I think we've known since 2004 that the Russians have given the North Koreans this capability. We've known since the 1990s that the Chinese have been developing this capability. And the capacity for a North Korean satellite to have an EMP weapon is a very real danger in real time, today.

So, I think we have to have, well, almost, a wartime urgency of setting this up, offsetting the cost and to your point, in some areas we don't currently have a solution and there are obvious significant research projects, DARPA and others, to be engaged in figuring out the specific breakthrough points, how are we going to solve these things? Because if we don't solve them there's a genuine catastrophe that could happen that would be of horrendous consequence.

The CHAIRMAN. Chairman LaFleur, and as you answer this I want to know whether you believe FERC has sufficient regulatory authority to address these EMP concerns and really, where we are with that, as you respond to this other point.

Ms. LAFLEUR. Thank you, Senator. I'll take the questions in turn.

So, your first question was is there technology available to protect against EMP? The answer is there is some technology available to protect some equipment against EMP. For example, the military sheaths some of its intelligence equipment in metal in some of its intelligence centers. So there is some technology available.

The difficulty on the electric grid is knowing where you would deploy the technology to best protect the grid in an effective way because when we are going to mandate a standard for thousands of transmission owners, we want to make sure it's going to work and it's going to do the job that it's intended to do.

Speaker Gingrich has referred to the study of the nine substations. I know that's a controversial study. I've testified about it here before. That was a study that was looking at simultaneous physical attacks on transformers and cascading of transformers, whether its results are right or not, that's what it was talking about.

If I were to go to protect the grid from EMP I'm not sure, I'm quite certain those nine substations, wherever they are, are not where I would go. I'd probably go to the control centers first because you can't even turn a substation on and off without the communications from a control center. Those are ubiquitous in every territory.

So we need to figure out, for this risk, which is different from a storm or a, even different from the risk we're protecting against with the physical security standard which was for the substations, where is the best place to go? That's the work Mr. Manning and others are doing.

To your second question, we do not have the authority, as you know, under the law to write a requirement ourselves and say everyone, you have to do this. We have been given a complex statute under which we oversee NERC in a voting protocol, and they file a standard. We can reject it if it's not strong enough and make

them change it. We can direct them to do a standard but it's a—that's the way the structure works.

Within that authority, we could certainly direct NERC and the industry to do a standard if we believed we knew what they should do. And I have every confidence they would respond as they have with GMD, physical security, supply chain management and other things where they opposed initially but when we directed it, they did a standard.

The CHAIRMAN. I appreciate that, thank you.

Senator Franken.

Senator FRANKEN. Thank you, Madam Chair.

In reading through the testimony provided for today's hearing, it became clear that some of the witnesses are quite alarmed about the threat of an EMP attack and the potential societal impacts and others are clearly more circumspect.

Chairman LaFleur, could you comment on where we should direct the efforts and resources we devote to enhancing grid security? What should our priorities be? Where would you place physical attacks which is on Metcalf, cyberattacks, EMPs, GMDs and other threats on a triage list?

Ms. LAFLEUR. Well, it's a difficult question because we're comparing attacks that are very numerous and kind of low barriers to entry, like cybersecurity when you don't have to be a nation-state. A lot of people can do it too, as several have said, high impact, low probability.

I mean, I think that, first of all, we have to have a strategy for all attacks. I think right now I would probably put cybersecurity as number one, but that doesn't mean we don't need to protect our substations from physical attacks or that we don't need to protect against solar storms, which we are protecting against, and work on the EMP issue and figure out how to protect that.

I think taking a step back, to me, where we should be going, the real solution, is to build resilience into the grid, to build the grid in a way that we have more redundancy, that we can island, that we have more inventories as we're working on because that works against all risks.

I think resilience, which is increasingly where our efforts are going, is the strategy that works, whether it's a hurricane or an earthquake or something else.

Senator FRANKEN. So when you are talking about island mode, making sure there are just, sort of, circuit breakers, the opposite of circuit breakers, just so that if one goes down, not everything goes down.

Ms. LAFLEUR. Well, you can't obviously, you can't have a backup for everything, but we have standards, for example, that critical control centers have to have backups, secondary supply lines and so forth.

In the geomagnetic disturbance standard, the first part of the standard we put out was an operating procedure standard. When we hear from NOAA that there's a solar storm coming within half an hour, there's an immediate transmission to every control center in the United States. And they have to know, okay, which—how do I go into safe mode? What do I do in the time that I have?

Now, we might have no warning of a bomb, but for GMD, that's precisely what they're working on.

Senator FRANKEN. Okay.

Mr. Wailes and Mr. Manning, can you give the perspective of those who work in the industry and daily face of the near end, long-term threats to the security reliability and resilience of our electrical system? Which threats do you believe we should prioritize?

Mr. WAILES. I actually concur with Chairman LaFleur. And we're looking at today's environment, we see the cybersecurity threat as a much higher threat. And we have a significant investment and a lot of work going toward that, as we speak.

But I would like to address, kind of, the perception that we don't have a lot of redundancy built into the system now. That is actually part of the core of reliability, again, is electric utility, reliability and low cost are our primary objectives, but reliability is the primary one.

So whether you're talking about, you know, transformer capacity to serve substations or you're talking about circuits, all of that is looking at that reliability is built into your generation fleet. When you look at how you plan against generation and reserves for different types of events, that is something we do routinely, but there are different things that we're looking at with current day threats that hadn't existed previously and how we're going to deal with those.

The research that EPRI is doing, the work we do, for example, with the ESCC. I think one of the striking things, many of you may have heard about the GridEx exercises which are really significant exercises that are developed between the Electric Subsector Coordinating Council, NERC and the ISAC, which is the electric sector Information Sharing and Analysis Center. They take a year and a half to develop these exercises, and they look at very catastrophic types of events.

Some of the learning out of that that we get between the Federal Government partners and the industry is more of an understanding of how much redundancy is in the system and some of the issues that we have to actually share information about how are we going to be more resilient and how are we going to respond. All of those things are an ongoing approach for us, on a continual basis.

The difference is those threats are changing. And that's one of the things we found, even with the EMP threat. And we all thought there was a cold war we didn't have to worry about that anymore, nor did we have, as pointed out in the opening comments, the kind of sensitive—we had analog devices. We didn't have devices that were as sensitive as we do today.

So as those threats have evolved, we have to get more understanding about how they impact what we do. And we also know that the easier threat now to us is a cybersecurity threat and the physical security threats.

Senator FRANKEN. I know I am way over.

Mr. Manning, would you respond to that briefly?

Mr. MANNING. Yes, Senator.

The first thing that came to my mind is that we like the information to make that decision, that we react, based off of our experi-

ences. So if we have a high probability of cyberattack, then we immediately respond to cyber issues.

We lack sufficient information to understanding exactly what the probability is and what the severity is of attacks like EMP. That information is becoming clearer and we're beginning to understand that. And once we have adequate information about EMP, then we can balance that sufficiently, I believe, with threats like cybersecurity where we have quite a bit of information.

Actually, I think we talked about it earlier that risk is really about managing probability and severity and we have to look at both of those things. Well, in the industry we can do absolutely nothing about probability of an EMP attack, so we're focusing all of our efforts on severity. And if we can reduce the consequences of an EMP attack to the point where the probability no longer matters, then I think, we've actually made progress.

Senator FRANKEN. I just want to make one last comment which is really a question.

Is this an argument for more distributed energy, more solar panels on rooftops, more island mode energy?

The CHAIRMAN. Let's go to Senator Cassidy.

We will leave that question hanging.

Senator FRANKEN. The hanging question.

Senator CASSIDY. I will start with Ms. LaFleur.

Madam Chair, the Hawaii outage after the atmospheric nuclear test, was that due to an E1, E2 or E3?

Ms. LAFLEUR. I believe it was due to E1. I believe it was communications equipment that was destroyed.

Senator CASSIDY. Mr. Manning, you all have looked at, you said, E3 and found it to be less consequential than a severe GMP. What I read in my notes is that E2s are more like lightning so it seems like E1 is, you said, not yet tested.

Now, again, just coming up to speed, what you already know. So that is communications. Would that also threaten the grid or no, would this be specific—more likely to affect communications?

Mr. MANNING. If I can circle back on that question.

Our findings on E3 are also partial. There is still additional work to be done on E3. We specifically investigated impact of bulk power transformers. We looked at the 37,000 or so bulk power transformers in the continental U.S. grid. As a result of only the E3 pulse, what we discovered is that the damage to those would likely be less severe than originally thought.

It has——

Senator CASSIDY. I only have three minutes.

You have got to hustle, man. I am sorry.

[Laughter.]

Mr. MANNING. It has a correlation to GMD, but it's not directly related to GMD; however, you can't stand that up on its own. It must be associated with the plethora of energy waves from a nuclear attack. So you must consider E1, E2, E3, all together, and we've only begun to consider that.

Senator CASSIDY. I got ya. So, whatever my questions about E1, it has to be considered within the context of E1, E2, E3, conglomerately.

Mr. MANNING. Absolutely, unless it's a handheld device which is only an E1 pulse.

Senator CASSIDY. Madam Chair, speaking of a geomagnetic, if I am getting all that right, what I quickly read about the Carrington event is that there was a 17.6-hour lead-in. They saw the flare, but the physical effect was not seen. And I read that in some places they actually unhooked their telegraph from the power source.

Typically you would have a several day lead-in. We see the flare. That said, is it possible if there is such a flare from the sun that everybody could go home and unplug their computers, put in their surge protectors and otherwise protect their equipment?

Ms. LAFLEUR. Well first of all, much more so than in 1859, our weather satellites give us good information, usually you know several days ahead something is coming, but the details of where it's going to go is more like in minutes or hours than days.

That's the purpose of the operating procedure standard that is communicated to the control centers so they can protect the high voltage transformers and so forth, which take a lot longer to replace which are the most impactful equipment on the system in many ways.

In theory, you could go protect your own equipment, but the solar storm doesn't have the same effect on communications. So, I don't think there's a lot of concern that it would destroy home electronics.

Senator CASSIDY. I guess I was using that as, kind of, a metaphor.

Ms. LAFLEUR. Yes. Electric companies could do things like that.

Senator CASSIDY. They could. So we do have some advance notice and we could take some protection?

Ms. LAFLEUR. That's why that was the first standard we put in place because you don't have to do equipment modifications. It's actually just planning of what you would do.

Even when I used to run a distribution company, even when we had hurricanes or snow storms coming, sometimes you configure your system in a different way to prepare because you know where your vulnerabilities are. It's similar, but bigger scale.

Senator CASSIDY. Now going back to the point that Senator Franken made that some of you were more sanguine and others less so. I read about a 1989 geomagnetic storm which only affected Quebec and maybe a few Australians over in Namibia, but as far as I know it didn't affect Louisiana. That said, it tells me that even though we were about this being global at first, at times we have these geomagnetic storms and it is local.

Ms. LAFLEUR. It depends on the size of the solar flare. One like a Carrington event is larger. Most of them are more regional. Our standard that's now in effect requires specific mitigation depending on the latitude and the soil and so forth.

Louisiana is a little closer to the equator. In general, the poles are—this is one—you have a lot of hurricane issues, but this particular problem closer to the poles is generally considered more exposed to solar radiation.

Senator CASSIDY. So my kind of sense from everything, what you're saying is that we really do have an understanding and some advance warning that someone said if we can prevent it, it's a lot

better, that at least with that which might come from the sun, granted it could overwhelm and the Speaker mentioned that.

Ms. LAFLEUR. Yes.

Senator CASSIDY. But still we are somewhat prepared for that from the solar.

Ms. LAFLEUR. Well, because we monitor all the time, some of the transformers have monitoring attached, they can get regular updates on what's happening with the sun and how it affects them. Fortunately we don't have a lot of experience monitoring explosives in the upper atmosphere. That's not the kind of monitoring experience we want to get. So, you can't develop the fact-based, experience-based information like with the sun.

Senator CASSIDY. Got it.

Thank you. I yield back.

The CHAIRMAN. Thank you.

Senator Wyden.

Senator WYDEN. Thank you, Madam Chair and thanks to all of our witnesses. This is a very, very hectic day. The Speaker knows a little bit about what those are like up here. I just have a couple of questions.

First, I want to note a point I am not sure has been made, and that is in the skinny budget the cuts that the Administration is looking at for agencies like NOAA and NASA is going to make it much tougher, much tougher, for the Congress on a bipartisan basis to deal with the important issues that we are talking about here today.

I think there is a real role for government to play as it relates to improving the resiliency of the grid, and those are the questions that I want to touch on with all of you. I will start, Mr. Manning, with you and Ms. Durkovich.

As you know, what we really are concerned about in our part of the world is the large earthquakes along the Cascadia Subduction Zone. This is a major, major issue for the people of the Pacific Northwest with respect to this whole issue of resiliency.

Now my take, with respect to the science, and it picks up on a point where, I think, Senator Franken was trying to go, is microgrids and distributed energy resources. And here we are talking about rooftop solar. Energy storage can play a very real role in helping the grid quickly recover if you get hit by an event like this.

So, for you, Mr. Manning, and you, Ms. Durkovich, could you just briefly walk the Committee through the role that these technologies could play in adding resiliency to the electric system when we are thinking about, in our part of the world, a physical threat like a Cascadia disaster?

For you, Mr. Manning, and you, Ms. Durkovich.

Mr. MANNING. So it's an excellent question, thank you, Senator.

There is no doubt that distributed energy that is grid connected introduces additional redundancy to the grid. As Kevin mentioned earlier, redundancy is a part of reliability. So the more redundancy we can add and couple into the grid, the greater potential we have for increasing reliability.

But it's not a failsafe. In the event of an earthquake, for example, distributed energy is probably an excellent solution to offer alternatives to centralized generation. In the event of an EMP, by

contrast, there's nothing that specifically protects those distributed energy resources any better than the centralized energy resources. So in the event of an EMP, you're likely to see the control systems for rooftop solar or for storage or for microgrids would also be impacted by that EMP. They would also be rendered ineffective unless they're hardened specifically for that. However, for weather events, for other events, even potentially cyber events, they add value because they add redundancy.

Senator WYDEN. Okay.

Ms. Durkovich?

Ms. DURKOVICH. Thank you.

That's really an excellent question. I think another example of how government and industry have come together to think about how we are going to address impacts to the grid from some of these lower probability, high impact events. In 2016, there was a major exercise called Cascadia Rising which focused on just this, the Cascadia Subduction Zone and the fact that, like a Carrington event, we are a little bit overdue for this scale of earthquake in the Pacific Northwest.

I would agree that certainly distributed energy can help speed restoration to the communities, but this is, again, another type of incident where we really need whole of community effort when you think about the potential damage and consequences that we're going to see in something like this.

And so, it is important for us to continue to do the large-scale exercises that bring together our state and local's industry and government to help us think about, alright, what are the impacts going to be to the grid? What are the impacts going to be to communications? To transportation? How are we going to get basic commodities into this area? How are we going to make sure first responders can get in and equally important the utility and the linesmen, to help get the systems up and running?

So this is not an easy challenge, but it's why we bring folks together to think through, alright, what are we dealing with and how are we going to speed recovery?

Senator WYDEN. Very good. Thank you all.

The CHAIRMAN. Thank you, Senator Wyden.

Senator Risch.

Senator RISCH. Thank you, Madam Chairman. Thank you for holding this hearing.

We have heard a lot of criticism, or at least concern this morning, about the government's response to the growing threat of grid security and to cybersecurity. In large part, I think, there is certainly criticism to be had and certainly a lot of concern to be had.

Part of it, I think, has grown out of frustration that, I think, there isn't a lot out there about what the government is doing. I sit on the Intelligence Committee, Senator King sits on the Intelligence Committee and Senator Wyden sits on the Intelligence Committee. I can tell you that these issues have not been ignored by the United States. Most of what we know about it, most of what we are doing about it, cannot be discussed in this setting. It is going to be a closed setting, only for people with the security clearance necessary.

So, in that regard, it isn't quite as bad as what everybody is saying. But Speaker Gingrich, your deep insights into the consequences are greatly appreciated. We have been through these exercises and your statements are certainly not overstated.

I would take issue though, as far as your recommendation, if we have an infrastructure bill coming. I can tell you based on what we know about where we are and what we are doing, I think that is appropriate at some point in time, but we are not ready yet.

You saw what happened when they had this last $2 trillion, whatever it was, bill to stimulate. When you start throwing money at the wall a lot of it doesn't stick, and the term "shovel ready" was used a lot. We are really not ready. We do not have shovel ready products yet. Certainly, we need more research and that could be included in that, but I would just be a little reluctant to start digging and laying stuff in the ground at this point.

But there are things going on on this, and I think a lot of us on the Intel Committee are convinced that the next significant events in America are going to be a cyber event. That is where we have vulnerability. But certainly the grid is linked to that. And the bad guys, of course, Senator Franken had asked which was more, what is the most concerning right now? Well, we have to be able to walk and chew gum at the same time because, as we sit here today, there are different people working on different ways to attack us. And these are all included in that, whether it be North Korea trying to develop a weapon to drop on us or whether it be other state actors and non-state actors who are trying to get us through the grid and through the cybersecurity.

Ms. LaFleur, thank you for the shout out today at our National Laboratory. Obviously, we are becoming, in Idaho, the go-to and the flagship on grid security. You saw the test bed that we have out there and the kinds of things that we are doing there on grid security, working with private industry. I think most Americans would be very pleased to see what is going on out there and the kinds of things that we are doing to try to mitigate them as we go into the future.

In any event, we are going to continue to work on this. I think it is important. I really appreciated Ms. Durkovich and Mr. Wailes' description of risk management because, you know, after you sit here for a while today, you realize the threats to America, how many there are and how diverse they are and the widespread places that they come from.

There are a lot of people out there that just, for their own reasons, want to do us harm. And yes, we have to be able to walk and chew gum at the same time. Yes, we have to be able to address all those threats. But you have got to do it on a risk management basis because there isn't enough money in the world to protect us 100 percent, whether it be the grid or whether it be the cybersecurity or just a normal kinetic attack.

There was frustration, I think, expressed for the Department of Defense. We work with the Department of Defense, the Intel community works with the Department of Defense all the time, and I think that criticism is probably pretty well taken. I say this with great love and respect for the Defense community, but they are much more focused on the classical kind of warfare and the clas-

sical kind of defense that has always been and we have always challenged them to provide for America.

These new things that are coming along, like cyber and grid and what have you, have not been in the wheelhouse. They are getting up to speed but so is the electrical industry and everything else.

Probably one of the most telling things we hear in the Intel community is when we have these experts in on the grid and everything and I think this, kind of, put it in perspective for me. When you work on these problems and you try to predict what is going to happen and then try to design a defense to it, these people will tell you, when it comes to cybersecurity we are where the Wright Brothers were. We don't know what we don't know. And we keep learning things.

A good example of that as Speaker Gingrich very rightly pointed out is the fact that all of this stuff is designed for efficiency. Well, when you design it for efficiency, you design in huge vulnerabilities.

The Ukrainian attack taught us something. In fact, some legislation came out of that, and that is that the Ukrainian attack was not as bad as what it could have been because their system was not very efficient. It actually had to go through human beings. And when it got to these human beings, the human beings recognized what was going on and they were able to mitigate that.

Senator King and I are co-authors of——

Senator KING. S. 79.

Senator RISCH. S. 79. Thank you, Senator.

We call it the back to the future bill where you actually back up and start to look at these efficiencies and see if there are some places where we can put in some of these kinds of things.

Anyway, I have talked long enough. Again, this is an incredibly important hearing, incredibly important subject. Thank you for holding it, Madam Chair.

The CHAIRMAN. We appreciate that input, Senator Risch.

Senator King, now you can speak to your bill here.

Senator KING. Thank you.

First, I want to welcome Speaker Gingrich. It is always a pleasure to have your wisdom and insights. I still remember very well a day we spent in Maine when we were lonely voices talking about digital education back in about 2000, so I appreciate that.

Mr. Manning, and I think this gets a little bit to where we have been focusing today, we were talking about distributed energy and you appropriately said that could be a part of the redundancy and defense. Unless they are hardened, you said. That is my question. Are there reasonably priced, hardening tools out there? In other words, could we build in to every house, as part of the electrical system, some kind of high test surge protector that would be a defense in this situation? And by the same token, a similar kind of device in the grid back at transmission points?

Mr. MANNING. That's a wonderful question.

I think the answer to that is there could be. Today, it's probably not, as we just heard, is not shovel ready. There are a lot of different components that need to be added together. But this will take a fundamental design change, in some respects, particularly

for home-based equipment. You'll have to think about it differently and make just complete design changes——

Senator KING. Are the utilities thinking about this for their critical points? In other words, to me this is an insurance question.

Mr. MANNING. Yes.

Senator KING. How much is the insurance policy going to cost versus the risk?

Mr. MANNING. And one of the things that we are doing with our report which will be out this summer is taking the military EMP standards and converting those to utility standards.

What we will find is that applying those utilities, those military standards to utilities broadly, will be prohibitively expensive. It's very difficult, it's very challenging, it's hard to do and it's very expensive.

So utilities may still choose, as we've heard already, they may choose to pick perhaps nine points or something like that and harden those points with military standards. But it won't be practical to support the whole system until we develop some more effective and lower cost alternatives.

Senator KING. It seems to me this is a place for American ingenuity and inventiveness and creativity to market for somebody.

Mr. MANNING. Absolutely.

Senator KING. An important market for homes as well as for the grid itself.

The bill that Senator Risch mentioned mandates a study. I should not have used the word mandate, suggest a study involving Idaho National Lab and several volunteer utilities on the possible importance of putting at certain points in the grid, analog devices, which is what saved the grid in Ukraine and that is exactly what we are trying to do. It is a bill that came out of our work on the Intelligence Committee, both of us are also on this Committee. And it is a great bill, Madam Chair.

But I think, Mr. Speaker, you have done a lot of thinking about this. We cannot defend ourselves. We cannot install defenses that are so expensive that they far outweigh the risk. How do we get products that can solve the problem?

Mr. GINGRICH. Well, let me use this as an excuse to make three quick points, ending on that one, okay?

Senator KING. Fine.

Mr. GINGRICH. First, every member of Congress already got briefed on the concept of hybrid warfare, what you're seeing in Ukraine.

Senator KING. Yes.

Mr. GINGRICH. Because it's what makes the whole panoply of risks come together simultaneously. You don't know——

Senator KING. We are seeing warfare change before our eyes.

Mr. GINGRICH. That's right.

And just as I talked about the paradigm change earlier, from efficiency to looking at resistance, resilience and redundancy, we have to rethink from the ground up what we mean and what the military means and what Homeland Security means.

Two, if I walked in here and said to you, you know, I've been thinking about how we run our cities and I can't decide whether we've got to cut out food inspection in the restaurant, the sewer,

the fire department or the police. Which one do you think we should drop? Because that's what we're doing right now in terms of this. If we had no choice as we rethink our infrastructure but to look at the totality of potential disasters and decide are we going to figure out a design that meets the totality. See, you can't say let's set priorities because the one you don't pick may be the one that kills you.

Senator KING. Sure.

Mr. GINGRICH. Lastly, there's a terrific book. I just did my newsletter yesterday. I very seldom do book reviews in my newsletter but it's called, "The Weapon Wizards." I recommend it. I'd like to get every member of Congress to read it. It is the Israeli capacity to innovate and how dramatically they've done it and they're really cheap, okay?

One of the things that I hope Trump is going to bring to the Pentagon, which would, as a Conservative, I'd like to see reduced from a Pentagon to a triangle by eliminating 40 percent of its redundancies.

[Laughter.]

But I mean this quite seriously.

We start out and we say, since we have to design an absurdly expensive, over-engineered obsolete model based on work done in 1963, if you applied that to the grid you couldn't afford it. To which the correct answer is, well, what if you went out and asked every smart, young person in America to come up with a $9 version that could be sold on Amazon?

Senator KING. Exactly.

You would be interested to know that we have had testimony at the Armed Services Committee in the last couple of months that Silicon Valley basically will not deal with the Pentagon because it is so, I would call it byzantine, but that would be an insult to the Byzantium empire.

[Laughter.]

Because it is so burdensome and cumbersome, and we are losing the innovation race.

Mr. GINGRICH. And at least half of that is the Congress which imposes patterns that are so stunningly stupid that if the Congress would look at the things it has passed into law in the past 40 years and get rid of half of that and then challenge the Pentagon bureaucracy to get rid of the other half, you'd be startled a year from now how rapidly we'd be innovating and how cheap it would be.

Senator KING. I am shocked you would use the words stupid and Congress in the same sentence, Mr. Speaker.

[Laughter.]

Mr. GINGRICH. I apologize.

Senator KING. Thank you, Madam Chair.

The CHAIRMAN. Thank you.

Senator Manchin.

Senator MANCHIN. Very quickly, thank all of you for being here, we appreciate it very much. Speaker Gingrich, it is always good to have you here.

Chairman LaFleur, first of all, anybody can answer this and if you have any comment to it, but the likelihood of the EMP attacks, the likelihood of where we are most vulnerable. I came in a little

bit late because, as you know, in this place we have competing committee meetings. But is it basically from a weapon from another country or is it basically going to be home grown to do damage to the delivery system? Where do you think we are the most vulnerable? Or what are you concerned about in vulnerability?

Ms. LAFLEUR. Well, the so-called suitcase EMP.

Senator MANCHIN. Yes.

Ms. LAFLEUR. A handheld device is, obviously, much easier to build than a bomb, but it's also easier to protect against. I think some of the these we're doing, we do know how to put fences on substations and cameras and perimeter zones if you have to throw something in somewhere, we know how to protect that. So I think that's more likely, but easier, to protect against.

Senator MANCHIN. You are requiring that because I can tell you we have an awful lot of power generating in West Virginia.

Ms. LAFLEUR. Excuse me?

Senator MANCHIN. We have a lot of power generating in West Virginia.

Ms. LAFLEUR. Yes.

Senator MANCHIN. And we light up most of the East Coast which they do not know about.

Ms. LAFLEUR. Yes.

Senator MANCHIN. If we ever turn the coal off, they would go dark. Maybe we should do that.

Anyway, the substations, I have seen substations that are very vulnerable. Are you requiring them to basically solidify that and protect?

Ms. LAFLEUR. What the physical security standard did was required each company, each transmission operator or owner to identify their most critical substations and come up with a specific plan to mitigate against physical attack.

Senator MANCHIN. Do you have anybody that inspects it?

Ms. LAFLEUR. Excuse me?

Senator MANCHIN. Does anybody inspect it?

Ms. LAFLEUR. Yes, we are inspecting and NERC does the first audit and FERC——

Senator MANCHIN. Well, if I see some vulnerable situations I can call you?

Ms. LAFLEUR. Yes.

[Laughter.]

Always.

But the—so that's that thing. I think the high-altitude HEMP——

Senator MANCHIN. Yes.

Ms. LAFLEUR. The high-altitude EMP is, I don't remember the adjective you used in your question, troubling because we, unlike the smaller, we don't know——

Senator MANCHIN. I understand.

Ms. LAFLEUR. The most—way to protect it.

Senator MANCHIN. You had something, right? Ambassador?

Ambassador COOPER. Yes, I don't know how to put a probability statement on but let me give you a couple of facts.

In 2004, several Russian generals who were experts in EMP, and I would note that they did more effective tests on this effect over

populated areas, in fact, in the '62, '63 timeframe than we did. They learned more about it than we did.

They told the commissioners, the EMP Commissioners, that they had passed, inadvertently, I think they said, but the information on how to design a super EMP weapon that is a low-yield device that produces lots of gamma rays.

Senator MANCHIN. At a high altitude?

Ambassador COOPER. High altitude, to the North Koreans, okay, who in turn, as you know, worked in a direct alliance with Iran on everything.

North Korea, by most estimates, has already anywhere from 10 to 20 nuclear weapons. We take comfort in the fact that there have been low-yield tests in North Korea.

Well low yield is what you use to produce a super EMP weapon, and they allege that they can launch this. They don't allege, a lot of experts I know claim that they can launch this, as Speaker Gingrich said, or put it in a satellite which comes toward the United States from our south, our undefended south, okay? We have no defense against that nor do we have a defense against missiles launched from ships in the Gulf of Mexico.

We have not put our—we know how to do it. This is not a matter of ignorance. And actually it's not a matter of cost either, which I'd be happy to defend another time, but we know how to do it. We just simply are not doing it. We're deploying what's called Aegis Ashore, and I'm proud of that system because I started it, you know, when I was running the SDI program. It's deployed around the world on our ships, it's deployed on the ground in Romania and will be operational in Poland by the end of the year. We have an operational site in Hawaii.

We ought to put a site in Panama City on First Air Force base at Tyndall Air Force base where First Air Force has the responsibility of the defense of the United States, give them a missile defense mission too.

Senator MANCHIN. Do you mind if we bring in——

Ambassador COOPER. We know how to do this.

Senator MANCHIN. Do you mind if we bring you to the Intel, a little Intel briefing?

Ambassador COOPER. I beg your pardon?

Senator MANCHIN. The Intel Committee for a little briefing, would you come?

Ambassador COOPER. I certainly would. I have my clearances still, by the way, so I wouldn't mind transferring them in.

Senator MANCHIN. That is great.

Ms. LaFleur, if I may, while I have got you, just real quick.

The vulnerability basically is reliability of the grid system. Do you feel comfortable of the system of this grid when the vortex almost, the polar vortex, about took us down that one time? I mean, where are we today, right now, in your evaluation, with the amount of diversity we have going into the grid, as far as electricity sources?

Ms. LAFLEUR. Well, today we still have quite a bit of fuel diversity. Coal, as you already referred to, plays a very important role in baseload in most parts of the country. And we have increasing

natural gas and increasing renewables. And the system operators are learning to run——

Senator MANCHIN. Do you consider gas as being a baseload?

Ms. LAFLEUR. It depends. Some, the big combined cycle, some of them are run as baseload run all the time and then there's also——

Senator MANCHIN. But are you concerned?

I am just saying from the reliability, baseload, to me, means uninterruptable power. Coal and nuclear base are uninterruptable. They have what they have. Gas is a pipeline delivery system that can be targeted by terrorists or any other type of a natural disaster. But you are building, we are building baseload of something that could be interrupted. Is that correct?

Ms. LAFLEUR. It's correct that to the extent we rely on gas, we have to build in fuel security that's different than the fuel security of coal which you can look out and see the pile.

Senator MANCHIN. Sure, absolutely.

What is your feeling of comfort on the reliability of the grid?

Ms. LAFLEUR. I think most parts of the United States are well supplied with gas pipelines but we have places where there are constraints and I think operating the grid with all the new technologies is something we're still working on.

Senator MANCHIN. Does anybody have anything else they would like to add?

Ambassador COOPER. Yes, Senator.

We've talked about E1, E2, E3. E1 is the high frequency, high amplitude, narrow pulse that causes damage to solid state electronics.

Our natural gas pipelines, portions of the grid itself and petroleum pipelines, probably are controlled with little units called SCADAs, little, small computers that are vulnerable if we haven't taken special precautions to harden them. And my information is we haven't. So, we have critical infrastructure to the operation of the, of all of our grid to these kinds of effects from nuclear, high-altitude explosions. And as I said earlier, I don't know how to put a probability statement on it, but I can tell you the threat is absolutely real.

I've worked on these problems for most of that half century since we began seriously improving our strategic systems to deal with it, and we set priorities in the Department of Defense. We didn't try to harden everything. We hardened what we thought was the most important things.

In my opinion, in the grid, we should be paying careful attention to our nuclear power plants to make sure they aren't a hazard if their grid goes down and they have to shut down—we don't want Fukushimas all over the place. So we need to make sure we have power to those, just to keep them safe and then to bring them back up to help support——

Senator MANCHIN. I want to thank all of you. I appreciate it very much. Thank you.

Ambassador COOPER. Thank you.

The CHAIRMAN. Thank you, Senator Manchin.

There has been discussion here about what we see out of Israel with their level of innovation. Ambassador Cooper, you have referred to other initiatives around the globe, but in terms of what

other countries are doing specifically to address a HEMP or other EMP-related event. Is anybody, kind of, leading the way here? Are there best practices that we might want to be looking to? Who is doing some good things?

Ambassador COOPER. The Israelis, the United Kingdom, I would go talk to those folks. We have international conferences every year——

The CHAIRMAN. To what extent do we cooperate with them then?

Ambassador COOPER. We meet with them.

There's a big difference though, their government tends to control what's going on.

The CHAIRMAN. Right.

Ambassador COOPER. Whereas in this country, as I said to you earlier, we have a crazy quilt of electric power companies across the nation. Why, I believe, we have to work from the bottom up and island, that term we've used here, around our nuclear power plants, keep them safe, bring them back online. We get 20 percent of the nation's electricity from those plants. And so, that's a valid resource if we lose the entire grid.

Today, I don't have confidence that we can do that because we don't have these crazy quilt components connected. So, we have a serious problem here, and we have been ignoring it collectively. I'm not trying to point fingers at anybody, but that's the reality.

The CHAIRMAN. Chairman?

Ms. LAFLEUR. Thank you for the question.

We have Memoranda of Understanding with Israel, Norway and some other countries, the U.K., to work on these things.

I would say, in the solar storm area, Scandinavia, is probably, the Scandinavian countries are doing the most. Obviously, their location would justify it and——

The CHAIRMAN. Well, the United States actually has a location up there too.

Ms. LAFLEUR. Yes, that is correct.

The CHAIRMAN. It's called Alaska.

[Laughter.]

Ms. LAFLEUR. My feelings exactly.

Ambassador COOPER. She noticed that.

[Laughter.]

Ms. LAFLEUR. That's why GMD has really been one of my biggest priorities, my feelings exactly.

On the grid security defense area thing, I would agree with the Ambassador that Israel, the entire Israeli grid is—it's just a different society in the way things are run. We have a much more open society in terms of how our infrastructure is designed and set up, I mean, and so, I think, in security Israel is probably leading.

The CHAIRMAN. Let me leave you with one question. Again, I am going to allow anybody to step in here. Ambassador, you mentioned this crazy patchwork that is out there. Some have mentioned the imperative of public/private partnership, but in order to have a public/private partnership there has to be a little bit of trust there, there has to be a willingness to share some information.

In fairness, I think we have seen some instances where information gets out there and you get burned in the media. Probably the most current example is what happened in December in Vermont.

As I understand it, Burlington noticed an alert about a suspicious IP address that had connected to one of their computers. They responded, reported. The next day, the Washington Post somehow learns about it. Then you have reports about Russian hackers infiltrating. Later follow-up shows that the IP address was not necessarily linked to Russia. It was not necessarily malicious activity. But you really have eroded any trust that may have been out there.

So how do we do a better job of this? How do we work to restore this level of trust and build a relationship that is going to be necessary in order to really address this?

Mr. Wailes?

Mr. WAILES. Well, I think that we have a perfect example of that of the relationship that the industry has built with the Electric Subsector Coordinating Council, the Department of Energy and the Department of Homeland Security.

There is no doubt that that was a significant issue and a learning experience for everyone. But I think that one of the things that needs to also be taken away is that proves the effectiveness of getting that information out because information came out, you know, here's some suspicious IPs that you need to look for, report to us right away. And that function worked. Now was there a communication issue and a potential issue associated with that, yes, and I think we're working on fixing that like we are lots of other issues between us.

The relationship, I think, between the industry, actually within the industry and within the industry and the Federal Government is stronger than it's ever been, recognizing we have a lot of common issues and we need each other's help in order to make the nation stronger. And I think we're doing a good job of that.

We have a long ways to go. There are a lot of threats, a lot of issues. But there are just so many examples of how that working relationship has worked. And I think, when we talk about that, one of the things we should even think about is five years ago you did not have a lot of security clearances in the industry. And now, thanks to DOE and DHS, even a utility our size has six or seven people that would have security clearances. We're able to do things they could never do before, and we're able to share information that we couldn't do before. So it's a learning experience. We all understand the communication challenges, and I think we're on the way to, at least for our sector, to do that.

Now, we also are very interested in trying to build a stronger relationship with those other connected sectors that have issues and trying to make sure that we actually look at cross sector coordination, such that the other critical sectors, along with the electricity sector, actually can have that same functionality with the government.

The CHAIRMAN. Well, I am encouraged to hear you say that you think things are getting better in terms of providing that level of security clearance because we had a hearing, not more than six weeks ago, where that issue was raised about the frustration with how long it actually took and it was actually a former member who was the former head of the Intelligence Committee on the House side and was still having trouble getting his clearance.

Mr. WAILES. I don't know what the current process is, but the number of people from years ago that we got in, through that process, was much higher than through that.

The CHAIRMAN. Yes.

Ms. Durkovich?

Ms. DURKOVICH. Yes, an excellent question.

And while the incident that you referred to is unfortunate, I would say, overall, the trust that has been established between government and industry in the partnership is stronger than it's ever been.

Kevin alluded to many of the activities that we have underway. In my former position I actually ran the private sector clearance program which is the program that provides clearances to infrastructure owners and operators who have the need to know. When I left, I think there were roughly about 3,000 owners and operators that had clearances.

Clearly what happened at OPM has slowed the ability for us to provide those clearances in a timely manner. But I think that those timelines are clearing up and those clearances, as well as many other authorities that Congress granted DHS, and that's everything from the protected, critical infrastructure information program to the critical infrastructure partnership advisory committee which allows us to both share information, to ask for vulnerability information from owners and operators to protect it from regulatory purposes from state sunshine laws, from FOIA.

So we can take that information, we can investigate, we can do forensics, we can anonymize and we can push it out. Industry is one key part of how we share information.

As part of the Electric Sector Coordinating Council and all of the other sector coordinating councils, we bring industry in on a regular basis to provide them with threat briefings, with classified briefings, to help them understand this complex risk environment. We can have conversations that are not available to the public about what we should be doing to protect our infrastructure. And the list really goes on.

But I think, there's two important points that I want to end with is one, better understanding the intersection of these critical lifelines and the vulnerabilities caused by them and how we can continue to ensure and have plans in place to mitigate cascading impacts in the event of some of the incidents that we've been talking about. And then, I think, the second piece of this is as we begin to modernize our infrastructure and we begin to move to smart cities, I cannot underscore the importance of baking security in at the beginning. You need the security people sitting next to the coders, the architects and the builders. It is imperative. Security is the new normal.

It will be a differentiator. It will be a differentiator for companies. It will be a differentiator for utilities. It will be a differentiator for cities. And it has to be one of the core principles as we go about modernizing our infrastructure.

So, thank you.

The CHAIRMAN. Good.

Ambassador Cooper, why don't you wrap up, please?

Ambassador COOPER. Okay. Thank you, Madam Chair.

I just wanted to comment on this last discussion about security. I think someone needs to do a serious look at the levels of security that is inhibiting this kind of open discussion of what the environments are that the industry has to design against as well as other factors.

I don't believe that there is an absence of technology to deal with the EMP issue in an affordable way.

And I want for your peripheral vision to just make one more point. I absolutely agree with you about the need for trust between the people and the parties that have to deal with this issue which is why I gave up on trying to get institutions here in Washington and even in the states, to deal with this issue. Lots of folks have tried, are trying, and are frustrated by the issues that you've mentioned. That's why I'm working very closely on an individual level with key people and when I say local, I mean, in three counties right now, and we're going to couple into the NERC exercise this November, the GridEx exercise as well, to expand our lessons learned upward in South and North Carolina and we'll go elsewhere.

I think that we have to wake up to the sense of priority of dealing with the issues. The EMP Commission has looked at the briefings that some of the folks at this table have given. It is their assessment that they're underestimating the threat, even for the solar threat. The magnitude of the E3 component for a nuclear device is larger than for the solar event. So, if we harden the grid for a solar threat, we will still leave ourselves vulnerable for the other.

And in addition, you have E1 as a component that threatens the solid state electronics throughout our grid and that includes the distribution systems for petroleum and natural gas. So, we need to deal with this issue in a very, I believe, direct way.

I think that we have hope that what we're doing to accomplish locally. And when I say island, I want to build an island around Duke's nuclear plant and its hydroelectric plant and coal plant all on that lake so that the local people are engaged in working the problem. And by the local people I mean the, you know, the mayor, the city council at the political level, but Joe Sixpack, who understands what we're doing through the National Guard and so on.

Our—general is an electrical engineer graduate of Georgia Tech. He understands these issues and he is committed to try to work with us and we'll expand outward from there to other states and other locations. I believe that's the way we have to go to really build trust among the key players that are required to cut across the patchwork, quilt patchwork, that I tried to describe to illustrate earlier.

And that's not to argue against initiatives at the state level or the federal level or so on. At least that raises consciousness about the nature of this threat.

But my concern is the devil is in the details. And we learned hard lessons in the Department of Defense, that it's not just having the right design. It's not just having the right deployment, and it's not even just having an operational concept that's important. If you don't test it, I don't believe it. And we learned through hard experience that maintenance and that sort of operations of operational

systems that were well designed and deployed, we create holes by which EMP can get through.

So this is a hard problem. We have to choose where we work carefully and protect what we need to work to ensure the viability of the grid and for the American people.

The CHAIRMAN. Well, ladies and gentlemen, thank you. I think the testimony this morning, the questions and responses back and forth, have been very helpful. I think this has been a great discussion.

I appreciate some of the suggestions that we have, but I also appreciate the urging that we really not let our guard down, recognizing that this is complicated, multifaceted and it requires an attention to it that is really daunting. But just because it is daunting does not mean that we should not be working with you, with our agencies, with the sector, really across the country.

I appreciate what you have said, Ambassador Cooper, about really starting out very local and understanding the implications, not just those that are tasked on the day-to-day, but helping to educate Americans about our vulnerability and what we can do to reduce that.

It is always important here in Congress that we be reminded of the urgency and the imperative of our task, and I think we were given that message this morning.

I thank you all for your contributions.

With that, the Committee stands adjourned.

[Whereupon, at 11:57 a.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

QUESTIONS FOR ACTING CHAIRMAN LAFLEUR
05.04.17 Committee on Energy and Natural Resources

FROM CHAIRMAN MURKOWSKI

1. **Not all entities that operate on the bulk power grid have access to guaranteed cost recovery through regulated rates, e.g., independent power producers. Would there be a means for cost recovery for these competitive entities who are ineligible for rate recovery ensuring we do not place a costly anti-competitive mandate upon them? What would those be: reimbursement fund, tax deductions?**

Response

A number of entities hold market-based rate authorization from FERC, allowing them to sell power at market-based, rather than cost-based, rates. Entities with market-based rate authority have the opportunity to recover their costs, including costs for compliance with Reliability Standards requirements, whether through individually negotiated power purchase contracts or through offers to sell into wholesale energy and capacity markets. The market rules and tariffs governing the offers to sell do not preclude sellers from reflecting costs of compliance with Reliability Standards in their offers.

2. **Ambassador Cooper has testified about work he is doing in South Carolina with Duke Energy, and I am told that American Electric Power recently testified in the Texas Senate about work it has underway in that State to reduce the vulnerability of the power system in that State to EMPs.**

    a. **Can you comment on this kind of voluntary effort by industry?**

Response

Voluntary efforts to improve grid reliability and resilience can provide protection beyond the requirements of mandatory reliability standards. With regard to electromagnetic pulse (EMP), a number of utilities are proceeding with various activities to voluntarily study and implement EMP mitigation methods. FERC has offered members of industry assistance with these voluntary efforts. Our collaboration with industry can include threat information sharing, assessment of best practices and their applicability, and assistance with implementation of mitigation measures. This work complements the mandatory reliability standards adopted pursuant to section 215 of the Federal Power Act that provide a good foundation for protecting the Bulk-Power System.

QUESTIONS FOR ACTING CHAIRMAN LAFLEUR
05.04.17 Committee on Energy and Natural Resources

b. Can you foresee the conditions in which cost recovery for scaled-up efforts of this type might be appropriate in rates for FERC-jurisdictional transmission service? And if so, could you speculate about the potential benefits and necessary cautions about such an approach?

Response

As a general matter, utilities may recover prudently-incurred costs in support of grid reliability efforts. With respect to costs associated with mandatory reliability standards, section 219(b)(4) of the Federal Power Act (FPA) specifically allows for recovery of "all prudently incurred costs necessary to comply with mandatory reliability standards issued pursuant to section 215 [of the FPA]." The statutory language is incorporated into FERC's regulations at 18 C.F.R. § 35.35(f), which further states that the proposed rates must also be just and reasonable and not unduly discriminatory or preferential. Formula rates, which allow for a streamlined process for utilities to obtain cost recovery, are one option available to industry. Individual utilities may decide whether to use formula rates or some other rate recovery mechanism.

In rulemakings approving Reliability Standards proposed by the North American Electric Reliability Corporation (NERC), FERC has indicated that cost recovery for compliance with mandatory Reliability Standards may be available. For example, in Order No. 830, in which FERC approved the second-stage Reliability Standard addressing geomagnetic disturbances (GMDs), FERC indicated that recovery for prudent costs associated with or incurred to comply with the Reliability Standard and future revisions to the Reliability Standard will be available to registered entities. In that case, cost recovery would be available for costs incurred to mitigate assessed vulnerabilities to a benchmark GMD event. As the phrase "prudently incurred costs" suggests, allowing for cost recovery to offset the costs of compliance with mandatory Reliability Standards must be balanced against the risk of allowing for recovery of costs unrelated or unnecessary to compliance with Reliability Standards.

FERC has also taken steps to address cost recovery for reliability investments outside of the NERC Reliability Standard context. In the wake of the September 11, 2001 attacks, FERC issued a policy statement on September 14, 2001 indicating that FERC "will approve applications to recover prudently incurred costs necessary to further safeguard the reliability and security of our energy supply infrastructure in response to the heightened state of alert." FERC affirmed and clarified that policy in a subsequent policy statement issued on April 19, 2004. Furthermore, FERC has issued orders to provide rate clarity and certainty

concerning efforts to ensure adequate inventories of critical grid infrastructure, like high-voltage transformers.

3. **One of the keys to a successful public-private partnership is trust and the willingness to share information. I am concerned, however, that there is a lack of trust by industry with the government – and for good reason. The December 2016 episode with Burlington Electric in Vermont is a perfect example. As I understand it, Burlington noticed an alert about a suspicious IP address that had connected to one of their computers and responded to that alert by dutifully reporting that fact to the government. The same day that they reported the alert, however, the Washington Post somehow learned about it and reported that Russian hackers had infiltrated the United States' electric grid. Later follow-up would show that the IP address was not necessarily linked to Russia and there was not malicious activity, but the damage to trust had been done. How do we restore and build trust between the private sector and government so that this type of information can be freely shared without concern about it becoming a media spectacle?**

Response

I agree that trust between the private and public sectors is critically important to information sharing efforts that support grid reliability. As part of its work with industry and other stakeholders, FERC conducts analysis and outreach to share threat information and best practices for defensive measures to help mitigate risk to FERC jurisdictional infrastructure. This collaborative approach facilitates open communication with industry representatives. The staff members that engage in this collaboration protect industry-generated information using, as appropriate, FERC's Critical Energy/Electric Infrastructure Information (CEII) program Non-Disclosure Agreements, Transportation Safety Administration's Security Sensitive Information (SSI) program, Department of Homeland Security's (DHS) Protected Critical Infrastructure Information (PCII) program, and other protection measures.

4. **EMP models are only as good as the data inputs provided. The United States has not tested any nuclear weapons since 1992, and no atmospheric tests since the Test Ban Treaty of 1963. My understanding is that many of our weapon designs have required post-deployment tests to resolve problems – and those problems were discovered only because of ongoing nuclear tests at the time. In each case, the weapons were thought to be reliable and thoroughly tested. How confident are you that the data being inputted into the models**

QUESTIONS FOR ACTING CHAIRMAN LAFLEUR
05.04.17 Committee on Energy and Natural Resources

with regard to the EMP effects of a nuclear weapon detonation is accurate – particularly since we have not conducted an atmospheric test since 1962?

Response

I cannot comment on the accuracy of this data. As a general matter, however, to get the most accurate modeling results, the most up-to-date information should be used as input for the models.

a. Since most of the data is controlled by the Department of Defense and the National Labs, does the private sector have access to the data needed to accurately model the potential EMP impact and effect of a nuclear explosion?

Response

FERC does not have information as to which private sector entities have access to the data needed to accurately model the potential EMP impact and effect of a nuclear explosion. This data is highly sensitive and access to it is controlled by other federal entities such as the Department of Energy and Department of Defense.

b. My understanding is that most HEMP models are based on a one dimensional, spherically symmetric model, neglect scattering effects, and are unable to model 2- and 3-D effects. There is also no high-fidelity model that predicts EMP from detonations from 5 kilometers to 20 kilometers above the Earth's surface. Given these shortfalls, how confident are you in the accuracy of current EMP models?

Response

I cannot comment on the accuracy of these models. As a general matter, however, in order to ensure accuracy, it is important for models to be as complete as possible and to include the relevant known effects.

FROM SENATOR STABENOW

1. **A primary component of today's hearing is our homeland defense strategies against foreign states and terrorists, including missile**

defense and others. For good reason, I presume much of this information is classified. However, can you speak further to FERC's coordination with the Department of Defense, Department of Homeland Security, and other national security entities when it comes to sharing information and assessing the risks associated with EMP attacks?

Response

FERC works closely with our federal partners as well as the appropriate stakeholders to better understand the risks and impacts associated with EMP on energy infrastructure. These efforts include working closely with federal agencies, state partners, and industry to provide classified and unclassified threat briefings, assisting with the development and identification of best practices for mitigation, and assisting with implementation efforts.

2. **During today's testimony, we heard that EMPs are a threat to our national security. However, the range of impacts appear vast, from naturally occurring events causing grid disruptions, up to - and including - the aftermath of a high altitude nuclear detonation. This Committee has held several hearings in this and previous congresses on the threats facing our electric grid and critical energy infrastructure. From your perspective, how does the threat posed from EMPs compare to other vulnerabilities such as cyber-attacks?**

Response

Effective protection of the Bulk-Power System requires that we address both events that occur regularly, such as attempted cyber incursion, and high-impact, low-frequency events that can disrupt reliability. Protection efforts include both targeted strategies to deal with particular threats and broader strategies to improve grid resilience and recovery through better planning, coordination, and operational awareness.

EMPs and cyberattacks share the potential for having significant, widespread impacts on energy infrastructure. Cyberattacks can be perpetrated from anywhere in the world, and for this reason they are very difficult to attribute to a malicious actor because of the level of anonymity that can be provided with internet communications. In addition, sophisticated hacking tools are becoming more widely available and the cyber threat is constantly evolving making such attacks more versatile. It is important to note that cyberattacks are made continually against energy infrastructure, although none to date have caused wide-spread or long-lasting interruption of service in the United States. The impact of an EMP

attack can be equally devastating or even exceed that of a cyberattack. Government studies and reports, such as those from the 2008 EMP Commission and the Government Accountability Office (GAO), cite risks caused by a man-made EMP or a naturally occurring solar weather event that could have a severe impact on the nation's electric grid as well as other critical infrastructures. In fact, GMD events are inevitable, with their only uncertainty being their timing and severity.

Considering the potentially wide-spread and long-lasting impact of either a cyber or EMP event, both threats should be addressed to more fully protect the security and ensure the resilience of the Bulk-Power System and critical energy infrastructure.

FROM SENATOR DAINES

1. **I want to take this opportunity to highlight some road blocks my state is facing in addressing these issues. As you stated in your testimony FERC and NERC are taking steps to address grid security as it relates to GMDs and EMPs, and they have already taken steps to address issues of physical protection, including vegetation management and cyber protection. Unfortunately, while existing standards and directives are well intentioned there have been major roadblocks. Our small Coops are finding it hard to participate in cyber discussions, and while FERC has strict vegetative management guidelines, our Coops are not able to cut trees or responsibly manage areas around transmission lines due to challenges with federal land managers and costly liability requirements. And, by the way vegetation-related events are currently one of the main causes of blackouts. Can you expand on the FERC and NERC standard for physical protection on vegetative management? Is there cooperation with local utilities and federal land managers?**

Response

The Energy Policy Act of 2005 gave FERC authority to review and, if appropriate, approve Reliability Standards developed by an Electric Reliability Organization (ERO). Upon approval, the Reliability Standards become mandatory and enforceable for the users, owners, and operators of the Bulk-Power System. FERC, the ERO, or Regional Entities working on behalf of the ERO can enforce FERC-approved Reliability Standards. In 2006, FERC certified NERC as the ERO and has approved Reliability Standards proposed by the ERO, including the

current Reliability Standard for vegetation management, FAC-003-4 (Transmission Vegetation Management).[1]

FAC-003-4 generally applies to all transmission lines operated at or above 200 kV, plus select lower voltage lines. The Reliability Standard explicitly applies to transmission lines that cross lands owned by federal entities. FAC-003-4 requires maintenance of a minimum vegetation clearance distance between power lines and trees to minimize disruption of electric service due to vegetation contacts with transmission lines. However, it does not prescribe how the transmission line owner must meet the performance requirement. It only sets a minimum requirement for vegetation management programs, *i.e.,* that they conduct inspections and meet the required clearances. Vegetation management practices are usually defined by the specific right-of-way agreements that the transmission line owner has secured with the property owner subject to any state or local regulations. Further, Montana's co-ops must comply with any currently applicable vegetation management regulations and environmental ordinances established by the State of Montana and/or local jurisdictions, to the extent they do not conflict with the FERC-approved Reliability Standards.

There is coordination between utilities and federal land managers. For instance, in 2016 a memorandum of understanding (MOU) on vegetation management for power line rights-of-way on federal lands was agreed to by the Edison Electric Institute, Utility Arborist Association, United States Department of the Interior (National Park Service, Fish and Wildlife Service, Bureau of Land Management), United States Department of Agriculture Forest Service and the United States Environmental Protection Agency. The MOU addresses industry concerns relating to vegetation management and its ability to deliver reliable electric transmission.[2]

The purpose of the MOU is to facilitate cooperation and coordination among the parties regarding vegetation management within and immediately adjacent to existing and future power line rights-of-way and associated facilities. One goal of the MOU is to facilitate implementation of cost-effective and environmentally sound vegetation management plans, procedures, and practices for power line rights-of-way that will reduce adverse environmental and cultural impacts while

---

[1] Reliability Standard FAC-003-4 is available at http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=FAC-003-4&title=Transmission Vegetation Management&jurisdiction=United States.

[2] The MOU is available at http://www.eei.org/issuesandpolicy/environment/land/Documents/EEI_MOU_FINAL_Signed_09.29.16.pdf.

enhancing the ability of utilities to provide uninterrupted electrical service to customers and address public safety. The MOU also addresses the use of incorporating vegetation management practices into the existing and future rights-of-way grants/authorizations across Federal lands. While the Montana coops are not signatories to the MOU, it may provide a framework for the coops to work with federal land managers.

2. **How can we incorporate our small and rural Coops into the conversation so that if or when we do craft standards for events like EMPs and GMDs that they are attainable and cost effective enough for or small and rural Coops to implement?**

Response

I think it is important that interested parties have an opportunity to meaningfully participate in the development of reliability standards. As a general matter, I believe that public power entities are well-represented in the NERC standards process, but I agree that we should endeavor to ensure that those standards are attainable and cost effective for all utilities that must comply with them.

Many small and rural coops mainly own only distribution facilities. FPA section 215 authorizes the Commission to approve Reliability Standards for the Bulk-Power System, and excludes facilities used in local distribution. Thus, Reliability Standards would typically not apply to facilities owned by small coops. In addition, small coops are often represented in reliability and regulatory issues by their trade organization, the National Rural Electric Cooperative Association (NRECA). So, while a small coop may be limited in its ability to represent itself, it is represented by NRECA, which is an active participant before FERC and in the NERC stakeholder process.

There are some large coops that own significant transmission and distribution facilities. Under NERC's rules for the development of new or modified Reliability Standards, NERC affords participants due process, openness and a balance of interests. The drafting meetings are open to the public, and all participants (either in person or by phone) can present their concerns. In addition, in the approval process at FERC, proposed Reliability Standards are considered in an open process that allows for public comment as part of FERC's consideration of a proposed standard. In both of these processes, NRECA and the coops affected by Reliability Standards can participate in the drafting and approval processes. For example, Tri-State Generation and Transmission Association, Inc. submitted written comments to FERC in the case that resulted in approval of a Reliability Standard addressing planning for a 1-in-100 year GMD event.

QUESTIONS FOR ACTING CHAIRMAN LAFLEUR
05.04.17 Committee on Energy and Natural Resources

FERC is also actively involved in efforts beyond its Reliability Standards process and has worked collaboratively with NRECA and the American Public Power Association. FERC works closely with our federal partners as well as the industry to better understand the risks and impacts associated with EMP on energy infrastructure. These efforts include providing classified and unclassified threat briefings, assisting with the development and identification of best practices for mitigation, and helping with voluntary implementation efforts.

FROM SENATOR CORTEZ MASTO

1. **Chairwoman LaFleur, thank you for your testimony. You spoke about FERC's work with state and local authorities on the risk of electromagnetic pulse (EMP) events, through briefings and developing best practices. I'm interested in hearing more about what the federal government is doing to ensure that state and local officials have real time updates on risks to the electric grid, either through EMP events, cyberattacks or other catastrophic events.**

    a. **You spoke during the hearing about the information the National Oceanic and Atmospheric Administration (NOAA) provides to state officials regarding warning signs of a naturally occurring EMP event. Does a similar information sharing process exist for warning signs of a potential manmade EMP event, from a state or non-state actor?**

Response

I am not aware of any such system for information associated with man-made EMP threats.

    b. **In addition, I know that getting information to the appropriate classification level can at times be a challenge for information sharing from the federal to state and local governments. Is the information shared in a timely enough manner where it could be properly acted upon?**

Response

The National Oceanic and Atmospheric Administration and the Space Weather Prediction Center is the official U.S. Government source for distribution of space weather related (e.g., GMD) information. A well-established notification process is in place that directly provides timely information to any subscriber including state and local government officials. As for EMP, cyberattack, or other

catastrophic events, DHS has established Fusion Centers to operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, state, local, tribal, territorial, and private sector partners.[3] Fusion Centers are operational in all 50 states as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands.

2. **The security of our infrastructure is of critical importance to me, particularly since so much of the economy in my home state of Nevada relies on electricity to keep tourism, gaming and the strip going around the clock.**

   In 2007, the Idaho National Lab led a research project that simulated a cyberattack on the electric grid. During the effort, as you likely know, they demonstrated the vulnerability of much of our electric grid to cyber weapons. Since that time, companies, as well as federal, state and local governments have taken steps to fortify our defenses against cyberattacks, but there is more to do.

   Can you talk about the likelihood of an EMP attack on our grid as compared with a cyberattack?

Response

EMPs and cyberattacks share the potential for having significant impacts on widespread portions of FERC jurisdictional infrastructure. Each has attributes that make them easier or more difficult to perpetrate, thereby affecting their likelihood.

Sophisticated cyberattacks can be perpetrated from almost anywhere in the world. Cyberattacks can be difficult to attribute to a malicious actor because of the level of anonymity that can be provided through internet communications. In addition, sophisticated hacking tools are becoming more widely available and the cyber threat landscape is constantly evolving, making such attacks more versatile. In addition, cyberattacks are constantly made against critical energy infrastructure, although none to date have caused wide-spread or long-lasting interruption of interstate electric service in the United States. Although the attacks are sophisticated and fast-changing, mitigation practices such as the adoption of NERC's Critical Infrastructure Protection Reliability Standards, National Institute of Standards and Technology standards, and others are well-accepted and have been widely implemented on critical energy infrastructure in the United States making it more difficult for an attack to succeed.

---

3 Information regarding Fusion Centers is available at https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

QUESTIONS FOR ACTING CHAIRMAN LAFLEUR
05.04.17 Committee on Energy and Natural Resources

EMP attacks require either a physical presence near the facility being attacked (as in a suitcase attack), or a presence at a more distant location using a platform such as an aircraft[4] or ship,[5] or the ability to gain control of a nuclear device. This required physical presence, access to an aircraft or ship, or access to nuclear capability typically makes an EMP attack have a higher barrier to entry. The impact of an EMP attack, however, can be equally devastating or even exceed that of a cyberattack. Government studies and reports, such as those from the EMP Commission and GAO, cite risks caused by man-made EMP or a naturally occurring solar weather event as potentially having a severe impact on the nation's grid as well as other critical electric infrastructure.

Because EMPs can have a higher barrier of entry, easier attribution, and require some level of physical proximity, or access to nuclear weapons, they are more difficult to implement. However, the results of an EMP attack may be more severe than a cyberattack.

By comparison, cyberattacks against critical energy infrastructure are happening continually, being used by other countries, terrorist groups, criminal gangs, hacktivists, and others. Recognizing that the work to protect against cyberattacks must continue and evolve, the widespread acceptance and implementation of effective mitigation measures have thus far prevented a cyberattack causing a significant outage in the United States.

As noted above, effective protection of the Bulk-Power System requires that we address both events that occur regularly, such as attempted cyber intrusion, and high-impact, low-frequency events that can disrupt reliability. Considering the potential wide-spread and long-lasting impact of either a cyber or EMP event, both threats should be addressed to more fully protect the security of critical energy infrastructure.

---

4 *See* http://www.boeing.com/features/2012/10/bds-champ-10-22-12.page.

5 Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures (2008) at 2, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

QUESTIONS FOR ACTING CHAIRMAN LAFLEUR
05.04.17 Committee on Energy and Natural Resources

3. **Given that an EMP attack needs to be delivered by a physical denotation device, in what instances would a country or terrorist group use an EMP attack as opposed to a cyberattack?**

Response

I am hesitant to speculate on the circumstances in which a country or terrorist group would choose one form of attack over another. As I stated earlier, however, both could result in significant grid impacts and I believe both should therefore be addressed.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to the Honorable Newt Gingrich

Question from Chairman Lisa Murkowski

Question: One of the keys to a successful public-private partnership is trust and the willingness to share information. I am concerned, however, that there is a lack of trust by industry with the government – and for good reason. The December 2016 episode with Burlington Electric in Vermont is a perfect example. As I understand it, Burlington noticed an alert about a suspicious IP address that had connected to one of their computers and responded to that alert by dutifully reporting that fact to the government. The same day that they reported the alert, however, the Washington Post somehow learned about it and reported that Russian hackers had infiltrated the United States' electric grid. Later follow-up would show that the IP address was not necessarily linked to Russia and there was not malicious activity, but the damage to trust had been done. How do we restore and build trust between the private sector and government so that this type of information can be freely shared without concern about it becoming a media spectacle?

Answer: We should expect a lot more hacking from a variety of sources. The United Stated CyberCommand has to develop a real time validator that can investigate and report. The hackers at Carnegie Mellon are a good start.

Question from Senator Debbie Stabenow

Question: During today's testimony, we heard that EMPs are a threat to our national security. However, the range of impacts appear vast, from naturally occurring events causing grid disruptions, up to - and including - the aftermath of a high altitude nuclear detonation.

This Committee has held several hearings in this and previous congresses on the threats facing our electric grid and critical energy infrastructure. From your perspective, how does the threat posed from EMPs compare to other vulnerabilities such as cyber-attacks?

Answer: EMP is a catastrophic disaster if it occurs. True cyber dominance would also be a catastrophic disaster. We cannot set priorities. We have to investband organize to beat both.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

Questions from Chairman Lisa Murkowski

Question 1: Ambassador Cooper, in your written testimony, you note that a man-made EMP is significantly different from natural EMP events, or Geomagnetic Disturbances. Could you please explain your reasoning on this matter?

- *A Geomagnetic Disturbance (GMD) involves multiple low frequency pulses lasting minutes over a period of hours to days. Warning is provided by an increase in solar activity 18-72 hours in advance—with a significant update 20-45 minutes before charged particles hit the earth. It couples energy to the long lines of the grid, which is then focused on substations and, in particular, threatens the large generators and transformers. It also will affect long haul communications and the internet. These effects can be regional or worldwide, depending on the duration of the solar storm. Current magnitude estimates being provided by NERC to the electric energy producers are judged by the EMP Commission to be considerably low. These effects are of larger intensity at higher latitudes and near large bodies of water.*
- *High Altitude EMP (HEMP) pulses include a similar low frequency pulse (called the E3 component of the HEMP pulse) of substantially larger amplitude—by a factor of several greater than current NERC estimates), plus:*
    - *An extremely high frequency pulse (with a pulse width of 100s of nanoseconds) called the E1 component, effectively an electric "shock" that poses a major threat to all solid state electronics, especially the SCADA systems that control key components of the grid—e.g., generation stations and their natural gas and petroleum pipeline fuel sources. It also poses a significant threat to telecommunications, computers and data centers. Note: This faster E1 component arrives before the E2 and E3 components and will interfere with control systems needed for safe grid shutdown, potentially leading to severe damage of the power generation plants, unless there is adequate protection against E1 effects.*
    - *A midrange frequency pulse, called the E2 component, is similar to lightning and can be protected against via typical lightning arrestors. But care must be taken to avoid degradation from the effects of the earlier arriving E1 pulse.*
- *HEMP effects are regional to continental, depending on the height-of-burst of the attacking weapon(s). Geographic coverage increases with weapon yield and E3 intensity increases at lower latitudes (unlike GMDs that decrease at lower latitudes).*
- *Bottom line: Hardening against GMD leaves the grid vulnerable to HEMP; hardening against HEMP will also protect against GMD.*
- *Thus, the current government and industry focus on grid GMD protection while ignoring HEMP is shortsighted to say the least.*

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

Question 2: Can you tell us more about your work in South Carolina and with Duke Energy and the important lessons learned? Should the federal government put more resources into that type of approach? Should we be looking at similar pilot projects to the one you have ongoing with Duke Energy? What recommendations do you have for the government and private sector to collaborate in order to emulate the success your efforts in South Carolina have enjoyed?

- ***First, please permit me to recap my motivation for and the progress of our Lake Wylie Pilot Study, which I hope will become a model that others can and will follow.***
- ***As indicated in my written testimony, I began this South Carolina effort understanding that neither Federal nor State efforts were dealing effectively with the existential EMP threat—nor were they likely to do so in my lifetime. In my written testimony I quoted liberally from an April 20, 2017 letter from the EMP Commission Chairman to Energy Secretary Rick Perry specifying several important criticisms of ongoing pertinent activities hindering progress in dealing effectively with the EMP/GMD threat.***
- ***For such reasons, I concluded years ago that we had to address the problem "from the bottom up," working with local (e.g., city and county level) authorities and citizens themselves to gain an understanding of the threat and how they need to engage those who provide their electricity to assure the viability of their critical civil infrastructure, in case of a major electric grid shutdown. Without considerable emergency management cooperation at the local level, there will be little hope for most citizens who today depend on electricity for life-line services in our "just-in-time" economy.***
- ***Moreover, I began with several biases, based on a lifetime of pertinent experiences associated with EMP issues, which guide my assessments and recommendations.***
  - ***I have no confidence that we will ever harden the entire grid, so I believe we have to establish priorities—I give top priority to assuring the safety and viability of our ~100 nuclear power plants that produce about 20-percent of the nation's electricity, and half the electricity of my home state, South Carolina. Thus, I believe our top priority is to build protected "islands" within the grid around our nuclear power plants, the vast majority of which are in the Eastern Interconnect of the grid.***
  - ***To assure the viability of the nuclear power plants in an indefinite grid shutdown, we must first assure their cooling water systems are viable to avoid Fukushima-like disasters. Then, we must assure that sufficient generating power and loading conditions are provided by the surrounding "island" in the grid—and linked with other critically important elements of the grid to ensure they are available to restart the nuclear power plants—and other power plants, which will shut down to protect themselves if the grid goes down.***
  - ***I don't believe anything that isn't regularly tested and subjected to independent critical review—effective design and deployment is not enough; truly effective testing and maintenance are major challenges.***
- ***Over the past two years, I have developed excellent relationships with key electrical engineering professors at my alma mater Clemson University and several Duke engineers (including Clemson graduates) who also are concerned about this threat—***

and through them access to other university graduate programs and other energy companies. We agreed on how we could proceed with a meaningful "bottoms-up" program to assure the viability of three Duke Energy power plants on Lake Wylie, on the Catawba River that runs between North and South Carolina—and of course key transmission infrastructure that interconnects those nuclear, hydroelectric and coal power plants and others to their customers. Duke Energy's senior management has agreed to share broadly the lessons learned from this important "Lake Wylie Pilot Study," described in greater detail in my written testimony. I want to make clear I was not and am not selling anything to or for Duke Energy and would not take money from them if they offered it. I just want to cut through the morass described above, and provide hope that my grandkids can survive if we experience an EMP attack or GMD event. I know that all our citizens want this objective met.

- *A critically important lesson that we have learned is that Duke Energy needs the active participation/cooperation of other Energy Utility Companies and Electric Cooperatives (CoOps) that actually maintain critical infrastructure that delivers Duke's electricity to key customers, e.g., the water/wastewater infrastructure that supports local hospitals and other critically important service activities, including many citizens themselves. Happily, we are now working with these key individuals in the local area around Lake Wylie—including the Deputy Mayor (a Clemson electrical engineering graduate) of Rock Hill, a major suburban city neighboring Charlotte, the home of Duke Energy's corporate headquarters. Moreover we are achieving cooperation of the county sheriff and key local citizens. The SC Adjutant General (a Georgia Tech electrical engineer) is supportive of our effort, and we are working with his emergency management staff to support their participation in November's GRIDEX-IV national exercise focused on the physical and cyberattack threats to the grid. Associated contacts will be helpful in SC and beyond. We expect a regional follow-on exercise involving the EMP/GMD threat, and also including at least the NC emergency management community.*
  - *I cannot overstate the importance of engaging these local people in any effort to improve the viability of the electric grid—not just locally but in networking throughout the nation. Several thousand electric utility companies and CoOps deliver electricity via their infrastructure to key customers and private citizens around the nation. We hope to demonstrate how to meet this complex challenge.*
  - *I also can't overstate the important role that informed and concerned local citizens can play. For example, a retired Physician, who has come to understand the threat and the urgent need for local authorities to be actively involved, has provided a great deal of support with the local citizens as well as city and county officials—and through his growing involvement in SC statewide activities, such as the GRIDEX-IV exercise. These connections also involve the National Guard, thereby enabling lessons learned to be propagated through multistate and NORTHCOM connections, potentially to be included in a national network.*

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

- ***My short answer to your direct question is that I believe we will indeed produce a "bottom's up" pattern worth considering by other states. I personally believe that this approach has more promise of success than anything that can be produced by the currently discordant activities of the Federal Government. Congress could be helpful in addressing that important shortfall—in particular by extending to permanent status the EMP Commission and placing it in the White House with a charter to provide critical assessments of efforts of the several departments with related responsibilities and to recommend to the President and Congress measures to rectify shortcomings.***

Question 3: One of the keys to a successful public-private partnership is trust and the willingness to share information. I am concerned, however, that there is a lack of trust by industry with the government – and for good reason. The December 2016 episode with Burlington Electric in Vermont is a perfect example. As I understand it, Burlington noticed an alert about a suspicious IP address that had connected to one of their computers and responded to that alert by dutifully reporting that fact to the government. The same day that they reported the alert, however, the Washington Post somehow learned about it and reported that Russian hackers had infiltrated the United States' electric grid. Later follow-up would show that the IP address was not necessarily linked to Russia and there was not malicious activity, but the damage to trust had been done. How do we restore and build trust between the private sector and government so that this type of information can be freely shared without concern about it becoming a media spectacle?

- ***I agree there is a major problem in assuring public trust in the government to address this, in my judgment, existential threat. Moreover, their skepticism is well founded. Washington (in both Executive and Legislative branches) is failing to address the issue as I discussed in my testimony—and few state governments acknowledge the existential threat, much less deal with it. This general dysfunctional leadership is why I believe we must actually work the problem "from the bottom up," as I testified and discussed in my answer to Question 2. It would help if the key departments, DoD, DHS and DOE, would get their collective act together. But I believe this will only happen with strong leadership from the White House. Extending the EMP Commission and placing its secretariat in the White House with access to the President would help tremendously.***

Question 4: EMP models are only as good as the data inputs provided. The United States has not tested any nuclear weapons since 1992, and no atmospheric tests since the Test Ban Treaty of 1963. My understanding is that many of our weapon designs have required post-deployment tests to resolve problems – and those problems were discovered only because of ongoing nuclear tests at the time. In each case, the weapons were thought to be reliable and thoroughly tested. How confident are you that the data being inputted into the models with regard to the EMP effects of a nuclear weapon detonation is accurate – particularly since we have not conducted an atmospheric test since 1962?

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

- *The usable HEMP data from our most pertinent 1962 South Pacific high-altitude nuclear tests were sparse. However, with theoretical calculations we have always been able to match that limited data. With improvements in measurement uncertainty evaluations (affecting the quality of the data), the theoretical calculations and data (peak values and entire waveforms) have agreed within 20-percent. We subsequently obtained relevant data from low-altitude, low-yield testing at the Nevada Test Site, against which we could evaluate our theoretical models for at least "source-region" EMP. And that experience helped to build additional confidence in our HEMP calculations. My own personal experience was, like all who sought to conduct meaningful nuclear tests—including underground nuclear tests, to try to avoid the EMP disruption of instrumentation intended to measure other effects, e.g., to understand X-ray and Blast and Shock effects.*
- *I understand the Soviets/Russians executed better planned and instrumented HEMP experiments. They had an advantage since they broke-out of the 1958 atmospheric test moratorium with a well-planned 1961 test series, and then our "knee-jerk" high-altitude test response produced limited results. Because our tests exposed mostly ocean areas rather than large land areas with extensive long-line power and communications infrastructure, we did not experience the system network effects that did the Soviets in their high altitude test series. President Kennedy signed the Limited Test Ban Treaty on October 5, 1963, terminating indefinitely our ability to do better HEMP testing.*
- *In the early wake of the end of the Cold War in the 1990s, we obtained at least some of that more extensive information from Russian scientists. And the EMP Commission is now looking into how best to use that information to provide more confident estimates of EMP environments and system response information that should be helpful to the electric power companies seeking to protect their infrastructure from EMP effects.*
- *Moreover, Russian generals informed EMP Commissioners in 2004 that they had passed design information on "super EMP weapons" to North Korea and anticipated that they would have such a weapon in a few years—that was 13 years ago. Now, the electric power industry should be taking these capabilities into account in assuring their infrastructure can operate through—or be restored after—a HEMP attack.*

a. Since most of the data is controlled by the Department of Defense and the National Labs, does the private sector have access to the data needed to accurately model the potential EMP impact and effect of a nuclear explosion?

- *Much is already public—was made in the 2008 EMP Commission Report. Additional important data and EMP hardening information are, in my opinion, overclassified and should be made available to the private sector ASAP. For example, the "For Official Use Only" DoD EMP Engineering Handbook, MIL-HDBK-423 should certainly be completely unclassified. Our enemies surely have*

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

long ago had it. Moreover, the E3 portion of the DoD EMP Environment Standard, MIL-STD-2169C, should be declassified and provided to the energy companies seeking to harden their critical infrastructure.

b. My understanding is that most HEMP models are based on a one dimensional, spherically symmetric model, neglect scattering effects, and are unable to model 2- and 3-D effects. There is also no high-fidelity model that predicts EMP from detonations from 5 kilometers to 20 kilometers above the Earth's surface. Given these shortfalls, how confident are you in the accuracy of current EMP models?

- ***EMP experts tell me that the DoD EMP environment standard established decades ago is reliable for predicting the E1 component of the EMP pulse, and that it is well represented by 1D full-physics models. In fact, I understand that it is a validated (by experiment and 2&3-D calculations) high frequency approximation for the 3-D model, referred to as the Longmire-Karzas-Latter model for E1 generation.***
- ***In the mid-1960s a combination of 1-D and 2-D codes were developed at the Air Force Weapons Laboratory (AFWL), RAND, and Mission Research Corporation (MRC) that accurately predicted the EMP fields produced by air and ground vertical asymmetry effects for nuclear tests, over the altitude range from zero to exo-atmospheric altitudes. Within the atmosphere, the geomagnetic effect is smaller than the vertical asymmetry effects, but has been accurately predicted by the same 1-D approximation used to predict the fields produced by exo-atmospheric nuclear explosions. For explosions where the gamma rays interact with the ground, another 1-D approximation, called the Graham-Schaefer effect, has accurately predicted the close-in near-surface fields, and has been verified in underground nuclear testing. Together, these constitute high-fidelity models of the EMP fields produced by atmospheric and exo-atmospheric nuclear explosions.***
- ***Two independent families of EMP codes were developed and supported by the Defense Nuclear Agency and the USAF/AFWL to enable comparative error analysis that yielded results within 10-30% of each other. The Congressional EMP Commission funded SAIC physicists to recheck the physics of these analyses and found them to be correct. Thus, I conclude that current theoretical analyses are sufficiently accurate to confidently design, develop, deploy and operate critical grid infrastructure to counter E1 pulse. That said, I would insist on prudent defense-conservative designs.***
- ***I understand that the EMP Commission is completing reports on the E2 and E3 components of the HEMP pulse, with an expectation that current calculations will provide accurate results that are expected to be validated within a factor of 2. Again, I would insist on conservative designs to counter E2 and E3.***

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

Question 5: Are there military applications to address HEMP or other EMP-related events that are not being made available to civilians? If so, how do we lift that barrier?

- ***As noted in my answer to question 4a, we should declassify as much of the DoD information on EMP effects and hardening technology as possible. I urge that Congress demand that the EMP Commission make specific recommendations on this matter as part of their June 2017 report, if not sooner.***

Question 6: Do you believe any additional research is needed on EMP threats?

- ***I don't want to overstate the issue, but I believe most of the current "research" by the DOE labs and EPRI is at best reinventing what has already been accomplished by DTRA and the military service laboratories (AFRL, ARL, NSWC) over the last 50 years. This DOE redundancy is actually unhelpful and could be eliminated my making that DoD information available to the energy companies that need it to do their job. As noted above, the EMP Commission can make an enormously important contribution by providing specific recommendation in its June 2017 report, if not sooner.***

Question from Senator Debbie Stabenow

Question: During today's testimony, we heard that EMPs are a threat to our national security. However, the range of impacts appear vast, from naturally occurring events causing grid disruptions, up to - and including - the aftermath of a high altitude nuclear detonation.

This Committee has held several hearings in this and previous congresses on the threats facing our electric grid and critical energy infrastructure. From your perspective, how does the threat posed from EMPs compare to other vulnerabilities such as cyber-attacks?

- ***EMP is the "800 pound gorilla" on the list of threats (a view expressed by AT&T officials, with which I agree). It affects the long line systems similarly to solar storm GMD events (but of higher amplitude), and in addition EMP has a high frequency punch (the E1 Component) that will take out office equipment, data centers, and machine control electronics. Today, virtually none of our critical civil infrastructure is protected. As noted above, the low-frequency E3 component is substantially larger than the GMD threat, which is today being underestimated by NERC—so GMD protection may not, probably will not, suffice even for E3 protection.***
- ***From a technical standpoint, EMP can induce over-voltages on everything from computers to heavy machinery controllers to data networks comprising the internet, to telephone networks, electric power plants and substations. And while not all electronic systems will upset or burnout, a large enough fraction will fail such that, without protection, cascading effects can bring the U.S. economy, or any economy, to a***

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

grinding halt. Among critical infrastructure systems, the power grid is probably the most certain to fail. Without electric power, most other infrastructures will be debilitated. Without protection, the power grid will be out of service for significant portions of time—as explained in the 2008 EMP Commission report.

- *DHS has identified 16 infrastructures, and of these the electrical power system and communication systems are arguably the most important to the national enterprise, but, ironically, they are also the most vulnerable. The reason is that they depend upon long lines, and since EMP levels are measured in Volts per meter, so the longer the lines in meters the higher the voltage induced on the lines. Intuitively, any system that has long lines (e.g., electric power or communications) will be the most vulnerable.*
- *We know how to protect systems against EMP. The DoD has been doing it since the 1960s, and has developed EMP environment and protection engineering standards. Simply put a shield around critical equipment; protect all the wire penetrations; include backup power systems and use fiber optics as much as possible. We know how to protect against solar storms (GMD) because Sweden and Canada have protected their grids against solar storms for years. Since we know how to protect against GMD with capacitive blockers and reactive power compensators, we know how to protect against the EMP E3, though we must take care not to underestimate its magnitude. And we must test regularly to assure even the best standards of operations are maintained after sound hardening capabilities are deployed.*
- *This is not to argue against protecting the grid against cyber and physical attack. Indeed, if there is an EMP attack our adversaries, who are well informed and competent, undoubtedly will include cyber and physical attack precursors to confuse us and disrupt our response not only to those attacks but to the pending EMP attack itself. The best approach is a multi-hazzard approach since the same high impact system failure locations are vulnerable to EMP, cyber and physical attacks.*

Question from Senator Steve Daines

Question: You stated that although EMP attacks are known to be included in North Korea's military doctrine and planning, bureaucracy and inaction have precluded DoD, DoE, and DHS from developing an effective EMP defensive posture. I serve on committees with jurisdiction over all three of those departments. From your perspective, what red tape needs to be cut to get the right leaders in a room and address this issue?

- *I believe that the Executive Branch must address its dysfunctional activities that inhibit efforts toward this end. The White House must lead. My recommendation is to place the re-instated EMP Commission permanently under a White House Secretariat with direct access to the President, with a mandate to resolve the interagency conflicts of interest and programmatic activities—especially among DoD, DHS and DOE. Initially,*

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Ambassador Henry F. Cooper, Ph.D.

I would urge that Congress seek an early assessment of the viability of the nation's critical national infrastructure and associated regulatory operations, with specific recommendations to the President and Congress for appropriate improvements.

- *Congressional initiatives could provide important incentives to encourage significant improvement in the various programs that must be conducted by the Executive Branch. Among them, I would encourage ways to incentivize local and state initiatives to work closely with the nation's several thousand electric utility companies and CoOps to assure electricity flows from the major electric power companies to key local, city and county key infrastructure, e.g, water-wastewater infrastructure that is key to hospitals, businesses, citizens, etc.*
- *Finally, local leadership and active involvement of all our citizens is key to success. I can think of no more effective means to reach that goal than to work through the National Guard as the vehicle by which our State Adjutant Generals can achieve an effective national arrangement. At the end of the day, success will require a more effective alliance between the Departments of Defense and Homeland Security. And the National Guard should be challenged to help achieve that alliance. Congressional encouragement toward that end could be most helpful in resolving current "roles and missions" gaps. Hopefully, our Lake Wylie Pilot Study will provide a template that other states and the federal government can exploit in working toward that end.*

Responses to Questions for the Record
U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration

CAITLIN DURKOVICH

Director, Toffler Associates

Former Assistant Secretary, Infrastructure Protection,
National Programs and Protection Directorate
Department of Homeland Security

Submitted to the

SENATE ENERGY & NATURAL RESOURCES COMMITTEE

Question 1: Much attention is focused on how to protect energy infrastructure, and particularly the electric grid, from a high-altitude EMP – or HEMP – burst due to its potential wide-spread impact. Given that a localized EMP burst is more powerful than a HEMP burst, would the same hardening technologies that are deployed for a HEMP burst successfully guard against a localized EMP attack?

Industry and government are working hand in hand to better understand the impacts of localized and high-altitude EMPs. The work that Electric Power Research Institute is conducting is critical to understanding how transformers, protective relays, SCADA, control cables would be affected by these types of bursts. This critical modeling can help inform where investments in shielding and other hardening approaches will have the maximum value.

Question 2: One of the keys to a successful public-private partnership is trust and the willingness to share information. I am concerned, however, that there is a lack of trust by industry with the government – and for good reason. The December 2016 episode with Burlington Electric in Vermont is a perfect example. As I understand it, Burlington noticed an alert about a suspicious IP address that had connected to one of their computers and responded to that alert by dutifully reporting that fact to the government. The same day that they reported the alert, however, the Washington Post somehow learned about it and reported that Russian hackers had infiltrated the United States' electric grid. Later follow-up would show that the IP address was not necessarily linked to Russia and there was not malicious activity, but the damage to trust had been done. How do we restore and build trust between the private sector and government so that this type of information can be freely shared without concern about it becoming a media spectacle?

The December 2016 Burlington Electric episode was an unfortunate episode in a long-standing and evolving trusted partnership between government and industry. That partnership is built on a foundation of safeguarding information and is leveraged daily to freely share physical and cyber vulnerabilities between government and industry. Congress provided government with authorities such as the Protected Infrastructure Information (PCII) Program under the Critical Infrastructure Information (CII) Act of 2002, which protects private sector infrastructure information voluntarily shared with the government for the purposes of homeland security and has established uniform procedures on the receipt, validation, handling, storage, marking, and use of voluntarily submitted critical infrastructure information. As the former senior official in charge of the PCII program, the protection of sensitive vulnerability information is taken very seriously and remains the foundation for information sharing activities between government and industry. The program has been enormously successfully and is currently in the early stages of the rule making process to modernize a rule that was drafted over 11 years ago.

That trust is also sustained through the Critical Infrastructure Partnership Advisory Council (CIPAC), which aligns with the National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Specifically, CIPAC facilitates confidential interaction between government and representatives from the community of critical infrastructure owners and most notably through regular meetings between senior government and indsutry representatives to discuss sensitive topics. The enduring nature of these meetings should give you confidence of the trust that exists between the private sector and government and the fact that information is often freely shared without becoming a media spectacle.

Question 3: You testified that HEMP threat vectors can originate from a missile; a satellite asset; or a "relatively low-cost balloon-borne vehicle." Please elaborate on the possibility of a balloon-borne vehicle to launch an EMP strike. Do you agree then with Ambassador Cooper's assert that "low-yield 'Super' EMP weapons" are a viable threat?

My answer to this question is informed by classified intelligence and briefings and as such I can only provide a partial response. I believe the threat of "low-yield 'Super' EMP weapons" is very low likelihood.

Question 4: Are there military applications to address HEMP or other EMP-related events that are not being made available to civilians? If so, how do we lift that barrier?

This is a question best answered by industry. There are utilities that are testing EMP/GMD shielding and other hardening approaches. I do not know if this includes military applications but if it does not, the best way to lift that barrier is to bring the stakeholders to the table to discuss options.

Question from Senator Debbie Stabenow

Question: During today's testimony, we heard that EMPs are a threat to our national security. However, the range of impacts appear vast, from naturally occurring events causing grid disruptions, up to - and including - the aftermath of a high altitude nuclear detonation.

This Committee has held several hearings in this and previous congresses on the threats facing our electric grid and critical energy infrastructure. From your perspective, how does the threat posed from EMPs compare to other vulnerabilities such as cyber-attacks?

There is no doubt we live in a dangerous world. State and non-state actors, insiders, and promulgators of disinformation are growing in kind and consequence. Borders no longer protect us – whether our shores or the fences and networks of our organizations. We have built a complex ecosystem where a disruption in one node can ripple across the system and where threats are not bounded to one sector or industry. Nor can we protect against every threat and secure every building, system, and network. Our country is too big, our infrastructure is too complex, the cost too expensive, and the outcome would alter our way of life.

This environment is the basis for government and private sector participants in the critical infrastructure community working together to prioritize and manage risks to achieve security and resilience outcomes. Think of a matrix where the x and y axis are likelihood and consequence respectively.

- **A denial of service attack is highly probable but the impact is minimal to operations**
- **Most natural disasters are high likelihood and low consequence – Superstorm Sandy or a 9.0 Cascadia subduction zone event are exceptions and flip – low likelihood, high consequence**
- **A GMD of the likes of the 1859 Carrington event – we are beyond that 100 year window so I would say more likely and certainly high consequence**
- **A cyber attack against industrial control systems. Lower probability than a DOS although increasing, and certainly higher impact. You only need to look at the December 2015 attack on the Ukrainian power grid.**

There are half a dozen more risks on that matrix including an HEMP - we place it at a very low probability but very high consequence.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Robin Manning

Questions from Chairman Lisa Murkowski

Question 1: In your written testimony, you mention that all three components of a HEMP event – E1, E2, and E3, are being evaluated. The effects of E2 are fairly well known given its similarity to a lightning strike. Studies have been done, or are underway to individually look at E1 and E3. Are there any studies that look at the cumulative effect of these three components? Would infrastructure react differently to an E2 blast after being hit by E1, or an E3 after being hit by E1 and E2?

The question posed is ultimately one that we are attempting to answer with our current research effort. We are unaware of any studies to date that have been conducted to evaluate the cumulative effect of all three components, E1, E2 and E3. We are aware of at least one effort, in addition to the EPRI project, that is currently attempting to evaluate the cumulative effects of all three components. However, there are significant research gaps with regards to equipment vulnerability and modeling which makes performing such assessments extremely difficult. Current research efforts at EPRI are aimed at developing the capability to evaluate the combined effects of all three components.

It is certainly possible that infrastructure could react differently to E2 or E3 following E1, but current research has not progressed to the point where we can provide a definitive answer. Results from the research described previously, once they are available, will be used to inform the potential impacts and address these important questions.

Question 2: Mr. Manning, in your written testimony, you suggest that the E3 component of an EMP is similar to a severe GMD event. Could you please explain your reasoning on this matter?

The interaction of the Earth's magnetic field in both a nuclear explosion and solar flares generates a similar result on the electric grid. Both induce very low frequency (quasi-dc) currents in the grid which appear very much like a direct current flow superimposed in the alternating current grid. These currents are called geomagnetically induced currents, or GIC. While the effect is similar, the magnitude and duration are very different. GIC currents are much larger following a nuclear event than GIC currents resulting from a geomagnetic disturbance (GMD) event. However, the GIC resulting from a nuclear detonation is relatively short duration, rising and falling in a matter of minutes, whereas, solar induced GIC can last for days with several periods of peak activity. In both cases, the flow of GIC in transformer windings results in half-cycle saturation, potentially leading to voltage collapse and additional hotspot heating in bulk-power transformers which can cause physical damage in some cases. Additionally, half-cycle saturation causes the transformers to inject harmonic currents into the grid which can result in additional impacts by causing equipment designed to supply reactive power to trip off-line; thus, further exacerbating voltage issues in the grid. Mitigation strategies, e.g. neutral blocking devices, etc., to reduce the impact of GIC currents are effective against both E3 and GMD induced currents. Additionally, utilities can monitor GIC in real time, and make informed

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Robin Manning

decisions about the impacts of GIC because of the lower energy and longer timeframe. This is not true for GIC induced by E3, which occurs too rapidly for human intervention.

Question 3: Much attention is focused on how to protect energy infrastructure, and particularly the electric grid, from a high-altitude EMP – or HEMP – burst due to its potential wide-spread impact. Given that a localized EMP burst is more powerful than a HEMP burst, would the same hardening technologies that are deployed for a HEMP burst successfully guard against a localized EMP attack?

Localized EMP is designed to emit a high-energy pulse that emulates the E1 signature of an HEMP. Mitigation measures designed to offer E1 HEMP protection, e.g. MIL-STD-188-125-1, would also provide a level of protection against localized EMP. However, because some weapons that may be used in a localized EMP attack generate significant energy levels at frequencies higher than those currently specified in MIL-STD-188-125-1, it is not clear whether the level of protection would be the same as that provided for HEMP (E1).

Question 4: Thank you not only for your testimony today but for your willingness to be a witness last year before this Committee's Subcommittee on Energy. Comparing your testimony from last July with your testimony for this hearing, it appears to me that EPRI specifically and industry generally has stepped up activity over the last year to address EMP and related issues and challenges. Can you summarize the trajectory of EPRI, industry, and related DOE efforts over the last year and where you expect to see these efforts moving over the next 2 or three years? Where would you expect us to be in three years' time on this issue compared with today? Is there any prudent way to move more quickly?

Many factors have brought EPRI, DOE and the industry together around the EMP issue over the past year, including growing awareness of the EMP threat and a deeper understanding of the potential consequences of an EMP attack. Evidenced by the broad industry participation, the EPRI EMP project is meeting a relevant need. This need also happens to align very well with the DOE push to take action around protecting the nation's infrastructure.

EPRI's research project is on-track with the 3-year plan. The impacts of E3 on bulk transformers was selected as the foundational threat because it held the highest potential for replacement challenges. Now that this component is complete, the project is moving to the voltage collapse issue from E3, the equipment and controls risk from E1, and the aggregate risk from all three energy waves (E1, E2 and E3) together. The voltage collapse results are expected late summer, and initial E1 results by year-end, 2017. Aggregation of all risks will be done last with the research project's scheduled completion in spring, 2019. Additionally, we are evaluating the potential for developing cost-effective mitigation options so that reliability can be maintained without utilizing more extreme approaches, e.g. MIL-STD-188-125-1.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Robin Manning

Project speed continues to be a challenge. Everyone involved would like to see the work completed as fast as possible. However, while a great of deal work has been done on EMP, very little has been directly applied to the electric utility infrastructure. Much of this work is first time, groundbreaking work. Even so, it is not the work itself that drives the timeline – it is the collaborative transformation. As important as the technical learning is building an understanding and communication of the resulting information. As this project advances, so too advances the knowledge base of the nation's electric grid owners and operators. While this may seem like a long time to wait, it is remarkably quick compared to our progress to date.

When this research project is finished in April, 2019, it will conclude with a broad understanding of the threat, mitigation and recovery actions around EMP. We anticipate that utilities and stakeholders will have concrete options for balancing the EMP threat against others.

Question 5: EMP models are only as good as the data inputs provided. The United States has not tested any nuclear weapons since 1992, and no atmospheric tests since the Test Ban Treaty of 1963. My understanding is that many of our weapon designs have required post-deployment tests to resolve problems – and those problems were discovered only because of ongoing nuclear tests at the time. In each case, the weapons were thought to be reliable and thoroughly tested. How confident are you that the data being inputted into the models with regard to the EMP effects of a nuclear weapon detonation is accurate – particularly since we have not conducted an atmospheric test since 1962?

a. Since most of the data is controlled by the Department of Defense and the National Labs, does the private sector have access to the data needed to accurately model the potential EMP impact and effect of a nuclear explosion?

b. My understanding is that most HEMP models are based on a one dimensional, spherically symmetric model, neglect scattering effects, and are unable to model 2- and 3-D effects. There is also no high-fidelity model that predicts EMP from detonations from 5 kilometers to 20 kilometers above the Earth's surface. Given these shortfalls, how confident are you in the accuracy of current EMP models?

Question from Senator Debbie Stabenow

Question: During today's testimony, we heard that EMPs are a threat to our national security. However, the range of impacts appear vast, from naturally occurring events causing grid disruptions, up to - and including - the aftermath of a high altitude nuclear detonation.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Robin Manning

This Committee has held several hearings in this and previous congresses on the threats facing our electric grid and critical energy infrastructure. From your perspective, how does the threat posed from EMPs compare to other vulnerabilities such as cyber-attacks?

We would refer you to the Intelligence Community and the Department of Energy for additional information regarding how the two threats compare.

Utilities often use a threat assessment process to balance investments. This is an effective way to gauge one risk verses another. This approach requires an assessment of both the probability of an event, and a consequence should the event occur. EMP probability is very difficult to assess, and most utilities will place this in an unlikely, but possible category. However, the consequences of even an unlikely event can be extremely severe. Contrast this with cyber-attacks which are now occurring daily, but largely with less severe consequences. An effective strategy would be to invest in reducing both the probability and the consequences of cyber-attacks, while focusing exclusively on reducing consequences of an EMP attack. This is exactly why utilities are interested in the EPRI project to inform the discussion around reducing EMP consequences. In any case, both require attention, albeit via different approaches. It is not a matter of which threat is more or less critical, it is a matter of what strategies can be deployed to lower the overall risk, including all threats evaluated.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017, Hearing: The Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Kevin Wailes

Questions from Chairman Lisa Murkowski

Question 1: Much attention is focused on how to protect energy infrastructure, and particularly the electric grid, from a high-altitude EMP – or HEMP – burst due to its potential wide-spread impact. Given that a localized EMP burst is more powerful than a HEMP burst, would the same hardening technologies that are deployed for a HEMP burst successfully guard against a localized EMP attack?

The impact of an EMP caused by a directed energy weapon depends on the size of the weapon used. Given that the damage resulting from this type of EMP would be localized, hardening technologies designed to protect against the widespread impact of a HEMP event may not provide adequate protection. However, there is a great deal of system redundancy built into the grid that would mitigate the impact of an individual directed energy weapon. To cause significant damage to the electric grid, dozens of directed energy weapons would need to be built, deployed, and detonated in a coordinated attack. More effective protections for these types of EMPs are physical protection measures, such as limiting proximity and controlling access to substations and control centers.

Question 2: One of the keys to a successful public-private partnership is trust and the willingness to share information. I am concerned, however, that there is a lack of trust by industry with the government – and for good reason. The December 2016 episode with Burlington Electric in Vermont is a perfect example. As I understand it, Burlington noticed an alert about a suspicious IP address that had connected to one of their computers and responded to that alert by dutifully reporting that fact to the government. The same day that they reported the alert, however, the Washington Post somehow learned about it and reported that Russian hackers had infiltrated the United States' electric grid. Later follow-up would show that the IP address was not necessarily linked to Russia and there was not malicious activity, but the damage to trust had been done. How do we restore and build trust between the private sector and government so that this type of information can be freely shared without concern about it becoming a media spectacle?

Trust is the foundation on which sharing information between industry and government is dependent. This is why the electric industry thought it so important for the Cybersecurity Act of 2015 and the energy provisions of the 2015 FAST Act to include language to ensure that shared information be kept classified and not allowed to be used for regulatory purposes.

You are correct in your characterization of this unfortunate event. The best way to restore and build trust between the private sector and government is to ensure that a leak like this does not occur again. While disappointed and frustrated with the way this incident was handled, to its great credit, Burlington Electric publicly stated that it would not pull back from sharing information with the federal government because it recognizes that protecting the grid against cyber threats, by its nature, requires a strong government-industry partnership. As I commented

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017, Hearing: The Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Kevin Wailes

during the hearing, this was a significant learning experience for both industry and our government partners. I would also add that processes like the DOE-OE417 reporting requirements need to be revised so utilities can share information anonymously.

Question 3: Your written testimony provides, and I quote – "there are concerns that installing 'protective devices' in some areas of the bulk power system could unintentionally cause problems in other areas. Further research and testing of these devices is needed. Even assuming that every conceivable blocking device were installed to protect every inch of the electric grid and caused no problems, power supplies still would likely be subject to disruption from other collateral impacts due to a HEMP event." Given that, what do you think is the most prudent way for industry and government to improve our efforts to ride through an EMP attack?

Industry and government need more scientific information on the potential impact of a HEMP and effective mitigation techniques. As I described in my testimony, the multi-year research effort being led by the Electric Power Research Institute (EPRI) is an attempt to model the effects of a HEMP on the grid using highly technical data. We must have a better understanding of the science of how a HEMP would affect the grid before mandating any particular devices or strategies. To move forward without this information would at best be wasteful, and at worst, be harmful due to the possibility of unintended consequences.

I also must again stress that the electric sector faces a broad threat landscape. We understand that we cannot protect all assets completely from all threats, and instead must manage risk. A HEMP event is categorized as a "high impact, low probability" threat. It would have a potentially catastrophic impact on society that would impact all critical infrastructure sectors. An attack of this magnitude would be an act of war or terrorism. As such, the federal government is responsible for preventing HEMPs as a matter of national security.

Question 4: Your written testimony recommends that the recently-reconstituted EMP Commission work more closely with, and I am quoting, "owners and operators of critical infrastructure, EPRI, ESCC, NERC, and the E-ISAC as the Commission executes its mission to assess the vulnerability of the electric grid to EMPs and to develop recommended policy actions. Combining the unique backgrounds of the EMP Commission with the knowledge of experts in grid engineering and operations would produce a more meaningful and informed product." Please elaborate.

The electric grid is a very complex yet resilient integrated network of generators, transmission lines, and control systems. Modeling how electricity flows thorough this system and how it will react to the loss of a generator or loss of multiple transmission lines is a complex process that is more art than science. The electric industry is comprised of experts in engineering and operations; they are not experts in nuclear weapons. The EMP Commission is largely comprised of those with expertise in nuclear weapons; they are not experts in modeling the complex grid

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017, Hearing: The Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Kevin Wailes

operations during extreme events. Neither side has all the expertise or answers. Congress should direct the EMP Commission to engage in meaningful consultation with the electric industry before releasing its next report.

Question 5: EMP models are only as good as the data inputs provided. The United States has not tested any nuclear weapons since 1992, and no atmospheric tests since the Test Ban Treaty of 1963. My understanding is that many of our weapon designs have required post-deployment tests to resolve problems – and those problems were discovered only because of ongoing nuclear tests at the time. In each case, the weapons were thought to be reliable and thoroughly tested. How confident are you that the data being inputted into the models with regard to the EMP effects of a nuclear weapon detonation is accurate – particularly since we have not conducted an atmospheric test since 1962?

I do not have the scientific or defense background necessary to answer this question. As such, I must defer to the extraordinarily qualified researchers at the national labs and EPRI, in which I have full-faith.

a. Since most of the data is controlled by the Department of Defense and the National Labs, does the private sector have access to the data needed to accurately model the potential EMP impact and effect of a nuclear explosion?

   Yes, the unclassified HEMP information provided in a number of reports and industry standards can adequately inform the research activities being conducted in the private sector. However, ensuring electricity sector engineers and DOE experts are privy to the classified research from DOD weapons programs is integral to ensuring critical infrastructure operators have the information they need to understand and mitigate threats posed by HEMP.

b. My understanding is that most HEMP models are based on a one dimensional, spherically symmetric model, neglect scattering effects, and are unable to model 2- and 3-D effects. There is also no high-fidelity model that predicts EMP from detonations from 5 kilometers to 20 kilometers above the Earth's surface. Given these shortfalls, how confident are you in the accuracy of current EMP models?

   Again, I do not have the scientific or defense background necessary to answer this question and, as such, must defer the national labs and EPRI. However, the modeling of the electric grid's reaction to a HEMP event requires different expertise from those who model the electromagnetic waves from a HEMP.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017, Hearing: The Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Kevin Wailes

Question 6: In your written testimony you mention the Schweitzer report and its conclusion that "existing IEEE substation design standards are sufficient to protect intelligent electronic devices from HEMP." How many of the substations in the U.S. adhere to these design standards?

Although I cannot cite a specific number, the majority of the substations in the United States adhere to IEEE standards; the larger and more critical the substation, the more likely it follows the standards. They key point to note here is that the industry has formulated standards on its own.

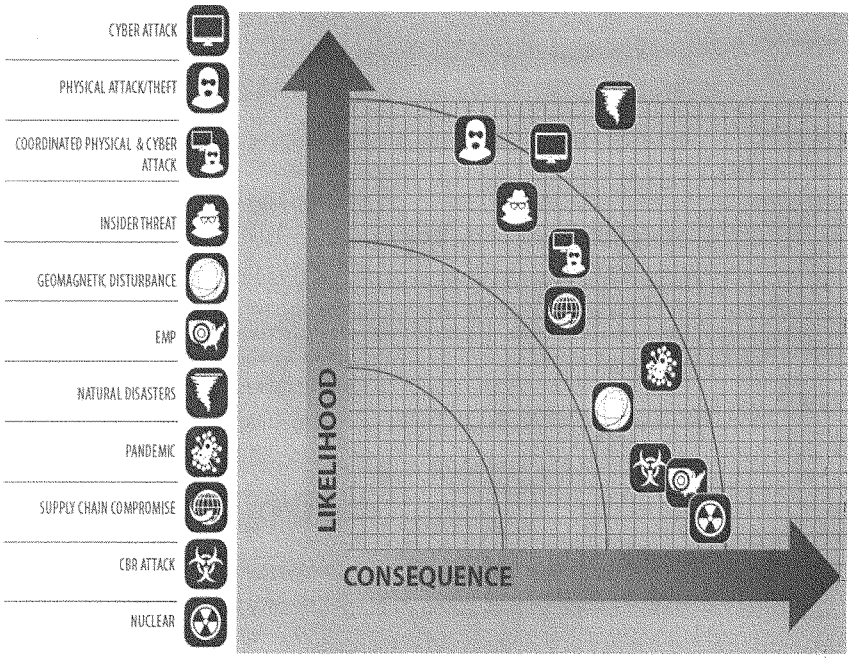
Question from Senator Debbie Stabenow

Question: During today's testimony, we heard that EMPs are a threat to our national security. However, the range of impacts appear vast, from naturally occurring events causing grid disruptions, up to - and including - the aftermath of a high altitude nuclear detonation.

This Committee has held several hearings in this and previous congresses on the threats facing our electric grid and critical energy infrastructure. From your perspective, how does the threat posed from EMPs compare to other vulnerabilities such as cyber-attacks?

A HEMP event is categorized as a "high impact, low probability" threat. I believe a cyber-attack aimed at disrupting electric service would be a relatively cheaper and easier weapon to deploy than finding the needed nuclear materials to assemble and deploy a sophisticated weapon. So clearly we must place more effort and resources on mitigating the highest and most probable risks. I have included a "threat landscape" visual produced by the North American Reliability Corporation (NERC) on the next page for your reference.

U.S. Senate Committee on Energy and Natural Resources
May 4, 2017, Hearing: The Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure and to Improve Capabilities for Adequate System Restoration
Questions for the Record Submitted to Mr. Kevin Wailes



U.S. Senate Committee on Energy and Natural Resources
May 4, 2017 Hearing: The Threat Posed by Electromagnetic Pulse
and Policy Options to Protect Energy Infrastructure
and to Improve Capabilities for Adequate System Restoration
Responses Submitted by Dr. David Brumley at the
Request of the Honorable Newt Gingrich

Question from Chairman Lisa Murkowski

Question: One of the keys to a successful public-private partnership is trust and the willingness to share information. I am concerned, however, that there is a lack of trust by industry with the government – and for good reason. The December 2016 episode with Burlington Electric in Vermont is a perfect example. As I understand it, Burlington noticed an alert about a suspicious IP address that had connected to one of their computers and responded to that alert by dutifully reporting that fact to the government. The same day that they reported the alert, however, the Washington Post somehow learned about it and reported that Russian hackers had infiltrated the United States' electric grid. Later follow-up would show that the IP address was not necessarily linked to Russia and there was not malicious activity, but the damage to trust had been done. How do we restore and build trust between the private sector and government so that this type of information can be freely shared without concern about it becoming a media spectacle?

Response to Part 1: ***"How do we restore and build trust between the private sector and government"*****:** Plainly speaking, there is no upside to reporting, only potential downside.

No upside: Typically the government has no ability to stop an intrusion during an event, and has little ability to find attackers after an event. It's like reporting to the cops your car window was broken and your radio stolen: they will take note of it, but don't expect to get anything back.

The potential downside: The company risks when reporting include at least:
- Potential liability issues to their customers
- Reputation loss if the information becomes public

Overall, I would agree with the senators statement: "One of the keys to a successful public-private partnership is trust and the willingness to share information." However, I believe a much more significant factor in a successful public-private partnership is value in both sides.

In the car analogy, the value to a citizen to reporting to the police is often such a report is needed for insurance purposes, while the benefit to the police is situational awareness.

Response to Part 2: ***"This type of information can be freely shared without concern about it becoming a media spectacle?"*** I do not know the specifics of how the Washington Post became aware of the incident, and therefore cannot comment on the specifics.

In general, I do believe that companies should be able to report security incidents to the US government without fear of it being leaked. I do believe there are many such places one could report an incident, including US-CERT and the FBI Infraguard (https://www.infragard.org/). Both provide strong privacy to the reporter.

○