EXAMINING VULNERABILITIES OF AMERICA'S POWER SUPPLY

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT &
SUBCOMMITTEE ON ENERGY

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

September 10, 2015

Serial No. 114–37

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
97–756PDF WASHINGTON : 2016

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

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
F. JAMES SENSENBRENNER, JR., Wisconsin
DANA ROHRABACHER, California
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
BILL JOHNSON, Ohio
JOHN R. MOOLENAAR, Michigan
STEVE KNIGHT, California
BRIAN BABIN, Texas
BRUCE WESTERMAN, Arkansas
BARBARA COMSTOCK, Virginia
DAN NEWHOUSE, Washington
GARY PALMER, Alabama
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
ALAN GRAYSON, Florida
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
KATHERINE M. CLARK, Massachusetts
DON S. BEYER, JR., Virginia
ED PERLMUTTER, Colorado
PAUL TONKO, New York
MARK TAKANO, California
BILL FOSTER, Illinois

SUBCOMMITTEE ON OVERSIGHT

HON. BARRY LOUDERMILK, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
BILL JOHNSON, Ohio
DAN NEWHOUSE, Washington
LAMAR S. SMITH, Texas

DON BEYER, Virginia
ALAN GRAYSON, Florida
ZOE LOFGREN, California
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON ENERGY

HON. RANDY K. WEBER, Texas, *Chair*

DANA ROHRABACHER, California
RANDY NEUGEBAUER, Texas
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
THOMAS MASSIE, Kentucky
STEVE KNIGHT, California
BARBARA COMSTOCK, Virginia
BARRY LOUDERMILK, Georgia
LAMAR S. SMITH, Texas

ALAN GRAYSON, Florida
ERIC SWALWELL, California
MARC A. VEASEY, Texas
DANIEL LIPINSKI, Illinois
KATHERINE M. CLARK, Massachusetts
ED PERLMUTTER, Colorado
EDDIE BERNICE JOHNSON, Texas

CONTENTS

September 10, 2015

Appendix II: Additional Material for the Record

EXAMINING VULNERABILITIES OF AMERICA'S POWER SUPPLY

THURSDAY, SEPTEMBER 10, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT &
SUBCOMMITTEE ON ENERGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:02 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Barry Loudermilk [Chairman of the Subcommittee on Oversight] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittees on Oversight and Energy

Examining Vulnerabilities of America's Power Supply

Thursday, September 10, 2015
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Mr. Richard Lordan, Senior Technical Executive, Power Delivery & Utilization Sector, Electric Power Research Institute

Ms. Nadya Bartol, Vice President of Industry Affairs and Cybersecurity Strategist, Utilities Telecom Council

Dr. Daniel Baker, Distinguished Professor of Planetary & Space Physics; Moog-BRE Endowed Chair of Space Sciences; Director, Laboratory for Atmospheric and Space Physics, University of Colorado Boulder

Dr. M. Granger Morgan, Hamerschlag University Professor, Departments of Engineering and Public Policy and of Electrical and Computer Engineering, Carnegie Mellon University.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT
SUBCOMMITTEE ON ENERGY

HEARING CHARTER

Thursday, September 10, 2015
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

PURPOSE

The Subcommittees on Oversight and Energy will hold a joint hearing titled *Examining Vulnerabilities of America's Power Supply* on Thursday, July 30, 2015, starting at 9:00 a.m. in Room 2318 Rayburn House Office Building. The purpose of this hearing is to examine the vulnerabilities of the national electric grid and the severity of various threats to the power supply if those threats are not adequately assessed and managed. The hearing will discuss various threats to the national electric grid, including: severe weather or other natural events; cyber, physical, or coordinated attacks; space weather; and electromagnetic pulse (EMP) attacks.

WITNESS LIST

- **Mr. Richard Lordan**, Senior Technical Executive, Power Delivery & Utilization Sector, Electric Power Research Institute
- **Ms. Nadya Bartol**, Vice President of Industry Affairs and Cybersecurity Strategist, Utilities Telecom Council
- **Dr. Daniel Baker**, Distinguished Professor of Planetary & Space Physics; Moog-BRE Endowed Chair of Space Sciences; Director, Laboratory for Atmospheric and Space Physics, University of Colorado Boulder
- **Dr. M. Granger Morgan**, Hamerschlag University Professor, Departments of Engineering and Public Policy and of Electrical and Computer Engineering, Carnegie Mellon University

BACKGROUND

The electricity infrastructure of the United States consists of power plants generating electricity, transmission and distribution lines, and transformers and substations, which all work together to bring power to American homes and businesses.

The stability, reliability, and security of the electric grid are important components to prevent extensive power outages that could interfere with the everyday lives of millions of Americans. However, the electric grid is vulnerable to a wide range of threats that could cut off power to families and businesses, including physical, cyber, EMP, and space weather threats.

Physical Threats

In August of 2003, a tree branch in Ohio – with the help of software issues and human error – caused a major power outage across the northeastern portion of the United States and part of Canada. The blackout was blamed for directly contributing directly to 10 deaths with further indirect impact on the surrounding population.[1] Even with one isolated incident, it took two days to return electricity to the entirety of the affected area.[2] After Superstorm Sandy in 2012, millions of people were left without power. Despite broad disaster relief efforts, it took thirteen days to restore power to at least 95 percent of customers in New York and eleven days to restore power to 95 percent of customers in New Jersey.[3]

In addition to natural events, man-made physical threats exist for the national grid. In 2013, unknown individuals led an attack on a Pacific Gas & Electric's Metcalf substation in California – severing six underground fiber optic lines and firing over 100 rounds of ammunition at transformers. The attack caused over $15 million in damage, but did not lead to any loss of power or life.[4]

Cybersecurity Threat

As the electric grid continues to be modernized and become more interconnected, the threat of a potential cybersecurity breach significantly increases. While there has been no reported cyber-attack that has resulted in widespread loss of power, there have been many attempted attacks. An investigation completed by USA Today earlier this year found that the United States' power grid "faces physical or online attacks approximately 'once every four days.'"[5] In addition, it appears that these cyber threats could be highly sophisticated. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into [industrial control] systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[6]

One area of potential vulnerability within the grid is the Supervisory Control and Data Acquisition (SCADA) systems, which have been in use since the 1970s. While, these systems have historically consisted of remote terminal units, which were often connected to a mainframe computer via telephone lines or radio connections, SCADA systems were not typically connected to central IT networks. These systems were also not designed with digital security features, so as SCADA systems were modified to connect to digital networks, potential access points for cybercriminals were created.

---

[1] Steve Reilly and Ryan Sabalow, "Power Grid Security Solutions and Ideas Arose After 2003 Blackout," USA Today, March 24, 2015, available at: http://www.nbcnews.com/news/us-news/power-grid-security-fears-surge-2003-blackout-n329381
[2] Ibid.
[3] Fahey, Johnathan, "Hurricane Power Outages After Sandy Not Extraordinary According To Report Analyzing Katrina, Past Storms," AP, available at: http://www.huffingtonpost.com/2012/11/16/hurricane-power-outages-after-sandy_n_2146393.html
[4] Reilly, Steve, "Bracing for a big power grid attack: 'One is too many,'" USA Today, March 24, 2015, available at: http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/
[5] Ibid.
[6] Campbell, Richard J., "Cybersecurity Issues for the Bulk Power System," Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

Electromagnetic Pulse

An electromagnetic pulse (EMP) is a burst of high power electromagnetic radiation that results from the detonation of nuclear weapons, or from non-nuclear devices that are designed to disrupt or destroy electronic equipment.[7]

In 2000, the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 established a Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (EMP Commission).[8] The EMP Commission was tasked with assessing the nature and magnitude of potential high-altitude EMP threats from hostile state or non-state actors that acquired a nuclear weapon; the vulnerability of the U.S. military and civilian infrastructure to EMP attacks; U.S. capability to repair and recover from damage inflicted by a domestic EMP attack; and the feasibility and cost of hardening select military and civilian systems against EMP attacks.

After the EMP Commission was reestablished in the National Defense Authorization Act for Fiscal Year 2006[9], it released a 2008 report that included recommendations on the preparation, protection and recovery of U.S. critical infrastructure against a possible EMP attack.[10] According to recent testimony from the Government Accountability Office, however, while the Department of Homeland Security has worked to address some of the vulnerability issues addressed in the 2008 report, it "has not fully coordinated with stakeholders in certain areas such as identifying critical assets or collecting information necessary to assess electromagnetic risks."[11]

Space Weather

In addition to manmade EMPs, a geomagnetic disturbance (GMD) brought on by naturally occurring solar weather events can cause an electromagnetic impact that can adversely impact the electric grid. In 1989, a GMD caused millions of Canadians to lose their power for approximately nine hours. During that incident, the electric grid collapsed within 92 seconds of the GMD event.[12]

Specifically, space weather is the term used to describe severe disturbances of the upper atmosphere and of the near-Earth space environment that can be caused by the magnetic activity of the sun.[13] Major occurrences that lead to space weather include solar wind; solar flares and

---

[7] GAO-15-692T, United States Government Accountability Office, Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, July 22, 2015, available at: http://www.gao.gov/assets/680/671554.pdf

[8] PL 106-398, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001. October 30, 2000. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-106publ398/content-detail.html

[9] PL 109-163, National Defense Authorization Act for Fiscal Year 2006. January 6, 2006. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-109publ163/content-detail.html

[10] GAO-15-692T, United States Government Accountability Office, Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, July 22, 2015, available at: http://www.gao.gov/assets/680/671554.pdf

[11] Ibid.

[12] Ibid.

[13] National Research Council, Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report (2008), 2008, available at: http://www.nap.edu/openbook.php?record_id=12507

coronal mass ejections; eruptive prominences; corotating interacting regions; and solar energetic particle events.[14]

Space weather can have an effect on everyday life, including: high-frequency radio communications, astronaut health, satellite function, and aircraft electronic systems. When a coronal mass ejection (a large explosion of "magnetic field and plasma from the Sun's corona"[15]) interacts with the Earth's magnetic fields it "creates colorful aurorae at high latitudes. More ominously, it can drive disturbances in the Earth's upper ionized atmosphere (ionosphere) that interfere with global navigation and communication systems, and can endanger electrical power grids through geomagnetically-induced currents (GICs)."[16]

There is also the potential of extreme space weather events, like the Carrington event of 1859, which resulted in failure of telegraph communications around the world and bright, colorful auroras in the sky.[17] A geomagnetic storm also occurred in May 1921, which suggests that while these extreme space weather events are rare, they could happen again in the future, with significant impact for modern, electricity-based technology.[18]

The "Smart Grid"

The nation's electric infrastructure is aging, and the electric power industry is in the process of modernizing it with its transformation to the "smart grid," or technology that provides an increased use of digital information and control technology to improve reliability, security, and efficiency of the electric grid. Research and development and private sector coordination towards incorporating smart grid technology was authorized in the Energy Independence and Security Act of 2007 (EISA) in order "to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth."[19]

In practice, the "smart grid" generally refers to a technology used to modernize utility electricity delivery systems using computer-based remote control and automation. These systems consist of two-way communication technology and modify computer processing that has been used for decades in other industries to functions on the electric grid.[20] In contrast, that vast majority of today's electric grid primarily delivers electricity in a one-way flow from generator to outlet, without automatic two-way communication between distribution and consumption sites.[21]

---

[14] McMorrow, Dan, "Impacts of Severe Space Weather on the Electric Grid," The MITRE Corporation, November 2011, available at: https://fas.org/irp/agency/dod/jason/spaceweather.pdf

[15] Space Weather Prediction Center, Coronal Mass Ejections, National Oceanic and Atmospheric Administration, available at: http://www.swpc.noaa.gov/phenomena/coronal-mass-ejections

[16] Gibson, Sarah, "Living with Space Weather (Baby, It's Charged Outside), The Blog, The Huffington Post, April 1, 2015, available at: http://www.huffingtonpost.com/sarah-gibson/living-with-space-weather_b_6981168.html

[17] Klein, Christopher, "A Perfect Solar Superstorm: The 1859 Carrington Event," History, March 14. 2012, available at: http://www.history.com/news/a-perfect-solar-superstorm-the-1859-carrington-event

[18] National Academy of Sciences, "Severe Space Weather Events – Understanding Societal and Economic Impacts Workshop Report (2008)," 2008, available at: https://www.nap.edu/download.php?record_id=12507#

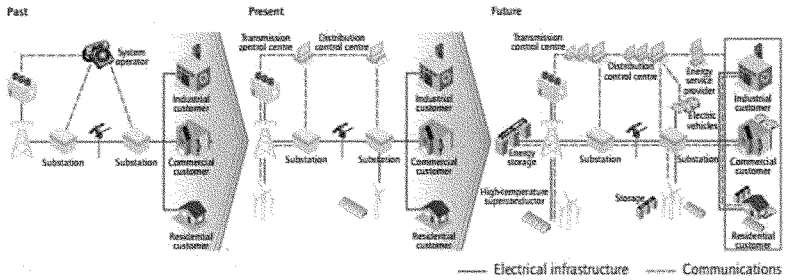
[19] PL 110-140, Energy Independence and Security Act of 2007. December 19, 2007. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-110publ140/content-detail.html

[20] Department of Energy, Office of Electricity Delivery & Energy Reliability, "Smart Grid," available at: http://energy.gov/oe/services/technology-development/smart-grid

[21] National Institute of Standards and Technology, "Smart Grid: A Beginner's Guide," available at: http://www.nist.gov/smartgrid/beginnersguide.cfm

The concern with the two-way communication aspect of the "smart grid" is that it opens up potential points of unauthorized system access and can present potential cybersecurity vulnerabilities. In addition, there are concerns with the security and privacy of smart electricity meters, which send data about energy use wirelessly to electric distribution companies and control the flow of power to customers.[22]

Figure 1. Smarter electricity systems



Source: International Energy Agency[23]

Complicating matters, components of the smart grid are controlled by software programming, which may make these devices and functions subject to manipulation over a network. Recent reports of cyber intrusions and malware found on industrial control systems are known to control energy flows on the electric grid, and include: BlackEnergy, HAVEX, and Sandworm.[24]

[22] Campbell, Richard J., "The Smart Grid and Cybersecurity -- Regulatory Policy and Issues," Congressional Research Service, June 15, 2011, available at: http://www.crs.gov/pdfloader/R41886
[23] International Energy Agency, "Technology Roadmap: Smart Grids," 2011, available at: https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf
[24] Ibid.

Chairman LOUDERMILK. The Subcommittee on Oversight and Energy will come to order.

Without objection, the Chair is authorized to declare recess of the Subcommittee at any time.

Good morning. I would like to thank our witnesses for being here today. I appreciate the witnesses' patience and understanding as we had to postpone this hearing from July. And I look forward to the testimony today that will help us examine the vulnerabilities of America's power supply.

Welcome to today's joint subcommittee hearing entitled "Examining the Vulnerabilities of America's Power Supply." Due to time constraints and in the interest of allowing our witnesses to be heard and their questions answered, I will submit my opening statement for the record and I encourage others to do so as well.

[The prepared statement of Chairman Loudermilk follows:]

PREPARED STATEMENT OF OVERSIGHT SUBCOMMITTEE CHAIRMAN BARRY LOUDERMILK

Good morning. I would like to thank our witnesses for being here today to help us examine the vulnerabilities of America's power supply.

The electricity infrastructure of the United States is aging, and the electric power industry is in the process of modernizing it with its transformation to the "smart grid" —the technology that provides an increased use of digital information and control technology to improve reliability, security, and efficiency of the electric grid.

That process of modernization, however, introduces new vulnerabilities in addition to ones that have existed for over a century. This hearing will discuss those various threats to the national electric grid, including: severe weather or other natural events; cyber, physical, or coordinated attacks; space weather; and electromagnetic pulse (EMP) attacks.

The blackout that darkened the Northeast in the summer of 2003 opened many eyes to the vulnerability and age of our electrical system. In that case, a tree branch in Ohio coupled with software issues and human error left many in the dark for two days. In addition to natural events like this and Superstorm Sandy—which left millions of people without power, man-made physical threats exist.

In 2013, unknown attackers coordinated an attack on a Pacific Gas & Electric Metcalf substation in California. Those attackers severed six underground fiber optic lines and fired over 100 rounds of ammunition at transformers. While the attack did not lead to any loss of power or life, it caused over $15 million in damage. The President and CEO of the American Public Power Association stated at a hearing last year that, "shooting at substations, unfortunately, is not uncommon."

Just as troubling is the amount of attempted cyber-attacks to the nation's electric grid. An investigation completed by USA Today earlier this year found that the United States' power grid "faces physical or online attacks approximately 'once every four days.'" In addition, in 2014, the National Security Agency (NSA) reported that it had tracked intrusions into industrial control systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems, and other critical infrastructure." We have also been examining cyber threats in the Homeland Security Committee, and this is an absolutely critical issue that must be taken seriously by Congress and the entire federal government.

On top of these threats, we also have the potential threat of an electromagnetic pulse, which would disrupt or destroy electronic equipment after the detonation of a nuclear weapon. Geomagnetic disturbances can also be brought on by naturally occurring solar weather events, such as in 1989 when a geomagnetic disturbance caused millions of Canadians to lose their power for about nine hours.

It is clear that there are many threats to our electric infrastructure, and we must therefore ensure that our federal systems are adequately protected, especially as we transition to the "smart grid." We need to rethink how we protect our facilities from physical attacks, like the Metcalf incident where investigators were never even able to identify the criminals.

In addition, as we have seen over the past few years, cybersecurity is an ever-evolving threat. The fact that we know of intrusions by entities with the capability to take down our control systems means that we must do everything in our power

to be proactive rather than reactive in order to protect our grid and prevent such a take-down from happening.

Mitigating these vulnerabilities and their potential consequences is ultimately essential for the safety and security of all Americans. Protecting our power supply is something that is crucial for day to day life activities and things that we take for granted—like heating and cooling a home or powering a business—as well as ensuring our national security.

I look forward to today's hearing, where I hope to learn more about the various vulnerabilities of our grid as well as the extent of the threats that could potentially leave us in the dark.

Thank you.

Chairman LOUDERMILK. I now recognize the Ranking Member of the Oversight Subcommittee, the gentleman from Virginia, Mr. Beyer, for an opening statement.

Mr. BEYER. Mr. Chairman, respecting your fine example, I will also submit mine for the record.

[The prepared statement of Mr. Beyer follows:]

PREPARED STATEMENT OF OVERSIGHT SUBCOMMITTEE
MINORITY RANKING MINORITY MEMBER DON BEYER

Thank you Chairmen Loudermilk and Weber for holding this important hearing today.

In September 1882 Thomas Edison flipped a switch that enabled the electricity generated from the Pearl Street power plant in lower Manhattan to power on 400 light bulbs for 82 customers living in a one-quarter square mile radius of each other, including 52 light bulbs at the New York Times. The electric grid was born and blossomed quickly, spreading across the country and around the world. Today the U.S. power grid is an intricate labyrinth of 200,000 miles of transmission lines, thousands of generating stations and hundreds of high voltage transformers.

This complex and interconnected power system fuels our national and global economy. It plays a key role in our national security. It enables the delivery of critical healthcare services. It improves our lifestyles in a multitude of ways, and provides emergency services that save lives. When the electric grid goes down today it is more than a passing inconvenience. The elderly and very young alike may die from a lack of access to critical medical services or availability of adequate heating or air conditioning. Police, fire and emergency response capabilities may be hindered. Businesses close. Grocery stores and gas stations may cease to open or operate. Hospitals may be unable to fully function effectively.

At the same time we have witnessed more and more severe weather events in the past few years that have disabled the grid, knocking down transmission lines and utility poles, flooding critical equipment and leaving customers without access to this critically important service for days on end. Reliant on the telecommunications infrastructure to operate and computer control systems to function the power grid has also become vulnerable to malicious cyber threats. Recent physical attacks on electrical power stations have highlighted the need to harden the grid against these kinds of threats. A successful, coordinated cyber and physical assault against key portions of the grid could leave cities or regions without power for long stretches of time. Geomagnetic Disturbances (GMDs), producing solar flares, can also disable portions of the grid and interfere with global navigation and communication systems. Electromagnetic Pulses (EMPs) intentionally produced by a weapon is one of the least likely, but most serious, threats to the power grid since its successful use would destroy critical electronic components that are vital for the grid's continued performance and could be difficult to replace quickly.

Protecting the power grid against all of these variables and potential vulnerabilities is not a problem that can be, or should be, faced by the utility industry alone. The government has a key role to play in ensuring that our shared reliance on electricity is as resilient as possible. The electric industry and federal government also need to have detailed plans for recovery operations if, or when, the electrical grid is degraded by natural disasters or intentionally disabled by malicious actors.

How we confront these multiple vulnerabilities and emerging threats is not straight-forward. There is no silver bullet to eradicating these threats. There is no cure-all for ensuring that the electric grid will never go down. It will—at times—as we have seen most recently due to the power of natural storms and the fragility

of our aging electrical infrastructure. Ensuring that we are prepared to recover from these potential events in a timely manner and able to restore power to critical facilities, such as hospitals, quickly demands our collective attention, from industry, the Administration and Congress.

Because I believe it is critically important that we are as prepared as possible to effectively deal with these potential incidents when they occur I asked the Government Accountability Office (GAO) to investigate these issues in a letter I sent to GAO yesterday. I would welcome other Members who are interested—on both sides of the aisle—to join me in this request. This is an important, non-partisan issue, and I am glad we are holding this hearing today.

I look forward to learning more about these important issues from our witnesses and hearing about any recommended actions they have to help keep the lights on as long as possible and get them back on as quickly as possible should they go out—regardless of the reason why.

I yield back.

Chairman LOUDERMILK. Thank you, Mr. Beyer. I appreciate that.

Now, I recognize the Chairman of the Energy Subcommittee, the gentleman from Texas, Mr. Weber, for an opening statement.

Mr. WEBER. Thank you. My opening statement is that I submit my opening statement for the record. Welcome.

[The prepared statement of Mr. Weber follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON ENERGY CHAIRMAN RANDY K. WEBER

Good morning and welcome to today's joint Oversight and Energy Subcommittee hearing examining vulnerabilities of America's power supply. Today, we will hear from a broad range of witnesses on the existing threats to the nation's electric grid, and the impact that potential attacks and incidents could have on our grid reliability and national security.

Our witnesses today will also provide insight into how industry and the federal government can work together to harden our electric grid against ongoing and changing threats.

The reliability of America's power grid is one of our greatest economic strengths. In my home state of Texas, reliable and affordable power serves a population that is increasing by more than 1,000 people per day, and provides power to the energy intensive industries that drive consumption. Texas is by far the nation's largest consumer of electricity. Keeping the Texas power grid reliable and secure is key to continuing this economic growth.

But it is common knowledge that utilities face significant and diverse threats to the reliability of power delivery. Our electric grid is vulnerable to physical threats caused by damage to existing infrastructure and growing cybersecurity threats as the grid is modernized.

Key infrastructure such as utility substations are often left completely exposed, with little more than a chain-link fence protecting the facilities that keep the lights on across the country. Small scale cyber and physical attacks to our electric grid are estimated to occur once every four days. And in over 300 cases of significant cyber and physical attacks since 2011, suspects have never been identified.

Our power grid is also at risk from geomagnetic disturbances, which can be caused by space weather or an Electromagnetic Pulse, commonly known as E-M-P, which could be generated in a nuclear attack. These high energy pulses could severely impact the operation of the electric grid and electric power systems across the country, disabling and damaging equipment essential to providing reliable power that could be nearly impossible to replace on a large scale.

We often think of cybersecurity and other threats to the power grid at a macro scale, but these types of attacks can occur even at the local level. In 2011, the Pedernales Electric Co-op, a non-profit co-op that serves approximately 200,000 customers north of San Antonio, was struck by a cyberattack. While the attack thankfully did not disrupt electric reliability, it is a stark reminder that threats to the grid are real, and are not going away.

Our nation's power supply cannot be protected overnight, particularly as utilities struggle to adapt technology to manage a growing number of cybersecurity threats. Cyber threats to the power grid will continue to evolve, particularly as more interconnected smart technologies are incorporated into the electric grid. As protective

technology improves, so does the capability and creativity of those conducting attacks.

While we cannot predict every method of attack, the federal government can and should play a role in assisting industry with developing new technology and security safeguards.

Accordingly, research and development efforts at the Department of Energy are focused on providing industry with comprehensive tools to conduct internal analysis to identify and address cybersecurity weaknesses so that industry can take the lead in addressing these vulnerabilities.

I want to thank our witnesses for testifying before the Committee today, and I look forward to a discussion about the threats to America's reliable power supply and the federal government's role in helping to secure our electric grid.

Chairman LOUDERMILK. Thank you, Chairman Weber.

I now recognize the Ranking Member of the Subcommittee on Energy, the gentleman from Florida, Mr. Grayson, for an opening statement.

Mr. GRAYSON. Ditto.

[The prepared statement of Mr. Grayson follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON ENERGY
MINORITY RANKING MEMBER ALAN GRAYSON

Thank you, Chairman Loudermilk, and Chairman Weber, for holding this hearing today. Today's hearing is focused on our nation's electric grid, and the many threats facing it.We as a society are increasingly dependent on the services electricity provides, and the electric grid has quietly become the basis of our modern lives. However, our electrical system is under constant stress from severe weather, malicious acts, and age. The stress on the system is constantly increasing as we dramatically change how we want to use the grid now, verses what it was designed to do, when it was built.

In 2000, the US experienced an average of 2.5 grid disruption events a month. Fourteen years later, in the first half of 2014, we had an average of 21.7 disruptions a month - a nearly nine-fold increase.

Between 2003 and 2012, 80 percent of all outages were weather related and cost the US economy an inflation-adjusted annual average of between $18 billion to $33 billion.

USA Today recently reported that physical and cyber attacks on the power grid occur about once every four days. In April of 2013, unknown snipers disabled 17 transformers with a .30 caliber assault rifle at the Pacific Gas & Electric Company's Metcalf substation outside of San Jose, California. The assailants fired 150 rounds and escaped undetected. They had cut a series of fiber-optic telecommunications cables prior to the attack hindering communication.

From malware inserted in electrical components used to operate the power grid prior to purchase by utilities to traditional cyber attacks, disabling even a portion of the nation's power supply can have serious consequences for the health and safety of our citizens.

Keep in mind, that the average age of a high voltage transformer in the United States is approximately 38 to 40 years old, with 70 percent of them 25 years or older. And that most high voltage transformers are custom built, and can take five to twenty months to design, build, deliver and install.

One of our challenges is grappling with the reality that many of these threats to the grid are not easily predicted with current capabilities.

High-impact low probability events are by definition, rare. We do not know when a large-scale malicious attack might happen, whether it's an electromagnetic pulse or a cyber attack. We have limited abilities to predict when a geomagnetic disturbance or extreme weather event will hit. And since these events rarely happen, we have little or no historical data to guide us.

While we should certainly support efforts to significantly improve our grid security capabilities, we cannot assume that it is even possible to completely protect the grid from every possible risk.

What we can do is increase our ability to estimate these risks. We can improve our ability to predict the impacts, even when we may not be able to predict the actual event. And we can take actions to improve our electric system's ability to withstand an event, and minimize the time it takes to recover from that event.

This Committee has an important responsibility to authorize research that can dramatically improve the ability of the grid to handle whatever comes at it.

Over the past 100 years we have incrementally created our electric grid, adding and subtracting equipment as the system expanded and became more interconnected. Our electrical system is considered one of the greatest engineering achievements of the 20th century by the National Academy of Engineering. We should be proud of this accomplishment.

I look forward to working with my colleagues to identify and fund the research efforts needed to make sure our electrical system remains a great achievement.

I thank each of our witnesses for being here today, and I look forward to hearing what each of you has to say.

Thank you, Mr. Chairman, and I yield back my remaining time.

Chairman LOUDERMILK. Thank you, Mr. Grayson.

And is Ms. Johnson not here? Okay.

At this time I would like to introduce our witnesses. You don't have the option, okay, so—we wouldn't get anywhere if you guys follow suit, so we did this so you would have plenty of time.

Our first witness is Richard Lordan. He is the Senior Technical Executive of the Power Delivery & Utilization Sector at the Electric Power Research Institute.

Our next witness is Ms. Nadya Bartol—is the Vice President of Industry Affairs and Cybersecurity Strategist at Utilities Telecom Council where she works on UTC cybersecurity initiatives worldwide.

Our next witness is Dr. Daniel Baker. He is the Director of the Laboratory for Atmospheric and Space Physics at the University of Colorado Boulder. He is a distinguished professor of planetary and space physics and the Moog-BRE. Is that proper? Okay. Endowed Chair of Space Sciences at the university.

And our final witness is Dr. M. Granger Morgan. He is the Hamerschlag University Professor in the Department of Engineering and Public Policy at Carnegie Mellon University where he is also professor in the Department of Electrical and Computer Engineering.

Thank you all for being here and I now recognize Mr. Lordan for five minutes to present his testimony.

MR. RICHARD LORDAN, SENIOR TECHNICAL EXECUTIVE, POWER DELIVERY & UTILIZATION SECTOR, ELECTRIC POWER RESEARCH INSTITUTE

Mr. LORDAN. Good morning, Chairman Weber and Mr. Loudermilk, Vice Chairman Knight and Johnson, Ranking Members Mr. Beyer, and members of the subcommittees. I am Richard Lordan, Senior Technical Executive at EPRI Transmission. I'm pleased to testify today on vulnerabilities of the electric grid.

For those of you who don't know, EPRI is a 501(c)(3) nonprofit organization that conducts research and development relating to generation, delivery, and use of electricity for the benefit of the public. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States. International participation extends to over 30 countries.

So my testimony is going to be kind of in two parts. One is on the general vulnerability of the grid and then I'm going to bore down on one threat which is electromagnetic pulse.

When I talk about the vulnerability of the grid, I'm really talking about vulnerability to high-impact, low-frequency events. They

called them HILF events, and they are rare but they have a high impact. And some of these things include natural events like severe weather, earthquakes, geomagnetic disturbances, and also man-made threats like physical security and EMP, which I'm going to talk about today.

So you asked about the vulnerability of the grid, and there are inherent vulnerabilities in the grid to these threats because the severity is generally higher than the design basis for the system. To completely eliminate these vulnerabilities would be cost prohibitive. It would defeat the industry's objective of providing reliable, safe, environmentally acceptable, and affordable power.

EPRI supports a prudent approach where you assess the vulnerabilities from all of these threats, calculate the impact should these events occur, and develop cost-effective countermeasures that improve transmission system resiliency.

I'm now going to talk about EMP with a comparison to geomagnetic disturbance. EMP and GMD are often conflated but there are important differences that I'll highlight. Dr. Baker could probably add some more. EMP, electromagnetic pulse, refers to a very intense pulse of electromagnetic energy typically caused by the detonation of a nuclear device or other high-energy explosive device.

There are three stages of an EMP and I'm pretty sure you know what they are but I'll do it again: E1, E2, and E3. The E1 is characterized by an incredibly fast rise time high-energy pulse. It has the ability to destroy electronics in the power system, and it affects itself by the electric field itself or by coupling to wires that are attached to these devices.

The E2 is similar to lightning and consequently can result in damage to electronics and potential flashover of distribution class insulation.

E3 is characterized by a longer duration, low-frequency content similar to GMD, and that's why people talk about EMP and GMD together. But the E3 part of EMP is much shorter than a GMD, and therefore, it will not have the consequence of transformer overheating and failure. It does have the ability to saturate transformers and transformers will create harmonics. They'll consume reactive power and there may be voltage collapse on the system.

With regard to risk management of these threats, so we talked about EMP and vulnerability. EPRI is leading an effort with the industry to characterize each of these threats, whether it's EMP, GMD, physical security or cyber, characterize the threat, then identify the key component—key components in the system and understand the vulnerability of those components, then assess the impact should this event happen. What's the effect on the system and what's the societal cost? Then we develop and assess mitigation strategies that will buy down that risk.

And lastly, after we've done all the different threats one by one, we support looking sideways and seeing, hey, are there any mitigation strategies that also support multiple threat that would improve your business case by increasing transmission resiliency?

So thank you again for inviting EPRI here today and I look forward to answering your questions.

[The prepared statement of Mr. Lordan follows:]

Written Testimony

Hearing of the House Science, Space and Technology Committee
Joint Subcommittees on Oversight and Energy

United States House of Representatives

Mr. Richard Lordan
Senior Technical Executive - Transmission
Electric Power Research Institute

"Examining Vulnerabilities of America's Power Supply"

September 10, 2015

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 US, and international participation extends to more than 30 countries.

EPRI's testimony focuses on: 1) the threat of high-impact, low-frequency events to the grid including Electromagnetic Pulse and other electromagnetic threats including Geomagnetic Disturbance and Intentional Electromagnetic Interference; and 2) risk management approaches to address EMP threats. These remarks are based upon EPRI research as well as industry knowledge and public domain documents.

1) High-Impact, Low-Frequency Events

High-impact, low-frequency (HILF) events are of growing concern in the power industry. HILF events include severe weather and other natural events; cyber, physical, or coordinated attacks; pandemics; unanticipated severe shortages of fuel or water for power generation; and electromagnetic pulse (EMP) and intentional EM interference (IEMI) attacks. There are inherent vulnerabilities in the transmission grid system to these threats because their severity is generally greater than the design basis for the system. To eliminate these vulnerabilities would be cost prohibitive, and would defeat the industry's objective to provide reliable, safety, environmentally responsible *and* affordable power.

The prudent approach is to assess the vulnerabilities, understand the impacts should these types of events occur, and develop cost-effective countermeasures to reduce the risk by increasing system resiliency. In the context of the transmission system, "resiliency" is the ability to harden the system against – and quickly recover from – HILF events, which include both severe weather, including space-weather, and man-made attacks. HILF events can disrupt generation, transmission, and distribution systems, as well as interdependent systems such as natural gas pipelines, other fuel transport, and telecommunications. Utilities have a large number of possible mitigating technologies from which to choose to enhance transmission resiliency in the face of HILF events.

Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD) are often discussed together when evaluating potential impacts on the power system and approaches for improving system resiliency. While these events are both in the category of electromagnetic high-impact, low-frequency events (along with physical attacks, severe storms, earthquakes, and other events), there are very important differences between EMP and GMD events that should be understood when evaluating resiliency improvement priorities and investment decisions.

Electromagnetic Pulse (EMP)
EMP refers to a very intense pulse of electromagnetic energy, typically caused by detonation of a nuclear or other high-energy explosive device. High-altitude EMP (HEMP) is a nuclear warhead detonated hundreds of kilometers above the Earth's surface to produce more widespread effects (areas impacted can be hundreds of kilometers in diameter). It is generally accepted that a HEMP will require a high-altitude delivery device (e.g., a missile) which will require a high level of sophistication and logistics. As a result, the HEMP threat is often associated with potential attacks from nation entities.

- EMPs are intentional man-made attacks of electro-magnetic energy specifically for the purpose of disrupting and/or damaging electrical/electronic systems. The three portions of the EMP may have different impacts on the transmission systems (see figure 1).
    - E1 – very fast rise time, may result in damage to electronic components either directly, or by coupling into the attached wires. GMDs do not have this characteristic.
    - E2 – characteristics are similar to lightning and consequently can result in damage to electronics and potential flashover of distribution class insulation. Neither GMD nor IEMI have this characteristic.
    - E3 – characterized by a longer duration and low frequency content similar to GMD but much shorter in duration. EMP has two potential grid impacts similar to geomagnetically-induced currents (GICs): (1) increased reactive power consumption and (b) potential protection system mis-operation from harmonics. A third potential impact of GICs, localized heating in transformers, is considered unlikely from EMP E3 because the duration of an EMP E3 is short in relation to the thermal time constant of power transformers.

- EMPs can occur with little or no warning. With the possible exception of enhanced visibility tools, most operational strategies are inapplicable. Therefore, response to the EMP threat generally comes in the form of hardening assets to reduce initial damage, and recovery to reduce the duration of the interruption.

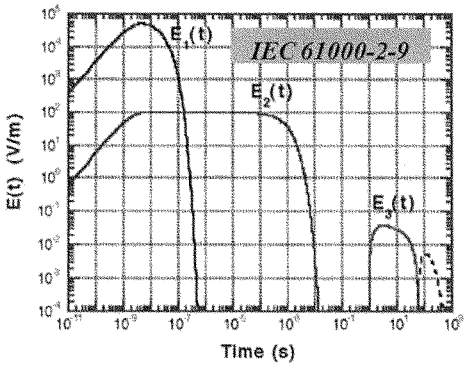


Figure 1: EMP Characteristics: Electric field magnitude as a function of time for an EMP pulse.

Geomagnetic Disturbance (GMD):

- GMDs are natural phenomena which generate slowly changing (quasi-DC) currents. These currents are similar to those created in the E3 portion of an EMP; however the E3 duration of an EMP is much shorter than a significant GMD.
- Locations that are closer to the Earth's poles are more susceptible to GMD than lower latitudes. Space weather warning systems provide a coarse estimate of GMD activity as much as four days before the storm reaches the Earth. These systems use direct observations of the sun. Accuracy of the forecast improves when the storm reaches the DSCOVR satellite, about one hour before the storm reaches the Earth. DSCOVR is a NOAA Earth observation and space weather satellite launched on February 11, 2015. It is positioned at the Sun-Earth L_1 Lagrangian point, 930,000 miles from Earth, to monitor solar wind condition, provide early warning of approaching corona mass ejections and observe phenomena on Earth including changes in ozone, aerosols, dust and volcanic ash, cloud height, vegetation cover and climate.
- Monitoring systems have been installed in multiple locations which measure the GIC currents in transformers across the grid.
- GMD events, many of which are low magnitude, occur on a regular basis which enables grid operators to improve their understanding of the phenomena, determine the impact on the grid, and evaluate trial countermeasures. These small storms can provide an indication of the grid's response to severe storms, and support development of prudent operational strategies.
- Although severe storms can occur any time during the approximately eleven-year solar cycle, more storms occur during the peak of the solar cycle.
- GMD storm duration can be in the order of hours or days while the duration of EMP is considered to be in the order of minutes.
- Utilities have established operational strategies to mitigate risk during GMD events.

Other Electromagnetic Threats

Intentional Electromagnetic Interferences (IEMI)

Like EMP, IEMI generates and delivers electromagnetic energy. IEMI is generated and delivered locally, and employs no nuclear material. IEMI devices have the potential to impact electronic assets in nearby locations such as control centers. Critical electronic equipment in these locations include

relays, supervisory communications and data acquisition (SCADA), communications, and energy management systems (EMS).

As stated earlier, there are inherent vulnerabilities in the grid system to these threats because their severity is generally greater than the design basis for the system. Today's power systems are operating in an increasingly complex electromagnetic environment in which large current and voltage components, sensitive electronics, digital signals, and analog waveforms coexist and interact. The widespread proliferation of smart grid systems, including substation automation and syncrophasor systems, are part of this increasing complexity.

2) Risk Management Approaches to Address EMP Threats

EPRI has worked with industry stakeholders to characterize EMP threats, including HEMP attack, EMP, and local IEMI attack. This work has provided the design basis for assessing vulnerability and developing mitigation strategies. EPRI has gathered available data on component vulnerabilities to the benchmark threats. The results, when complete for all critical components, will support calculation of the system impact. EPRI has gathered leading practices by electricity providers who have applied trial implementation of countermeasures to reduce vulnerability.

A number of risk-management approaches can be considered to reduce the impact of EMP on the transmission system. Some of these methods are being considered by various utilities for implementation:

Risk Assessment
Prudent application of scarce resources requires careful countermeasure and site selection. While it may be difficult to identify regions of the grid that are more likely to be attacked by an EMP, it may be possible and prudent to identify and focus resources on the most critical components necessary for the reliable operation of the transmission system.

Hardening of Assets
Hardening for new and existing systems generally focuses on reducing the impact of electromagnetic waves on electronic equipment. Some hardening options include:

- New control rooms with EM shielding in the form of a Faraday Cage are being implemented at some locations. Cable entrances may be considered, including the number and location of penetrations as well as the implementation of surge protection, filtering and grounding strategies. Other challenges include staff entrances/exists and ventilation ducts.
- New relay houses which are EMP hardened are being developed and tested by some utilities. These relay houses utilize metal buildings with special consideration to ensure bonding of metal members, improved grounding, and cable entrances.
- The use of power supply and communication cables with integrated shields, as well as consideration for the grounding strategies for these shields, are being implemented (e.g., individually-shielded twisted pair cables with an overall shield which is grounded).
- Surge protection and grounding of cables entering and exiting the facilities is routine practice due to everyday lightning activity that could affect the electronic equipment.
- Filtering can be applied at cable entry points to reduce high-frequency conducted energy which can impact the attached electronic activity.
- Relocation of unprotected, sensitive control equipment to inside the shielded enclosures.
- Relocation of control cables to a lower EM environment, such as conductive conduit, to reduce induced voltage.

- The use of fiber optic cables rather than metallic cables for communications. Fiber optic cables have much lower susceptibility to EM impacts.
- Utilities are engaging original equipment manufacturers (OEMs) to incorporate EM resiliency into new components, such as relays and communications systems.
- Neutral blockers for transformers to reduce the impact of GMD have been implemented. These blockers may aid in the reduction of induced E3 currents. The impact of neutral blockers on system operation requires consideration.

Recovery

- Because a severe EMP attack can damage key electronic system components, strategic sparing is prudent. Sparing can be considered for relays, which are susceptible to the E1 and E2 component of an EMP. Storing critical spares in shielded EM enclosures is a consideration.
- Other equipment which supports restoration could also be protected from EMP. This includes equipment associated with black start, backup communications systems, transportation, and diagnostics components.
- Asset owners may consider adding the EMP threat to their transformer spares strategy. Lower voltage transformers below 69 kV can be affected by the E1 and possible E2 portions of an EMP. Larger power transformers are unlikely to be impacted directly.
- In addition to spares, mobile systems to support recovery can be considered, such as mobile transmission capacitor banks, mobile substations (typically for distribution), and mobile substation control houses.
- Redundant systems can be applied which are not susceptible to EMP, such as electro-mechanical relays.
- Utilities may consider disconnecting, and possible grounding, redundant relays and communication systems that are installed, so that they are available after an EMP. However, caution is warranted for this approach because system resiliency to traditional threats may be compromised.
- Restoration plans and training can be embellished to incorporate recovery from EMP. Relay technicians will be especially important to EMP recovery.

Conclusion

EPRI looks forward to offering continued technical support to the electricity sector, public policy-makers and other stakeholders to ensure safe, reliable, affordable, and environmentally-responsible electricity.

Chairman LOUDERMILK. I now recognize Ms. Bartol for five minutes to present her testimony.

TESTIMONY OF MS. NADYA BARTOL,
VICE PRESIDENT OF INDUSTRY AFFAIRS
AND CYBERSECURITY STRATEGIST,
UTILITIES TELECOM COUNCIL

Ms. BARTOL. Good morning, Mr. Chairman, and Members of the Subcommittee. My name is Nadya Bartol. I'm the Vice President of Industry Affairs and Cybersecurity Strategist at the Utilities Telecom Council. Thank you for the opportunity to testify today about the vulnerabilities of America's power supply.

UTC is a global trade association for the communications and information technology interest of electric, gas, and water utilities; pipeline companies; and other critical infrastructure industries.

Cybersecurity is a serious concern with respect to great vulnerability. It is a complex challenge that requires comprehensive process-driven solutions. It is and will remain a risk we must actively manage as long as society wants to have the conveniences of a modern world increasingly underpinned and enabled by smart interconnected technologies.

Some of the variables in the complex cybersecurity grid vulnerability landscape are outside of our span of control. Although there are a number of variables within our control, there's no easy way to fix them either, as mitigating those variables to an acceptable level may take a long time.

With respect to what is outside of our span of control, the grid is vulnerable to a variety of threats, including individual hackers, activist groups, cyber criminals, and nation states.

With respect to what is within our span of control, those vulnerabilities are related to the shortage of qualified cybersecurity workforce, age of legacy infrastructure, lack of legal framework for information sharing, and evolving practices for assuring security in supplier products and services.

The 2015 Global Information Security Workforce Study, an international survey of nearly 14,000 information security professionals published by ISC2, estimates the shortfall in the global information security workforce to reach 1.5 million by 2020. This problem is exacerbated in the energy space because we have two different sets of systems: systems that run the grid, referred to as operational technology (OT) and business systems that we refer to as information technology (IT). These two sets of systems command a different set of priorities that are served by individuals with different backgrounds, different vocabularies, and different goals and objectives.

We need to educate and train more people with a skill set blended across those two types of systems, IT and OT, in order to make a noticeable difference. This challenge impacts the energy utilities, numerous vendors that supply systems for the grid, as well as the integrators who design and integrate larger, more complex systems for utilities. The deficit of cybersecurity workforce permeates all levels of the energy utility organization, and the same is true for the entire energy utility ICS and ICT supply chain.

The technology of the grid is in itself a cybersecurity concern. The grid is based on layers that have accumulated over time, and the legacy structure was not designed to be secured because security was not a concern when that infrastructure was implemented. And utilities have been utilizing a variety of technologies, methods, and techniques to help manage and mitigate some legacy infrastructure's vulnerabilities. However, this is an ongoing concern, and acquiring and implementing such technologies, modifying network architectures, or replacing legacy infrastructure takes time and resources.

The energy sector suffers from inconsistent threat information throughout the sector. Progress has been made but we still need a legal framework for information sharing that would remove the barriers that remain. Building robust systems that can be resilient in the face of cybersecurity threats requires considering security from inception. Utilities rely on vendors for systems design, development, implementation, and maintenance and are working on their approaches to productively communicate their assurance needs and then monitor the underperformance against those.

Recently published standards and best practices provide requirements, methods, and techniques that help address this challenge. This includes NIST Cybersecurity Framework which is broadly used in the energy space.

Cybersecurity is a complex challenge that cannot be solved overnight or permanently. It does not lend itself to a cookbook of solutions, nor can we envision every possible scenario to mitigate. We're dealing with an asymmetric threat. However, we can act to reduce the cyber-related vulnerabilities of the grid. These actions include increasing supply of cybersecurity workforce that understands both IT and OT contexts, financially enable utilities to upgrade or phase out their legacy infrastructures, enacting information-sharing legislation that removes current barriers, and supporting industry-based standardization and NIST framework implementation to help integrate security considerations into current and future technologies.

I look forward to further dialogue.

[The prepared statement of Ms. Bartol follows:]

Executive Summary

Statement of Nadya Bartol

Vice President, Industry Affairs and Cybersecurity Strategist

Utilities Telecom Council

Before the

Subcommittee on Oversight and Subcommittee on Energy

Committee on Science, Space, and Technology

U.S. House of Representatives

September 10, 2015

Founded in 1948, the Utilities Telecom Council (UTC) is a global trade association for the communications and information technology interests of electric, gas and water utilities, pipeline companies and other critical infrastructure industries – both here in the United States and in other parts of the world. The Council serves as the source and resource for our members to deploy technology and solutions that deliver secure, reliable and affordable mission critical services. UTC's mission is to shape the future of utility mission critical technologies by driving innovation, fostering collaboration and influencing public policy.

Summary of the major points of my testimony:

- Cybersecurity cannot be completely solved, and will remain a risk we must actively manage.
- Relying strictly on technical solutions to solve cybersecurity is insufficient and dangerous because people will always circumvent the technology if they are motivated to do so.
- The grid is vulnerable to a variety of threats including individual hackers, activist groups, cyber criminals, and nation states. We can monitor, better understand, and mitigate this threat, but fundamentally it is outside of our span of control.
- Those vulnerabilities that are within our span of control require long-term solutions: shortage of qualified cybersecurity workforce, age of legacy infrastructure, lack of legal framework for information sharing, and evolving practices for assuring security in supplier products and services.

Statement of Nadya Bartol
Vice President, Industry Affairs and Cybersecurity Strategist
Utilities Telecom Council
Before the
Subcommittee on Oversight and Subcommittee on Energy
Committee on Science, Space, and Technology
U.S. House of Representatives
July 30, 2015

Good morning Mr. Chairman and Members of the Subcommittee. My name is Nadya Bartol. I am the Vice President of Industry Affairs and Cybersecurity Strategist at the Utilities Telecom Council. Thank you for the opportunity to testify today about the vulnerabilities of America's power supply.

Background

Cybersecurity presents a serious concern with respect to grid vulnerability. It is a complex challenge that requires comprehensive process-driven solutions. Cybersecurity cannot be completely solved, and will remain a risk we must actively manage as long as society wants to have the conveniences of a modern world increasingly underpinned and enabled by smart interconnected technologies. Technology industry estimates that by 2020 there will be 50 billion interconnected smart devices in the world. Many of those devices will run our electric grid, smart cities, and smart cars. These devices will support and enable improved quality of life we have come to expect from our technology.

Relying strictly on technical solutions to solve cybersecurity is insufficient and dangerous. Today, we can use available technology solutions designed to reduce cybersecurity risks. However, people will inevitably circumvent technology in order to reduce costs, increase efficiencies or just to prove that they can beat the technology. Furthermore, as recent breaches have taught us, lack of understanding and/or training means that even with robust technology solutions our defenses fail us if

people do not understand what the technology is telling them. Whatever the motivation we need to acknowledge and manage the human factor of cybersecurity.

Today's grid is quite resilient. Since the Northeast Blackout in 2003, utilities have implemented reliability standards and smart grid technologies that should substantially reduce the risk of a similar physical world cascade event. These measures will also work to limit the impact of any individual, single point of failure, cyber-related event. Furthermore, the electric industry is working continuously to manage cybersecurity risks and address evolving cybersecurity threats, regulatory requirements, and emerging technologies. Cybersecurity practices in the electric industry are subject to mandatory cybersecurity requirements under the North American Electric Reliability Corporation (NERC) Critical infrastructure Protection (CIP) standards. These standards have improved cybersecurity practices throughout the US energy market. This includes even those companies who are not subject to regulatory jurisdiction, but nonetheless look to these standards for guidance.

In the past, the systems that utilities used to monitor and manage the grid were isolated from the Internet. As utilities have implemented smart grid and other advanced technologies, they have created new and numerous connections across the distribution grid and beyond the utility meter into the home. While these connections should not be direct and can be architected, designed, and operated to minimize risk exposure, the connections' existence by its very nature presents an ongoing risk.

"Security by obscurity" for industrial control systems (ICS) has rapidly disappeared. In addition to the growing interconnection between traditional ICSs and corporate enterprise networks, we have seen a move away from control systems utilizing highly proprietary hardware, software, and protocols. While proprietary protocols are still used , the underlying technology is now largely IT-based, sharing fundamental similarities with traditional IT enterprise network components and more easily

discoverable and understood by the hacker community. Increased use of common IT-based technology exponentially increases the exposure of the electric grid to cyber threat.

Discussion

Some of the variables in the complex cybersecurity grid vulnerability landscape are outside of our span of control. Those can only be mitigated to a certain extent. And while there are a number of variables within our control, there is no easy way to fix them either as mitigating those variables to an acceptable level may take a long time.

With respect to the **vulnerabilities that are outside of our span of control**, the grid is vulnerable to a variety of threats including individual hackers, activist groups, cyber criminals, and nation states. Evidence from several published reports by security researchers, government organizations, and the industry indicates that the threat from nation states has recently increased. I am referring to the Havex and Black Energy malware that has been described in ICS CERT alerts ICS-ALERT-14-176-02A and ICS-ALERT-14-281-01B published in June and December of 2014, respectively. Those two threats specifically target ICSs and related product vendors. Additionally, the Operation Cleaver report that was published by Cylance in December 2014 details activities stemming from Iran that target energy and utility companies throughout the world, including the US and Canada.

With respect to the **vulnerabilities that are within our span of control**, those are related to the shortage of qualified cybersecurity workforce, age of legacy infrastructure, lack of legal framework for information sharing, and evolving practices for assuring security in supplier products and services.

Shortage of qualified and knowledgeable cybersecurity workforce in the energy space. The 2015 Global Information Security Workforce Study, an international survey of nearly 14,000 information security professionals published by ISC^2, estimates the shortfall in the global information security

workforce to reach 1.5 million by 2020. Furthermore, 86 percent of respondents to the ISACA's 2015 Global Cybersecurity Status Report, which surveyed more than 3,400 ISACA members, identified a cybersecurity skills gap. 92 percent of respondents planning to hire more cybersecurity professionals said they expect to have difficulty finding skilled candidates. This problem is exacerbated in the energy space because we have two different sets of systems – systems that run the grid, referred to as Operational Technology (OT) and business or enterprise systems that we refer to as Information Technology (IT). These two sets of systems command a different set of priorities and are served by individuals with different backgrounds, vocabularies, and goals. UTC members have told us that they have tried transplanting an individual from IT to OT and vice versa with somewhat mixed success. We need to educate and train more people, a lot more people, with a skillset blended across IT and OT in order to make a noticeable difference.

This challenge impacts the energy utilities, numerous vendors that supply systems for the grid, including ICSs and communications devices, as well as the integrators who design and integrate larger more complex systems for utilities. Because these systems existed in isolation in the past and were not required to be secure, the ICS manufacturers' use of cybersecurity practices is relatively recent compared to the IT industry as a whole. Techniques commonly used by large IT houses for the last 10-15 years are much newer in the OT space. People need to learn to use them and more people need to apply them to the newly developed systems. This also applies to the myriad of new smart technologies that are currently entering the industrial space that are required for running smart networks and smart cities. The deficit of cybersecurity workforce permeates all levels of the energy utility organization. There are simply not enough cybersecurity journeymen to do the work and not enough cybersecurity leaders to determine what is needed and how to proceed. The same is true for the entire energy utility ICS and information and communication technology (ICT) supply chain.

This is why UTC has partnered with an accredited university to develop a graduate certificate program in Critical Infrastructure Cybersecurity. This program aims to educate IT and OT practitioners, as well as compliance and other technology practitioners in the utility space, in the security aspects of utility systems and networks, holistically addressing both IT and OT.

Legacy Infrastructure. The technology of the grid is in itself a cybersecurity concern. Our grid is based on layers of technology that have accumulated over time. Unlike the high-tech industry that measures generations in terms of the 18-24 month intervals of Moore's Law, grid components measure lifespans in decades. Even the new technology that is now implemented in the grid has not necessarily been designed and implemented with security in mind from the beginning. Bolting on security is proven to be less effective and more expensive than building it in, but the former practice still persists due to perceived higher costs and deficit of knowledgeable workforce. Currently US energy utilities have a variety of legacy equipment that will take years and billions of dollars to replace. This infrastructure was not designed to be secure because security was not a concern when that infrastructure was implemented. Utilities have been utilizing a variety of technologies, methods, and techniques to help manage or mitigate some legacy infrastructure's vulnerabilities. However, this is an ongoing concern. Acquiring and implementing such technologies, modifying network architectures, or replacing legacy infrastructure takes time and resources.

Lack of legal framework for information sharing. The Energy sector suffers from inconsistent threat information throughout the sector. This results in a somewhat fractured response to threats when they arise. Numerous organizations such as DHS ICS CERT and the Energy Sector Information Sharing and Analysis Center (ES-ISAC) are working to improve the quality of threat sharing including how actionable and timely it is. Machine-to-machine methods are offered by DHS and now the ES-ISAC through the Cyber Risk Information Sharing (CRISP) program. But we still need a legal framework for information

sharing that would remove the barriers that remain. UTC is a member of Protecting America's Cyber Networks (PACN) Coalition. We are a strong supporter of the two information sharing bills passed by the House of Representatives in 2015 and are advocating for the passage of Cybersecurity Information Sharing Act (CISA) by the Senate before the end of the year.

Evolving practices for assuring security in supplier products and services. Building robust systems that can be resilient in the face of cybersecurity threats requires considering security from inception. Utilities rely on vendors for system design, development, implementation, and maintenance. To address this challenge, it is critical to discuss the acquirer's security needs and requirements with suppliers, and to articulate those requirements during the procurement process in a productive way. It is also critical to monitor how these requirements are adhered to and to make appropriate modifications throughout the lifecycle of the solution. This is still a challenge in many industry sectors, including the Energy sector. Standards and best practices published over the last 2-3 years provide requirements, methods, and techniques that help address this challenge. This includes NIST Cybersecurity Framework which is broadly used in the Energy space. A number of UTC member organizations established initiatives aiming to address this challenge. This is why UTC recently published a white paper providing a standards-based roadmap for implementing basic cyber supply chain risk management practices. We also have offered numerous workshops and seminars on this topic to our members and to the industry at large. Recently this challenge has been acknowledged by the industry regulator, the Federal Energy Regulatory Commission (FERC). On July 16 FERC requested comments on a NERC proposal to develop a new standard addressing supply chain management.

Conclusion: Cybersecurity is a complex challenge that cannot be solved overnight or permanently. It does not lend itself to a cook book of solutions, nor can we envision every possible scenario to mitigate.

We are dealing with an asymmetric threat. However, there are many actions the industry can take to reduce the cyber-related vulnerabilities of the grid. These actions include:

- Increasing supply of cybersecurity workforce that understands both IT and OT contexts
- Providing incentives to utilities to modify or phase out their legacy infrastructures
- Enacting information sharing legislation that removes current barriers
- Supporting industry-based standardization and NIST Framework implementation to facilitate integration of security considerations into current and future technologies.

Chairman LOUDERMILK. Thank you, Ms. Bartol.

I now recognize Dr. Baker for five minutes to present his testimony.

TESTIMONY OF DR. DANIEL BAKER,
DISTINGUISHED PROFESSOR OF
PLANETARY & SPACE PHYSICS;
MOOG-BRE ENDOWED CHAIR OF SPACE SCIENCES;
DIRECTOR, LABORATORY FOR ATMOSPHERIC
AND SPACE PHYSICS,
UNIVERSITY OF COLORADO BOULDER

Dr. BAKER. Thank you, Mr. Chairman.

Extreme space weather events pose a threat to all forms of modern high technology, particularly the backbone provided by the electric power grid. The occurrence of severe space weather impacting our nation's infrastructure is not a question of "if" but "when." My group studied a powerful solar storm that occurred just three years ago on the 23rd of July 2012. This solar eruption produced a coronal mass ejection that moved from the sun's to the distance of Earth orbit in only about 15 hours. This is among the very fastest-moving solar blasts ever witnessed in the space age. It was a ferocious disturbance that fortunately was directed somewhat away from Earth. We realized that a direct hit by such an extreme coronal mass ejection would cause widespread power blackouts, disabling everything that uses electricity.

According to a 2009 study from the U.S. National Academies, the total economic impact from an event of this sort could exceed $2 trillion or 20 times greater than the cost of Hurricane Katrina. Multi-ton power grid transformers disabled by such a storm could take years to repair or replace.

The current capability of our technological society to predict space weather is primitive. Through programs supported by the National Science Foundation, NASA, NOAA, we observe the sun, and we can see the general properties of the expansion of the solar atmosphere and powerful solar storms heading in our general direction. However, the measurements at the first Lagrangian point provide only about 4five minutes of warning at best as to what will impact Earth. This is insufficient time for implementing most mitigation strategies.

I spent two sobering days on the 20th and 21st of July at the 6th Electric Infrastructure Security Summit here on Capitol Hill. Representatives from over 20 world nations attended the EIS Summit. CEOs from key electric power utilities and leaders from the U.S. military and several federal agencies spent time grappling with the immense challenges that would result if nuclear EMP or geomagnetic disturbances were to take down the North American power grid. In the EIS world, such events are termed "Black Sky" days. The 100-plus EIS delegates acknowledged that the collapse of the power system would be devastating, and that industry, government, and academia must all work together to the greatest degree possible to minimize the impact when such a Black Sky day occurs.

In space weather, as in many things, forewarned is forearmed. Many studies have shown that improved prediction of space weath-

er would have important economic impacts on our society in the same way that improved terrestrial weather forecasts have greatly improved our economic wellbeing and the quality of daily lives.

Is our problem of improving space weather forecasting hopeless? Absolutely not. But it will require a substantially increased and dedicated government research program. Government-funded programs must be chosen to advance our civilization, our strategic importance in the world. In fact, efforts that would result in sufficient space weather prediction capability would be among our highest national—should be among our highest national priorities. Unfortunately, today's federal investments and policies are not aligned with this set of space weather needs.

The U.S. National Academies published a Decadal Survey in Solar and Space Physics in 2012. I was privileged to chair that activity. The Decadal Survey established the priorities for research relevant for space weather and basic research for NASA and NSF in the years 2013 to 2022. However, to date, NASA has not requested, nor has Congress funded, any of the significant initiatives recommended by the Decadal Survey.

The Heliophysics Division of NASA, which has the main responsibility for the research required to improve space weather predictions, is NASA's smallest science division. NSF space weather activities are only a small part of the geosciences division with many high priorities for other research areas. NOAA has the responsibility for making the actual space weather forecasts through the Boulder space-based—Space Weather Prediction Center, but these forecasts can only be based upon larger research efforts supported by the NSF and NASA.

A very substantial program was envisioned in the Decadal Survey that would build on the—a true operational 24/7 national space weather program. This would be a large investment but is essential for our nation's future. A key activity now underway is—by the federal agencies to address the Federal Space Weather Framework, as identified by the acronym SWORM with funding appropriately above the Decadal minimum level, the Decadal plan and the SWORM implementation plan could yield the required predictions in sufficient time.

The existential threat to our society represented by severe space weather events, especially to the national power grid, demand a similar national commitment even in these times of fiscal constraint. The nation should issue a challenge to the space research community to provide the predictive capability for space weather sufficient to make our economy more resilient and to reduce to an acceptable level our national vulnerabilities. The nation should recognize that this is a pressing challenge and that substantial resources will be required. In return, the space research community must give its common pledge that it will deliver what the nation requires. I would respectfully suggest that the time for budgetary and policy action is now.

Thank you very much.

[The prepared statement of Dr. Baker follows:]

House Science, Space, and Technology Committee

Subcommittee on Oversight and Subcommittee on Energy Hearing

Examining Vulnerabilities of America's Power Supply

2318 Rayburn House Office Building Washington, D.C. 20515 | September 10, 2015

Extreme Space Weather and the Electric Power Grid

Daniel N. Baker, Ph.D.

Extreme space weather events pose a threat to all forms of modern high technology, and particularly the backbone provided by the electric power grid. Such storms begin with an explosion--a "solar flare"—in the magnetic canopy of a localized magnetic active region on the Sun. X-rays and extreme ultraviolet radiation from the flare reach Earth at light speed, ionizing the upper layers of our atmosphere. Side effects of this solar electromagnetic pulse could include radio blackouts and global positioning satellite (GPS) navigation errors. Minutes to hours later, the solar energetic particles typically arrive. Moving only slightly slower than light itself, electrons and protons accelerated by the solar storm could charge satellites and damage their electronics. Then would arrive the coronal mass ejections (CMEs), which are billion-ton clouds of magnetized plasma that may take less than a day to blast across the Sun-Earth divide, and stand to cause the most damage to our terrestrial and space-based infrastructure, including the electric power grid.

The occurrence of severe space weather impacting our nation's infrastructure is not a question of "if" but "when." I, and my team, have studied a powerful solar event that occurred almost precisely 3 years ago on 23 July 2012. This solar eruption produced a CME that moved from the Sun's surface to the distance of Earth's orbit in only about 15 hours. This is among the very fastest moving solar blasts ever witnessed in the modern space age. It was a ferocious disturbance that—fortunately—was directed somewhat away from Earth. Space scientists realize that a direct hit by an extreme CME such as the one that narrowly missed Earth in July 2012 could cause widespread power blackouts, disabling everything that uses electricity. Most people would not even have water because urban water supplies largely rely on electric pumps as do gasoline pumps, communication systems, and myriad other modern human technologies. Damage from such an extreme event would run into the trillions of dollars.

Before July 2012, when researchers talked about extreme solar storms their touchstone was the iconic Carrington Event of Sept. 1859, named after English astronomer Richard Carrington who actually saw the instigating solar flare with his

own eyes. In the days that followed his observation, a series of powerful CMEs hit Earth head-on with a potency not felt before or since. Intense geomagnetic storms ignited auroral displays as far south as Cuba and caused global telegraph lines to spark, setting fire to some telegraph offices and thus disabling the 'Victorian Internet." A similar storm today would have catastrophic effects. According to a study from the U. S. National Academies (chaired by myself and published in 2009), the total economic impact could exceed $2 trillion or 20 times greater than the costs of a Hurricane Katrina. Multi-ton power grid transformers disabled by such a storm could take years to repair or replace.

The severe space weather associated with extreme solar storms would affect humans on vast spatial scales. Notably, such storms have the real possibility of knocking out dozens to perhaps scores of spacecraft on which society depends. Loss of communication satellites, weather observing spacecraft, and the GPS network of navigation and timing platforms could have severe and rapidly propagating effects throughout society. Impacts on the power grid would quickly spread to be of continental scale size. Under the worst of scenarios, policy makers, emergency preparedness workers, and health practitioners could be left powerless and cut off from much of the modern societal infrastructure for extended periods of time. The risk of widespread space weather-related outages, which could result in society being without food, water, fuel, and information for days, weeks, or months, renders this a hazard of paramount concern.

The current capability of our technological society to predict space weather is primitive. Through research and operations programs supported by the National Science Foundation (NSF), NASA, and the National Oceanic and Atmospheric Administration (NOAA), we observe the Sun, and we can see the general properties of the expansion of the solar atmosphere, the solar wind, and powerful bursts from solar storms heading in our general direction. But the initial direct measurement we currently have of the solar wind or CMEs is at the first Lagrangian point (L1) where spacecraft can hover between Earth and the Sun. Measurements at L1 provide only about 45 minutes of warning (at best) as to what will impact Earth. This is insufficient time for implementing most mitigation strategies.

Compounding the space weather challenges to our society are the complex responses of the magnetosphere and ionosphere, the regions of Earth's atmosphere most vulnerable to solar inputs and disturbances. These responses are extremely difficult to predict in detail. With regard to major and potentially disastrous space weather events, our situation today is similar to the forecasting of terrestrial hurricanes prior to the era of satellite observations. In those earlier days one might know there was a hurricane at sea, but where and in what strength it would make landfall was determined only when the hurricane struck. One need only reflect back on the devastating hurricane in Galveston, Texas, in 1900 to realize the societal consequences of such blindness to natural hazards.

In July, I spent two sobering days at the 6th Electric Infrastructure Security (EIS) Summit here on Capitol Hill. Representatives from over 20 nations around the world attended the EIS Summit. CEOs from key electric power utilities and leaders from the U.S military and several federal agencies spent two days grappling with the immense challenges that would result if nuclear weapon-induced electromagnetic pulse (EMP) or geomagnetic disturbance (GMD) were to take down the North American power grid. In the EIS world, such events are termed "Black Sky" days. The hundred-plus EIS delegates all acknowledged that the collapse of the power system would be devastating and that industry, government, and academia must all work together to the greatest degree possible to minimize the impact when such a Black Sky Day occurs.

Thus, there is great economic value in improving our capability to predict space weather. More efficient management of our bulk electrical power grids is necessary so that these grids can more effectively respond to variations in the Earth's magnetic field resulting from space weather. This in turn would result in more effective utilization of our communication networks and GPS tracking systems, as these systems are strongly influenced by variations in the ionosphere. Under the most extreme conditions, protection would be possible from disastrous bursts from the Sun that can disable our orbiting satellites or completely paralyze the electric power system. In space weather, as in many things, forewarned is forearmed. Many studies have shown that improved predictions of space weather would have important economic impacts on our society in the same way that improved terrestrial weather forecasts have greatly improved our economic wellbeing and the quality of our daily lives.

Is our problem of improving space weather forecasting hopeless? Absolutely not! But it will require a substantially increased and dedicated government research program. The prediction of space weather, as with the prediction of terrestrial weather, must be based upon comprehensive numerical models that assimilate real-time observations. Then, based upon observations, these models can predict the space weather that will affect the Earth. However, unlike terrestrial weather models, observations of the space environment are by their very nature extremely sparse.

Quite importantly, there also are basic physical processes at work in space that are unknown or only poorly known to us. Knowledge of this underlying physics is essential for translating sparse observations into actionable predictions. The technology needed to advance the research is available, as is a dedicated community of researchers at our nation's research universities and federal laboratories. There is absolutely no reason why, with a focused effort, that prediction of space weather cannot be brought to a level that delivers economic value and protects our technological civilization.

It is crucial that government funded research programs be chosen to advance our civilization, our way of life, and our strategic importance in the world. Such research should protect our citizens and our economy. In fact, research that would result in a sufficient space weather prediction capability should be among our highest national priorities.

Unfortunately, today's federal investment and policies are not aligned with this set of space weather needs. In 2012, the National Research Council of the National Academies published a Decadal Survey in Solar and Space Physics, as it has similarly done for other space science disciplines. I was privileged to chair that activity for the U.S. National Academies. The Decadal Survey established the priorities for research relevant for space weather, among other activities, for NASA and the NSF in the years 2013-2022. The Steering Committee for the Decadal Survey was told to plan for at most a modestly increasing budget during this period, and that is what the committee did. However, to date, NASA has not requested, nor has Congress funded, any of the significant initiatives recommended by the Decadal Survey.

The Heliophysics Division of NASA, which has the main responsibility for the research required to improve space weather predictions, is NASA's smallest science division. The NSF also provides essential support for the research community conducting space weather research and NSF conducts important ground-based observations as well. This prominently includes our colleagues from the National Solar Observatory (NSO) who are now moving in full force to their new facilities on the University of Colorado campus in Boulder. Yet, these NSF activities are only a small part of the Geosciences division with high priorities for other areas of research. NOAA has the responsibility for making the actual space weather forecasts through the Boulder, Colorado based Space Weather Prediction Center, but these forecasts can only be based upon the models and observations provided by the much larger research efforts supported by NSF and NASA.

Even if the basic Decadal Survey initiatives were funded they would not be sufficient to perform fully the research required to advance our capabilities to predict space weather on a schedule that serves the needs of the nation. A much more substantial program was envisioned in the Decadal plan that would build a true operational 24/7 national space weather program. This would be costly, but is essential for our Nation's future. A key activity now is underway by federal agencies to address "The Federal Space Weather Framework". This work is identified as the Space Weather Operations, Research, and Mitigation Task Force—known by the acronym SWORM. The Decadal Survey initiatives recommended strongly such a framework in which the required research and actions can be conducted. With funding appropriately above the requested minimum level, the Decadal plan and the SWORM implementation plan could yield the required predictions in sufficient time.

It is worthwhile to recall earlier challenges that the nation has given to its space program. The landing of humans on the moon, for example, was recognized as being of national importance, difficult and expensive to achieve, and from President Kennedy's speech in 1961, "every scientist, every engineer, every technician and civil servant must give his personal pledge that this nation will move forward" in this exciting adventure. The existential threat to our society represented by severe space weather events—especially to the national power grid—demand a similar national commitment even in these times of fiscal constraint.

Our economy and our way of life are influenced by, and in many ways are vulnerable to, space weather. The nation should issue a challenge to the space research community to provide the predictive capability for space weather sufficient to make our economy more resilient and to reduce to an acceptable level our societal vulnerabilities. The nation should recognize that this is a pressing challenge, and that substantial resources will be required. In return the space research community must give its common pledge that it will deliver what the nation requires. I would respectfully suggest that the time for budgetary and policy action is now.

To summarize key points:

- A solar "superstorm" is a real and present danger to our society;
- The occurrence of such a storm is not a question of "if" but "when";
- We know how to better safeguard the electric grid from severe space weather damage;
- We should take the policy steps and the physical steps to protect the electric grid;
- We should fund immediately the program plans laid out in the NRC Decadal Survey to begin to assure that adequate alerts and warnings are provided for severe space weather events.

Chairman LOUDERMILK. Thank you, Dr. Baker.

I now recognize Dr. Morgan for five minutes to present his testimony.

TESTIMONY OF DR. M. GRANGER MORGAN, HAMERSCHLAG UNIVERSITY PROFESSOR, DEPARTMENTS OF ENGINEERING AND PUBLIC POLICY AND OF ELECTRICAL AND COMPUTER ENGINEERING, CARNEGIE MELLON UNIVERSITY

Dr. MORGAN. Good morning. And thanks very much to Chairman Smith, Loudermilk, and Weber, and Ranking Members Johnson, Beyer, and Grayson for the opportunity to testify today.

As you heard, my name is Granger Morgan. I'm a professor at Carnegie Mellon, where I work on issues in engineering and public policy, including issues in the power system, often with the National Academy of Sciences, of which I'm a member.

Unlike food and water, none of us consume electricity directly. Rather, we consume the services that electricity makes possible, and those services have become ever more critical to the safe, effective, and productive functioning of our lives as individuals and to our society and hence also to our national security.

Today, I'll talk about three things: 1) Strategies to avoid physical disruption of the power system; 2) Strategies to speed the process of putting the system back together after physical disruption; and 3) Strategies to assume the continued provision of critical social services when grid electricity is not available.

Because the power system is spread out across the landscape, it's inherently vulnerable to both natural and intentional physical damage. In addition to space weather, natural hazards include wildfires, tornadoes, floods, earthquakes, tsunamis, hurricanes, and ice storms.

We all know about the devastation that Hurricanes Sandy and Katrina caused to the power system. Ice storms can be equally devastating. The 1998 ice storm in Quebec and Ontario is a vivid illustration of the power system's vulnerability to natural hazards. It collapsed miles of high-voltage power lines blacking out over 2–1/2 million customers in Canada and the United States, caused damages of over $2–1/2 billion, involved 28 deaths in Canada and 17 in the United States, and left some people without power in the dead of winter for many weeks.

Of course, we can't avoid hurricanes and ice storms but we can make the high-voltage power system much more resilient. Twenty-five years ago, a report by the Congressional Office of Technology Assessment noted that the power system is vulnerable to attackers using "just high-powered rifles." A terrorist organization that wanted to cause a massive disruption to the U.S. power system could order rifles and armor-piercing bullets on the internet, place sharpshooters in the back of station wagons like the 2002 Washington snipers, and from a distance put holes in carefully selected sets of critical high-voltage power transformers. The 2013 rifle attack on the 500 kV substation in Congresswoman Lofgren's district vividly illustrates the risk.

In a National Academy report I chaired on terrorism and the power system, we recommended replacing chain-link fences that surrounded many large substations with robust and opaque barriers, as well as a variety of other steps to limit access, increase security, and to harden the system. Progress has been made, but more is needed.

Our Academy report also recommended that the Department of Homeland Security and the Department of Energy develop a stockpile of emergency replacement transformers, an idea first studied years ago by EPRI. Between 2012 and 2014, DHS demonstrated this idea, but there's an urgent need to move beyond demonstration to implement a stockpile.

Earlier this month, Paul Parfomak at CRS prepared an excellent report on power transformers and I urge the Committee to give his comprehensive summary a careful reading.

The power industry is well organized to deal with damage from a range of normal disasters. However, there's a need to better address recovery from larger events. In my written testimony I've elaborated on options and on efforts by several groups to reduce vulnerabilities.

Equally important, the nation should take steps to assure that critical social services can continue to operate when the power system goes down, whatever the cause. Key strategies include: LED traffic lights with solar cell and battery backup so that traffic doesn't snarl and block emergency vehicles in key transportation corridors; more systematic and reliable use of backup generators; cell phone and other communication systems that will remain intact and continue to operate not just for hours but for days; and greater use of smart meters and microgrids to allow local islands of power to continue to support key social services.

I've run two meetings at the National Academy on power system resilience, the more recent under the auspices of the Resilient America Roundtable that I chair. Web addresses for the video of those meetings are provided in my written testimony.

Thanks very much for your attention.

[The prepared statement of Dr. Morgan follows:]

2015 September 10

Written testimony from Prof. M. Granger Morgan prepared for the 2015 September 10 hearing on "Examining the Vulnerabilities of America's Power Supply" before the Committee on Science, Space and Technology Subcommittee on Oversight and Subcommittee on Energy of the U.S. House of Representatives.

Thank you for the opportunity to provide my thoughts on this important topic.

I hold the position of Hamerschlag University Professor of Engineering at Carnegie Mellon University where I have appointments in three different academic units:

- The Department of Engineering and Public Policy
- The Department of Electrical and Computer Engineering
- The H. John Heinz III College.

At Carnegie Mellon I co-direct, with Professor Jay Apt, our Electricity Industry Center (see: www.cmu.edu/electricity). I am a member of the Advisory Board for the DoE Office of Electricity. Last month I rotated off of the council of the Electric Power Research Institute (EPRI) on which I have served three times and chaired for several years. As a member of the National Academy of Sciences I served as chair of the National Academies' study *Terrorism and the Electric Power Delivery System* (NRC, 2012). Since the publication of that report I have also organized and chaired two meetings on issues of power system resilience at the National Academies. Video recordings of both of these two-day events are available on line:

- Workshop run by the NRC Board on Energy and Environmental Systems on the Resiliency of the Electric Power Delivery System in Response to Terrorism and Natural Disasters. See: http://sites.nationalacademies.org/deps/BEES/DEPS_081081
- Expert meeting run by the NRC Resilient America Round Table on Improving Power System Resilience in the 21st Century. See: http://sites.nationalacademies.org/PGA/ResilientAmerica/PGA_146736

At the Academies I serve as co-chair of the Resilient America Round Table (See: http://sites.nationalacademies.org/PGA/RESILIENTAMERICA/). I am a Fellow of the IEEE, of the Society for Risk Analysis and of the AAAS.

Unlike food and water, none of us consume electricity directly. Rather, we consume the services that electricity makes possible. Those services have become ever more critical to the safe, effective and productive functioning of our lives as individuals, to our society, and hence also to our national security.

Most of the blackouts we experience are not the result of disruptions of the bulk power system. Rather, they result from more local events such as thunderstorms and vehicles crashing into utility poles. However, regional blackouts of the bulk power system do occur, sometimes as a result of errors made by system operators, sometimes as a result of

damage caused by natural events. The power system is inherently vulnerable because it is spread out all across the landscape.

Figure 1 (reproduced from NRC, 2012) shows that the distribution of larger outages in the U.S. bulk power system displays a "fat tail" – that is larger outages are much more common than one might expect from a simple statistical model. Because of restructuring of the electric power industry, which has resulted in using the high-voltage transmission system in ways for which it was not originally designed, today that system operates under stress, with the result that it has a reduced ability to absorb disruptions.

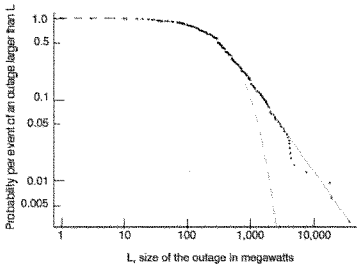


Figure 1: Relative frequency of electrical outages in the United States between 1984 and 2000. Of the 533 transmission or generation events shown, 324 involved a power loss of >1 MW (average of once every 19 days), and 46 involved a power loss of >1,000 MW (average of 3 per year). Dots indicate actual outage events. The dashed line is an exponential (Weibull) distribution fit to the failures below 800 MW loss. The solid line is a power law fit to the NERC data over 500 MW loss. SOURCE: Data compiled by NERC DAWG, plotted by Jay Apt, Carnegie Mellon University, 2006. Reproduced from NRC (2012).

In this testimony, I address three topics:

1) strategies to avoid physical disruption of the power system;
2) strategies to speed the process of putting the system back together after physical disruption; and
3 strategies to assure the continued provision of critical social services when grid electricity is not available.

1. Strategies to avoid physical disruption of the power system.

From time-to-time Mother Nature produces events that can cause significant damage to the power system. Hurricanes and associated storm surge, wildfires, tornadoes, floods, earthquakes, tsunamis, ice storms and space weather can all cause serious physical damage and widespread hardship.

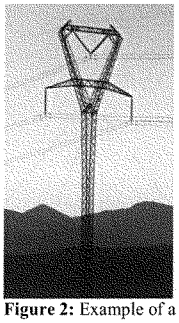


Figure 2: Example of a guyed transmission tower. Such towers can be less expensive but subject to "domino collapse." Image from Wikimedia.

However, while such events are inevitable, there are a variety of things that system designers and operators can do to make the power system more robust and thus minimize the damage they cause and the resulting adverse consequences. For brevity I offer just two examples.

It is less costly to build high-voltage transmission lines in such a way that guyed towers are partly supported by the power cables themselves (Figure 2). However, if a single tower collapses, because of a heavy load of ice, an earthquake, a hurricane, tsunami, or terrorist act, then many other towers many also fall in what is often termed a "domino collapse." By spending a bit more money and periodically inserting towers that are strong enough to be self-supporting, damage

can be limited. For example, in California regulations require that every tenth transmission tower must be stronger so that an earthquake will not trigger such a collapse.

Because the power system is spread out across the landscape it is inherently vulnerable to both natural and intentional physical damage. Large substations are especially vulnerable. They contain high-voltage transformers, circuit breakers, and other large equipment, that if damaged can be very difficult and expensive to replace. Many transformers involve custom designs. It can take many months to secure replacements. Moving these large and extremely heavy devices also poses big challenges. Recent years have witnessed efforts to increase the resilience of such systems, for example by shock mounting equipment in earthquake prone areas, taking greater precaution against intrusion by wildfire, etc.

Fortunately, the U.S. has not experienced any large coordinated terrorist attacks on the power system (see pages 9-15 of NRC 2012 for a discussion of why that might be and when and to whom the system might be an attractive target). However, deliberate attacks on power systems have been common in some parts of the world. In North America, modest attacks have been carried out by vandals, environmental absolutists, Canadian First Nation groups concerned about facilities on traditional lands, and disgruntled former employees.

If a terrorist group wanted to attack the U.S. power system, the obvious target would be a carefully selected set of high voltage power transformers. Such transformers are expensive, hard to replace, and often sit out in the open surrounded by only a chain-link fence. A 1990 OTA report noted that the bulk power system is vulnerable to "saboteurs with explosives or just high-power rifles."

Unlike the 1990 OTA report, in the National Academies' report on *Terrorism and the Electric Power Delivery System* that I chaired, we were careful *not* to be explicit about means by which an attack might be carried out. However, after the 2013 rifle attack on the substation in Metcalf, CA, such caution is probably no longer needed. A terrorist organization that wanted to cause massive disruption to the U.S. power system could order rifles and armor piercing bullets on the Internet, place sharpshooters in the back of station wagons like the 2002 Washington snipers, and from a distance put holes in a carefully selected set of critical high-voltage power transformers.

Replacing chain-link fences with opaque and more robust enclosures around substations can reduce vulnerability and increase system resilience. There are many similar strategies that can be adopted to make power systems more robust in the face of both natural and terrorist events. A description of some of these can be found in Chapter 6 of the NRC report *Terrorism and the Electric Power Delivery System* (NRC, 2012).

2. Strategies to speed the process of putting the power system back together after physical disruption.

The electricity industry has an excellent track record in restoring damaged portions of the system after natural disasters, such as hurricanes. There are standing arrangements for

cooperation between firms and line crews from other companies who are often dispatched from many hundreds of miles away to aid in recovery.

Many of the preparations and strategies that power companies make to deal with natural hazards are equally applicable to deal with the physical disruption that might be caused by terrorist events. Chapter 7 of the NRC report *Terrorism and the Electric Power Delivery System* (NRC, 2012) discusses strategies for system recovery at some length.

As noted above, if a terrorist group wanted to attack the U.S. power system, the obvious target would be a carefully selected set of high voltage power transformers. As the Department of Energy explained in its recent Quadrennial Energy Review (QER, 2015):

> LPTs [large power transformers] can weigh hundreds of tons, are expensive, and are typically custom made with procurement lead times of 1 year or more. In addition, due to their size and weight, moving LPTs presents logistical challenges requiring specialized equipment, permits, and procedures…
>
> The loss of critical LPTs can result in disruptions to electricity services over a large area. Such a loss could be due to the customized nature of the components and the associated manufacturing requirements, as well as physical attacks (such as the Metcalf incident), natural hazards (such as geomagnetic disturbances…), or extreme weather (such as floods, salt water corrosion, and sudden heat waves). In the Metcalf attack on a substation in California, "multiple individuals outside the substation reportedly shot at the [high-voltage] transformer radiators … causing them to leak cooling oil, overheat, and become inoperative."…
>
> The United States has never experienced simultaneous failures of multiple high-voltage transformers, but such an event poses both security and reliability concerns. The Edison Electric Institute, seeking to manage such vulnerabilities, has established a Spare Transformer Equipment Program, enabling utilities to stockpile and share spare transformers and parts. The inventory under this program is not large enough, however, to respond to a large, coordinated attack. Transformer design variations and the logistical challenges associated with their movement pose additional challenges to maximizing the effectiveness of the program. A National Research Council study referring to this effort noted that "... The industry has made some progress toward building an inventory of spares, but these efforts could be overwhelmed by a large attack" and that "it alone is not sufficient to address the vulnerabilities that the United States faces in the event of a large physical attack."…

Paul Parfomak, a specialist in energy and infrastructure policy at the Congressional Research Service has prepared an excellent report on this topic, which the Committee staff has kindly shared with me. Rather than summarize, below I reproduce the abstract of that report (CRS, 2015) and urge the committee to give the full report a very careful reading.

> The U.S. electric power grid consists of over 200,000 miles of high-voltage transmission lines and hundreds of large transformer substations. High voltage (HV) transformer units make up less than 3% of U.S. transformers, but they carry 60%-70% of the nation's electricity. Because they serve as vital nodes, HV transformers are critical to the nation's electric grid. HV transformers are also the most vulnerable to damage from malicious acts.
>
> For more than 10 years, the electric utility industry and government agencies have engaged in activities to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These activities include coordination and information sharing, spare equipment programs, security standards, security exercises, and other measures. There has been

some level of physical security investment and an increasing refinement of voluntary security practices across the electric power sector for at least the last 15 years. However, recent grid security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have changed the way grid security is viewed and have focused congressional interest on the physical security of HV transformers. They have also prompted new grid security efforts by utilities and regulators.

On November 20, 2014, the Federal Energy Regulatory Commission (FERC) approved a new mandatory Physical Security Reliability Standard (CIP-014-1) proposed by the North American Electric Reliability Corporation (NERC). The new standards require certain transmission owners "to address physical security risks and vulnerabilities related to the reliable operation" of the power grid by performing risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks. Legislative proposals would expand federal efforts to prevent or recover from a physical attack on the U.S. grid. These include the Enhanced Grid Security Act of 2015 (S. 1241), the Critical Electric Infrastructure Protection Act (H.R. 2271), the Terrorism Prevention and Critical Infrastructure Protection Act of 2015 (H.R. 85), a House bill to establish a strategic transformer reserve program (H.R. 2244), and the Grid Modernization Act of 2015 (S. 1243).

There is widespread agreement among government agencies, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks could require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the actual risk of a multi-HV transformer attack remains an open question. As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several issues as part of its oversight of the sector: identifying critical transformers, confidentiality of critical transformer information, adequacy of HV transformer protection, quality of federal threat information, recovery from HV transformer attacks, and the overall resiliency of the grid. Maintaining an integrated perspective on prevention, recovery, and resilience may help to promote an effective balance among industry investment, regulatory requirements, and federal oversight.

Our National Academies report on *Terrorism and the Electric Power System* (NRC, 2012) recommended that the Department of Homeland Security and the Department of Energy develop a stockpile of emergency replacement transformers, an idea first studied years ago by EPRI. While still very large, these transformers would be somewhat easier to move. However they would not be as efficient as the devices they were replacing and so would provide only temporary service during the many months it would take to manufacture, move and install permanent replacements. Between 2012 and 2014, DHS demonstrated this idea (NYT, 2012). Attachment 1 describes the program. While this demonstration is clearly useful, there is an urgent need to move beyond demonstration to implementing a stockpile.

As noted above and in Parfomak's report, the Edison Electric Institute and others have worked to better coordinate the modest existing stocks of spare transformers, but those stocks are not sufficient. DOE recently released a request for information to gather input on setting up a transformer reserve, and eight private energy companies have launched "Grid Assurance," an independent organization that will stockpile transformers and other critical equipment.

A variety of technical and operational actions exist that can be taken now to reduce the vulnerability of the bulk power system. While power companies are moving to implement many of them, it is also true that the risks faced by most individual facilities are relatively small. In some cases, it is not reasonable to expect private firms to make investments that, while they may carry considerable collective social benefit, yield little immediate benefit to the firms that are involved. Congress would do well to work on identifying strategies to change those incentives.

In addition, research could produce additional and perhaps more cost-effective strategies to increase system resilience. The Office of Electricity of the U.S. Department of Energy, and the several DoE National Labs they support through their programs, are, in my view, doing very good work. They have considerably greater technical expertise than DHS to address the key issues of grid security in parallel with the issues of grid modernization, and, in my view, should be given a more leading role in that area. That office has operated with modest funding for many years and could benefit from increased support.

At the level of more basic power-systems research, the National Science Foundation (sometimes in collaboration with DOE) has funded several research center activities including PSERC (http://pserc.wisc.edu/home/index.aspx) and CURENT (http://curent.utk.edu). Such collaborative academic research makes valuable contributions to improving the resilience and security of the power system and should be encouraged.

3. Strategies to assure the continued provision of critical social services when grid electricity is not available.

For many years the power engineering community focused exclusively on the problem of assuring the continued operation of the bulk power system. While that is clearly very important, it is also important to work on developing strategies to assure the continued provision of critical social services in the event of serious power outages (Talukdar et al., 2003; IEEE, 2004; Ch8 in NRC, 2012).

Since occasional power outages are inevitable, and blackout from terrorist attack is possible, the nation should take steps to assure that critical social services can continue to operate when the power goes out. Key strategies include:

- LED traffic signals with solar cell and battery back-up so that traffic does not snarl and block emergency vehicles in key transportation corridors. Such systems are commercially available.[1]
- More systematic and reliable use of back-up generators.

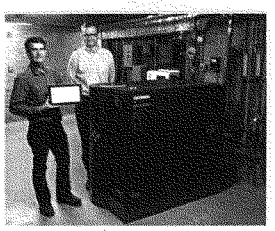


Figure 3: Example of an advanced CHP system developed by Dean Kamen of DEKA Research and Development. (Photo by G. Morgan.)

[1] Battery back-up LED traffic lights are now in use in a number of states (e.g., CA) and cities (e.g., NYC). Trickle charge LED chargers are less common but also commercially available.

On both of these see Apt and Lave (2004).

- Cell phone and other communication systems that will remain intact and continue to operate, not just for hours but for days.

The development of modern "smart grid technology" and of distribute resources, such as conventional and advanced (Figure 3) natural gas fired combined heat and power generators, provide the technology that can be used to support the creation of islands of reliable power to support critical social services when, for whatever reason, grid power becomes unavailable.

Narayanan and Morgan (2012) have elaborated strategies that show how this might be done (Figure 4). Because many utilities are already installing distribution automation, smart meters, and other needed technology, their analysis of the incremental cost to implement such a system:

> ...suggests that at least a few regions might find it reasonable to invest in a system of the type we have outlined to secure critical social services in the event of a large, long-duration outage... Clearly, no electric utility will make these investments on its own. However, if a public utility commission (PUC) concluded that installing such capabilities constituted a prudent investment, then in regulated distribution companies non-depreciated capital costs and operation costs could be recovered through the rate base with the approval of the regulator. Alternatively, local, county, or state government might choose to fund the project with tax revenue, contracting with the local distribution utility and other parties to implement the changes.

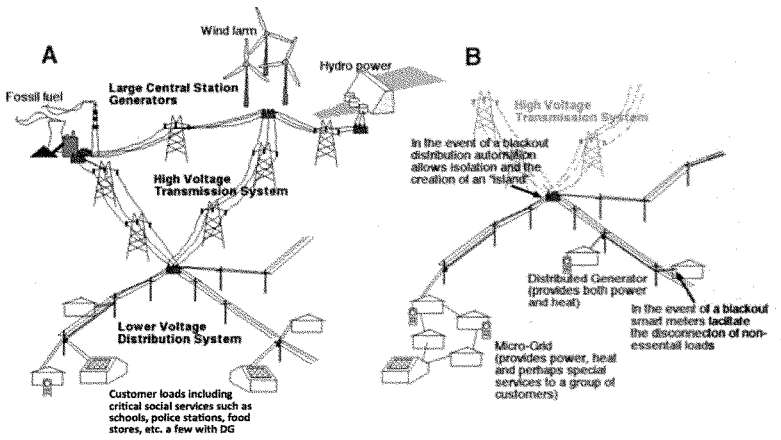


Figure 4: Left, simplified illustration of the electric power transmission and distribution system under normal operation. Right, simplified illustration of the islanded distribution system during a large, long-duration blackout in which DG units serve local critical social services. Smart meters have disconnected loads that are not critical. Feeders have been reconfigured to form an isolated "island" using distribution automation and added low-power fault-handling equipment. Figure modified from Narayanan and Morgan (2012).

Some of the issues involved in promoting the wider development and adoption of micro-grids, and systems of the sort discussed by Narayanan and Morgan (2012), fall under the

limitations imposed by state laws that grant "exclusive service territories" to legacy utilities (making it difficult to build even small privately operated micro-grid systems) and under the responsibilities of state public utility commissions. However, there are also roles the Federal government can play. In this connection, the National Academies' report on terrorism and the grid made the following recommendations:

Recommendation 8.1 The Department of Homeland Security and/or the Department of Energy should initiate and fund several model demonstration assessments each at the level of cities, counties, and states. These assessments should examine systematically the region's vulnerability to extended power outages and develop cost-effective strategies that can be adopted to reduce or, over time, eliminate such vulnerabilities. These model assessments should involve all relevant public and private participants, including public and private parties providing law enforcement, water, gas, sewerage, health care, communications, transportation, fuel supply, banking, and food supply. These assessments should include a consideration of outages of long duration (≥ several weeks) and large geographic extent (over several states) since such outages would require a response different from those needed to deal with shorter-duration events (hours to a few days).

Recommendation 8.2 Building on the results of these model assessments, DHS should develop, test, and disseminate guidelines and tools to assist cities, counties, states, and regions to conduct their own assessments and develop plans to reduce their vulnerabilities to extended power outages. DHS should also develop guidance for individuals to help them understand steps they can take to better prepare for and reduce their vulnerability in the event of extended blackouts.

Recommendation 8.3 State and local regions should use the tools provided by DHS as discussed in Recommendation 8.2 to undertake assessments of regional and local vulnerability to long-term outages, develop plans to collaboratively implement key strategies to reduce vulnerability, and assist private sector parties and individuals to identify steps they can take to reduce their vulnerabilities.

Recommendation 8.4 Congress, DHS, and the states should provide resources and incentives to cover incremental costs associated with private and public sector risk prevention and mitigation efforts to reduce the societal impact of an extended grid outage. Such incentives could include incremental funding for those aspects of systems that provide a public good but little private benefit, R&D support for new and emerging technology that will enhance the resiliency and restoration of the grid, and the development and implementation of building codes or ordinances that require alternate or backup sources of electric power for key facilities.

Recommendation 8.5 Federal and state agencies should identify legal barriers to data access, communications, and collaborative planning that could impede appropriate regional and local assessment and contingency planning for handling long-term outages. Political leaders of the jurisdictions involved should analyze the data security and privacy protection laws of their agencies with an eye to easing obstacles to collective planning and to facilitating smooth communication in a national or more localized emergency.

Recommendation 8.6 DHS should perform, or assist other federal agencies to perform, additional systematic assessment of the vulnerability of national infrastructure such as telecommunications and air traffic control in the face of extended and widespread loss of electric power, and then develop and implement strategies to reduce or eliminate vulnerabilities. Part of this work should include an assessment of the available surge capacity for large mobile generation sources. Such an assessment should include an examination of the feasibility of utilizing alternative sources of temporary power generation to meet emergency generation requirements (as identified by state, territorial, and local governments, the private

sector, and nongovernmental organizations) in the event of a large-scale power outage of long duration. Such assessment should also include an examination of equipment availability, sources of power generation (mobile truck-mounted generators, naval and commercial ships, power barges, locomotives, and so on), transportation logistics, and system interconnection. When areas of potential shortages have been identified, plans should be developed and implemented to take corrective action and develop needed resource inventories, stockpiles, and mobilization plans.

With the exception of some limited work in the area of Recommendation 8.6, I am unaware of any actions that have been taken to follow up on these recommendations.

References:

Apt, Jay and Lester Lave, "Blackouts Are Inevitable: Coping, Not Prevention, Should Be the Primary Goal, " *Washington Post*, August 10, 2004; Page A19, available on line at: http://www.washingtonpost.com/wp-dyn/articles/A52952-2004Aug9.html

CRS 2015. "Physical Security of the US Power Grid: High-voltage transformers substations, " Report 7-5700/R43604 prepared by Paul W. Parfomak, Specialist in Energy and Infrastructure Policy, 36pp.

IEEE 2004. "The Unruly Power Grid," an article by Peter Fairley in *IEEE Spectrum*, August 2004, pp. 22-27.

Narayanan, Anu and M. Granger Morgan, "Sustaining Critical Social Services During Extended Regional Power Blackouts," *Risk Analysis*, *32*, 1183–1193, 2012.

NRC 2012. *Terrorism and the Electric Power Delivery System*, National Academies Press, 2012. 146pp. Available at: http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system

NYT 2012. "A Drill to Replace Crucial Transformers…," an article in *The New York Times* by Matthew L. Wald, March 15, p. B4.

OTA 1990. *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage,* OTA-E-453, NTIS order #PB90-253287, 63pp. Available on many different web sites including: http://ota.fas.org/reports/9034.pdf

QER 2015. U.S. Department of Energy Quadrennial Energy Review: Energy transmission, storage and distribution infrastructure, 347pp.

Talukdar, Sarosh N., Jay Apt, Marija Ilic, Lester Lave and M. Granger Morgan, "Cascading Failures: Survival versus prevention," *The Electricity Journal*, 25-31, November 2003.

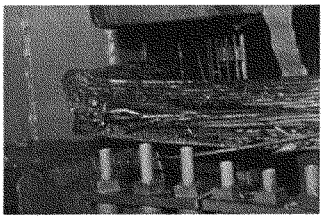
Attachment 1: One page description from the U.S. Department of Homeland Security of their recovery transformer demonstration program. The transformers were developed by ABB. See: http://www.abb.com/cawp/seitp202/9a9f00ef6e90dd00c1257a7e0042e142.aspx

DHS Science and Technology Directorate

Recovery Transformer

Extra high voltage transformers are the backbone of the electric grid but face many challenges, creating a potential vulnerability for the grid.

The United States electric grid is incredibly complex with more than 80,000 miles of extra-high voltage (EHV) transmission lines carrying electricity over long distances from generation stations to distribution networks. At critical nodes, EHV transformers either step up voltage for transportation across long distances or step down voltage prior to distribution to consumers. Ninety percent of consumed power passes through these critical pieces of equipment at some point on the transmission grid. If these transformers fail—especially in large numbers—the nation could face a major, potentially long term, blackout.

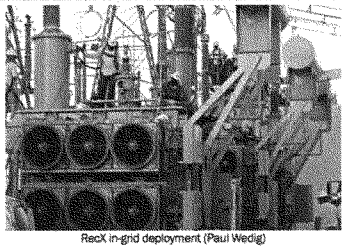


A damaged transformer at the Salem Nuclear Plant. (Metatech)

Many of the EHV transformers installed in the United States are approaching or exceeding the end of their design lifetimes (approximately 30 to 40 years), making them more vulnerable to failure. EHV transformers are huge, weighing hundreds of tons, making them difficult to transport. In some cases, specialized rail cars must be used (and there is a limited supply of these). Typically, it can take several months to transport and install a single EHV transformer due to the size and complexity of the equipment.

S&T develops new technology for the power grid, reduces time to recover by 75 percent or more

The Department of Homeland Security Science and Technology Directorate (S&T) partnered with the electric utility industry and the Office of Infrastructure Protection to initiate the Recovery Transformer (RecX) project. Through this project, S&T developed a prototype EHV transformer that drastically reduces the time to transport, install and



RecX in-grid deployment (Paul Wedig)

energize an EHV transformer to recover from outages associated with transformer failures from several months to less than one week, in the case of an emergency. S&T developed the RecX to be easier to transport (weighing approximately 60 tons versus hundreds of tons for traditional transformers) and quicker to install, reducing potential recovery time for transportation, installation, & energization of EHV transformers by more than 75 percent.

Together with industry partners, S&T successfully demonstrated the RecX prototype for one year ending in March 2013. The team transported a RecX from St. Louis to Houston, then installed, commissioned and energized it in less than a week, then monitored the RecX's performance over to validate its design and operational behavior. The RecX proved successful in an operational environment; it has the capability to reduce the impact of outages and increase the resiliency of the uniquely critical energy sector that directly effects not only functions across all other critical infrastructures but the nation's safety, prosperity, and well-being as well.

RecX Transportation (Paul Wedig)

Homeland Security
Science and Technology

To learn more about RecX, contact sandt.rsd@hq.dhs.gov.

2014-11-11

Chairman LOUDERMILK. First of all, let me thank the witnesses for their testimony. This is a very, very important issue to both of these subcommittees.

And Members are reminded that the committee rules limit questioning to five minutes, and the Chair recognizes himself for the first five minutes.

Ms. Bartol, I want to focus on you because I spent 30 years in the IT industry prior to coming to Congress, and as part of that, I actually worked with a lot of small utilities, municipal-owned utilities in automating a lot of their SCADA systems, providing fiberoptic connectivity and allowing them to be more automated in the control of substations, et cetera.

You had mentioned supply chain as part of your testimony, which is one of the areas of the concern with me. And I think you also mentioned a standardization. Is there any standard as far as configuration, what infrastructure components for a network looking at the cybersecurity side gateways, routers, security devices? Do you know, is there an industry standard or an accepted product list that we know that if a utility implements this type of product or this type of configuration, then it's approved, it would be more likely to be secure or that something that's lacking? And what's your comment as far as is what we need in standardization?

Ms. BARTOL. I don't believe there's a list as you're describing, and it really—what's needed depends on each individual utility's configuration and architecture. There are standards that provide a set of processes and so to say rules that help organizations think through how to do this well, to help them think through putting together processes and relationships with suppliers that are more robust than otherwise. And those—there's—in this document—there's an international ISO document specifically just for security and supply relationships. There's an IEC document for control systems. So there's a number of standards. They tend to look at the process more than specific configuration because it all depends on individual——

Chairman LOUDERMILK. Right. Is there a vulnerability there? And I'm coming from the equipment side because I know many of the especially small utilities will build the SCADA systems where they can control substations and different elements within that EMC or within that municipality. Then they'll connect it to the internet so their technicians can respond remotely without coming in.

We have seen that that's a huge vulnerability. When I was in the military, we had an approved products list that have been tested that says if you're going to do this—which that are going to happen, you know, given that's going to happen—if you use this product with this configuration, then you're going to more likely be secured, but I know that there's numbers of small utilities out there that can easily be—I know they are very vulnerable the nation.

Would a standardized equipment list that has been tested—because we also know that a lot of these guys go in and they will buy their equipment from eBay or wherever they can get it cheaper and I know at one time some foreign-made hardware is actually encoded in the firmware with holes, backdoors to allow people to get

in. Is that something that you feel is needed? And also, I'd like Dr. Morgan to answer—I see that you're trying to respond.

Ms. Bartol, would you comment on that? Is that something that you feel is something that we should look at?

Ms. BARTOL. A list of approved tested equipment would be tremendously helpful. My only reservation here is that, once you put a list in stone, if it's hard to get on it, then it would stifle innovation. So it can be done, it should be done, it needs to be done carefully, and there are several groups trying to work on this kind of a concept right now.

Chairman LOUDERMILK. Thank you. Dr. Morgan?

Dr. MORGAN. Well, on the cyber issue, I mean your comment about interconnecting to the internet of course was critical. You might think in terms of not so much of specific equipment but in terms of architectures or system designs because that's the big issue. I mean if I do silly things like have wireless systems in substations that somebody from the outside can hack or if I have an internet connection for my SCADA, then I'm just sort of asking for problems.

I might say one other thing on the cyber issue, and that is I know how to really cause a lot of disruption and inconvenience with cyber attacks. There haven't actually been any successful ones that I'm aware of, but I don't know how to cause large-spread physical damage.

In contrast to the sort of thing that Dr. Baker was talking about or the sort of physical events that I was describing, which could, you know, if we got caught without appropriate preparation, could result in disruptions that came—that lasted for months or maybe longer——

Chairman LOUDERMILK. Right.

Dr. MORGAN. —as opposed to, you know, days or weeks, which a cyber attack clearly could cause.

Chairman LOUDERMILK. Yeah. Thank you. One last question, Ms. Bartol. You talked about legacy systems, and I've recently read that there's a physical or online attack once every four days, and I assume that is accurate. But when we are talking about going from a legacy system, which really what we're doing now is we're putting new technology on top—layering on top of the legacy system. When you're talking about going to a legacy system, I'm assuming you're talking about a smart grid type system. And part of that is the smart meters. Is there a vulnerability of having smart meters at home and what type of information are we gathering from that?

Ms. BARTOL. To my knowledge, the information gathered from the smart meters is information about electricity usage. Nothing that qualifies as personal information is gathered. The vulnerability lies in the fact that this is smart technology, this is IP internet protocol-accessible technology and lots of access points, a lot more access points than before. So the Swiss cheese is bigger and you have more opportunity to come in. That's the vulnerability really.

Chairman LOUDERMILK. Okay. Thank you.

And I apologize to the Committee; I exceeded my time. I now recognize the gentleman from Virginia, Mr. Beyer.

Mr. BEYER. Thank you, Mr. Chairman.

And thank all of you very much for coming and talking with us.

Dr. Baker, in talking about severe space weather events and black sky days, number one, how frequent are these? Are these something that we can see once in our lifetime or once in 200 years or once every five years? Is it realistic to think that we can extend the warning time from the 45 minutes at Lagrange 1 to something much longer than that? And then as dramatic as these are, are there really mitigation efforts we can take that will make a difference?

And by the way, are they limited to solar events or are there other extreme space events that we should be concerned about?

Dr. BAKER. With respect to the latter, there could be some other extreme events, but the most probable is really a solar-driven event of the sort we're talking about. How frequently these occur is the subject of continuing investigation, but the largest of these events are probably like equivalent of a 1-in-100-year kind of flood or something like that. But we are learning more about the sun all the time and recognizing that these could be occurring more on the time scale of every decade or two, every solar cycle.

The—I—the other part of your question I guess——

Mr. BEYER. Extending the warning period——

Dr. BAKER. Extending the warning period——

Mr. BEYER. —the 4five minutes we have now.

Dr. BAKER. Yes, that's one of the key things that is under research right now. By looking at the sun, we can see that coronal mass ejections are being emitted from the sun. This can give us perhaps warning of 12 to 14 hours, something like that. If we knew what the conditions inside of that material that was expelled from the sun were, whether that was going to be extremely harmful or relatively benign, has largely to do with the interplanetary magnetic field. If we could do that, then we could give perhaps eight to ten hours of warning. That would be extremely beneficial for many who are trying to prepare themselves for the largest of these events that are coming.

Mr. BEYER. All right. Thank you, Dr. Baker.

And Ms. Bartol, you talked about the need for information-sharing legislation. Can I take it from that that information-sharing right now is prohibited by state or federal law? And are you aware of any initiatives or any proposals right now in play to make that information-sharing legal?

Ms. BARTOL. It's not prohibited but it is difficult due to various unclarities and restrictions that do exist. We—you know, the industry appreciates two bills passed by the House before summer, and we hope that the Senate will pass the information-sharing bill. It's about giving liability protections to organizations that need to share and it's mostly about the threat indicators. There's—it sort of made of data that comes in and you put in your system. That's what's being——

Mr. BEYER. I know all of us on the committee would love to pursue that in a constructive way.

And, Dr. Morgan, you talked about the ice storms. You lead with that. As long as I've been paying attention, they've been bringing down power lines throughout the Northeast and Canada. Is there

new engineering out there to make the overhead power lines less susceptible? They're burying all the power lines in new projects around Virginia, for example.

Dr. MORGAN. Yeah, they're burying lower-voltage power lines. You're not likely to want to bury 500 and 765 kV transmission lines or the DC (direct current) lines that come down from La Grande in Quebec. But you can do things like build more robust towers. I mean one of the problems in the Quebec example that I gave was that there was a lot of collapsing of towers, and actually California has passed legislation that says that every so many towers you've got to put a robust tower that can—that won't collapse. I mean it's much cheaper to build towers that are just guide and held up by the wires but then you can get a domino collapse.

So there are things like that you can do. They cost a bit more and you have to find regulatory strategies to pay for it, but the California example is one case where it's been done.

Mr. BEYER. Great. Thank you.

And Mr. Lordan, it's fascinating with the E1, E2, E3 questions. On GMD and time to respond, how best do we expand that time to respond? What—on the E1, E2, E3—are these only coming from nuclear weapons? And is there something we can do on arms control and nonproliferation to guard against that?

Mr. LORDAN. So let's do E1, E2, E3 warning first. Typically—the EMP is a nuclear device. Typically, a nuclear device or some high-powered device, the fast rise time for the E1 is the most important part and a nuclear device is the way to go for that. We assume no warning for that, and so we've—we believe operational strategies are inapplicable for EMP, a nuclear attack. Are there things that DOD can do to give us warning, to mitigate attack? Certainly, but that's outside of my purview.

And if I could go on to GMD——

Mr. BEYER. Yeah, please.

Mr. LORDAN. —for warning. Okay, so the average storm is about four days. Dr. Baker says there's fast ones. So we can observe the sun and we can tell when it's coming, and there's things that you can do in that four day period even though you know that it's kind of vague but you're not sure exactly how big and you're pretty sure it's going to hit you but you're not exactly sure. There's things you can do. You can defer maintenance on your transmission line so you have more capacity, you can back off generation so that you have a little bit of room to add voltage support. So there's things like that you can do.

And we are doing studies with NASA where they're trying to improve the accuracy of the observations of the sun in the first four days before it reaches DSCOVR satellite, yes.

Mr. BEYER. Thank you. Thank you, Mr. Chairman.

Chairman LOUDERMILK. Thank you.

The Chair now recognizes the Chairman of the Energy Subcommittee, the gentleman from Texas, Mr. Weber.

Mr. WEBER. Thank you.

Mr. Lordan, a friend of mine likes to say that nothing is faster than the speed of light, and if you don't believe that, try opening the refrigerator door before the light comes on.

An NNEMP, a nonnuclear electromagnetic pulse device, now you talked about the sun flare. I was astounded by that and did a little math. The sun is 93 million miles from Earth or 94.5 at its aphelion. So at 186,000 miles an hour, how long do you anticipate it would take an event like the solar flare to hit us?

Mr. LORDAN. The storm is fast but not as fast as the speed of light. It travels about a million miles an hour, the typical one. And there's faster ones. So 93 million miles will get you there in about 96 hours is 4 days, so that's an easy way of doing it. And then the Lagrange 1 point where Dr. Baker referred, we have a satellite there. There's an A satellite, there's a DSCOVR satellite, and then when it reaches that point, you get a lot better information, but unfortunately, the gravitational Lagrange point is only one hour away from Earth. There's only—one million miles away.

Mr. WEBER. Okay. And my study, I know that the NNEMP, nuclear electromagnetic pulse weapons, there's a lot of discussion. There's nonnuclear electromagnetic pulse weapons, and they talk about capacitor banks.

Mr. LORDAN. Um-hum.

Mr. WEBER. So I owned an air-conditioning company for 34 years and we're used to a lot of power, you know, calculations on a house being built, the size of a wire and all that kind of stuff needed, so I pay close attention to it. And of course being from Texas we have the ERCOT, Electric Reliability Council of Texas. We have our own grid, about 85 percent of the State. So we pay real close attention to that.

But from the nonnuclear weapon standpoint, the capacitor banks that could go on the end of a missile, are you familiar with those?

Mr. LORDAN. Yes, sir. And there are smaller devices that are more accessible to more parties so we're trying to figure out the risk spectrum, the folks who can supply high-altitude nuclear device and have the missile capacity to get it here. It's small—

Mr. WEBER. Okay.

Mr. LORDAN. —and the effect is high. These intentional electromagnetic interference, which is what you're referring to, these are more accessible to more folks. The thing about those devices is that they provide a local impact, and therefore, you'd need to have a coordinated attack to make a big impact. And so I think this group is talking more about high impact—

Mr. WEBER. Right, and we're going to discuss that grid. I think it was Dr. Morgan who might have said you wouldn't want to put high-voltage underground. And one way to harden the grid would be to have most of your utilities underground. But when you say small, back to the NNEMPs, define small, 4 feet, 6 feet, 2 feet.

Mr. LORDAN. I think—I'm going to say—I'm not sure exactly. I think I see things in a bread truck is what I usually see the picture of—

Mr. WEBER. Okay.

Mr. LORDAN. —but I think they can be they can be smaller than that.

Mr. WEBER. Okay. So let's go on to what I think Dr. Morgan said. You wouldn't want to put high-voltage wire underneath the ground, and a lot of utilities in a lot of States require—a lot of subdivisions require that utilities come into the neighborhood now un-

derground, whether it's—you know, of course obviously water, sewer, electricity, phone, that kind of stuff, as opposed to the aerial overhead. How high does voltage have to be before you think you wouldn't want to put it underground?

Dr. MORGAN. Well, it's a matter of cost. I mean you can put a 500 kV line underground. I mean we run 500 kV lines across things like, you know, oceans with—

Mr. WEBER. Sure.

Dr. MORGAN. —cables but it's really expensive, and so—

Mr. WEBER. So you're not talking about from an engineering perspective——

Dr. MORGAN. I'm saying—I'm not saying you can't do it—

Mr. WEBER. —just the dollar amount?

Dr. MORGAN. —I'm saying it's excluded.

Mr. WEBER. Right.

Dr. MORGAN. On the issue of EMP, he's right. I could take out a substation with a small homemade EMP device. And I could also take—

Mr. WEBER. Now, let's define small. Is that three feet, two feet?

Dr. MORGAN. Something that would fit in the back of a pickup truck.

Mr. WEBER. Okay, so a truck bomb?

Dr. MORGAN. Well, yeah, I mean if you want to think of it that way.

Mr. WEBER. Okay.

Dr. MORGAN. On the other hand, you know, I could also take it out with a rifle, and so it's not clear to me that EMP—

Mr. WEBER. Okay.

Dr. MORGAN. —is the sensible—

Mr. WEBER. Well, let's go there. You talked about—one of you talked about the snipers from 2002.

Dr. MORGAN. Yeah.

Mr. WEBER. So transformer is a set of coils, and again we dealt with transformers, high-voltage, low-voltage in the air-conditioning business with oil in it, a light oil——

Dr. MORGAN. Right, in a big steel box.

Mr. WEBER. That's right. Why don't they just make the steel thicker and less——

Dr. MORGAN. Well, that's one of the things that's being talked about. Another thing, of course, that's being talked about is—I mean, you know, you can buy armor-piercing bullets on the internet, and so it's—there is—you really have to make it quite a bit thicker. But the other thing I can do is things like simply making it hard to see from the outside.

Mr. WEBER. Sure. Well——

Dr. MORGAN. I mean at the moment—

Mr. WEBER. You betcha.

Dr. MORGAN. —it's behind a chain-link fence.

Mr. WEBER. And, Mr. Lordan, you wanted to weigh in.

Mr. LORDAN. Just real quick. I mean you can make the tank thicker but the radiator where you're trying to dispel the heat is—

Mr. WEBER. You've got to have a way to get the heat out. Yeah.

Mr. LORDAN. And the attack in 2013 that you alluded to, they shot the tank a few times but what they really shot was the radiators—

Mr. WEBER. Well, a really good sniper can take the insulators out and bring the wires off down in contact with metal structure so——

Dr. MORGAN. Yeah, but that one's easier to fix. It's if I actually fry the transmitter—

Mr. WEBER. Oh, absolutely. You know, let a squirrel get across a couple of those things, it doesn't do the squirrel a lot of good and I've seen quite a number of transformers blown. Okay. Well, thank you. I yield.

Dr. MORGAN. May I say one last thing, and that is if I'm a terrorist and I have a nuclear weapon, it seems most unlikely I'm going to use it to do an EMP. You know, unfortunately, it's true. I'm going to put it in a major metropolitan area.

Yeah.

Mr. WEBER. We had that discussion in my office this morning with my staffer in this area because I said, look, you're going to want to have death and destruction that shows up on TV. You're going to put it in a football stadium, for example.

Dr. MORGAN. Exactly. And EMP at that point is the last of our worries.

Mr. WEBER. Yeah, good point. Thank you. I yield back.

Chairman LOUDERMILK. The Chair now recognizes Mr. Grayson, who is the Ranking Member on the Energy Subcommittee.

Mr. GRAYSON. All right. I'm going to be asking Dr. Morgan a couple of questions based upon what would have been able to avoid major blackouts in the past, what kind of research and other efforts we should be undertaking now to avoid things that have already happened. Here's an interesting list. These are the 12 largest blackouts in history and what caused them. The first one I lived through, it was in New York in 1965. It was caused by the tripping of a 230 kilovolt transmission line and a domino effect that followed that; 1978, Thailand, the generators failed; 1989, Canada, a geomagnetic storm; 1999 in Brazil, a lightening struck an electricity substation near Itaipu; 2001, India, failure of a substation; 2003, in the United States and Canada there was a high-voltage power line that brushed against some overgrown trees; 2003, Italy, two internal lines overloaded; 2005, Indonesia, failure of a 500 kilovolt transmission line; 2006 in Europe, a power company switched off a power line in order to let a cruise ship pass; 2008, China, winter storms; 2009, Brazil, the Itaipu generator failed for a while; 2012, India, the largest in history, 670 million people lost electricity and three power grids collapsed because circuit breakers tripped.

So going through this list, clearly most of them were internal to the grid. Most of them were not caused by external events. There's not any instance in that list of cybersecurity issue, there's not any instance in that list of an electromagnetic pulse, not any instance of a terrorist attack, not any instance of any squirrel attack, and only one instance of space weather. So I think this can help us to focus what really would matter in this case, which is how do you avoid blackouts? Dr. Morgan?

Dr. MORGAN. Well, I certainly agree with that assessment. I would say one other thing first, which is the blackouts that most of us experience on an annual basis are not caused by the sort of large-scale blackouts that you just described but they're caused by, you know, people crashing their truck into a utility pole or a branch coming down on a line in a thunderstorm or something like that.

For the big ones that you did discuss, there are obviously several things one can do. One needs much better training and supervisory controls so that you don't take steps that put the system into a vulnerable state. And there's a lot of research going on at DOE and elsewhere and within the industry on how to provide better control and also how to better train operators. Up until recently, it's been really hard to analyze the dynamic flows in a power system in real-time. Computers are getting to the point that you can get close to doing that. The strategy in the past has been think of all the contingencies that could override arise, analyze them all and figure out what I ought to do in each of those cases, and keep people prepared to move on those things. So the answer is, yes, there's a lot that can be done and much of it is being done.

Mr. GRAYSON. Well, if you had to pick one single thing that would make blackouts like the ones that I described, the large-scale blackouts less likely, one form of research or development, what would that be?

Dr. MORGAN. Better supervisory status control, that is knowing what—how close to the edge I am and what my vulnerabilities are so if an event does—I mean all of these things are triggered by some event like, you know, an operator making a mistake or an ice storm or a flood or something, but I need to know what the status of the system is and have operators prepared to back off or do other things to take contingency—or to consider contingencies.

Up until recently we've always used the sort of N minus 1 rule, that is the rule that if one thing goes, the system ought to continue to operate okay. And we're getting sufficiently tight in terms of the capacity with which we're stressing the system that probably that's not a sufficiently conservative rule anymore and so people need to do analysis to figure out where they are at and what sorts of failures could cause what kinds of problems.

Mr. GRAYSON. So are there national federal programs or even utility company programs along the lines of what you described or is it basically ad hoc at this point?

Dr. MORGAN. No, there are—it's not basically ad hoc. There are serious research programs at a number of the national labs like PNNL and EPRI and others on the industry side are also actively engaged in this sort of work. This is an issue that the industry really does understand and is working hard to address.

I might say one other thing, and that is that the sort of replacement transformer issue that I mentioned addresses not just the kinds of destruction that could happen from terrorism or from natural events of the sort that you described but also the sort of thing that Dr. Baker talked about. I mean there are multiple reasons why one would like to have standby equipment, and transformers are just really big and hard to move and expensive, and so we ought to be doing better there.

Mr. GRAYSON. Thanks. I yield back.

Chairman LOUDERMILK. The Chair now recognizes the gentleman from Florida, Mr. Posey.

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

Thank you, witnesses, for appearing today. And, Mr. Chairman, I thank you especially for holding this hearing. This issue is so vitally important to the national security of our country and I think possibly ultimately the survival of our species.

The New York Times had a bestseller for a while. It's called "One Second After" by William Forstchen. I assume you all have read that before?

Mr. MORGAN. No.

Mr. POSEY. Well, my next question was going to be could you find any inconsistencies with the reality in the book? The book allegedly was written based on a Congressional intelligence report on the EMP threat. And it's staggering.

Mr. LORDAN. Would you want me to——

Mr. POSEY. Yes, sir.

Mr. LORDAN. Yeah. Do you want me to answer that——

Mr. POSEY. Yes.

Mr. LORDAN. —question? Okay. So, yeah, it was a novel, and so there were liberties taken and they did base this on classified information, which I don't have access to. But when we analyzed what the impact would be, and this is what we call a high-altitude electromagnetic pulse, detonated seven, ten miles above the Earth, we know that there were some relays are going to be affected but not all. We know that some computers, some communication systems are going to be impacted but not all. And it is possible and likely that there could be blackouts, but then there's a recovery and there's things you can do to recover more quickly.

Mr. POSEY. Okay. Dr. Baker mentioned the solar flare that we avoided. I think it crossed the path of our orbit about two weeks—if we had been about two weeks further ahead, it would have been very serious consequences. You talked about it being in trillions of dollars. Could you quantify that just in a couple of brief sentences, the kind of impact that would have had on everyday life?

Dr. BAKER. Well, I think—yes, it was—missed the Earth by about one week, about seven days, six or seven days. If it had occurred about a week earlier, so—it would have certainly hit the Earth. That would have been the kind of scenario that we think we would most dread. It would be a huge impact on the power grid. It would stand the chance of knocking out a number of the large, extremely high-voltage transformers on the backbone. We don't know how many, we don't know exactly the failure modes, but the $2 trillion really comes from looking at if one is without electrical power for weeks or months or extending into the timescale of a year or so, that this really then starts to be in the trillion of dollars kind of cost.

Mr. POSEY. What kind of damage do you think it would have been to our satellite systems?

Dr. BAKER. Well, that's the other component of this, which I'm glad to have the chance to respond to here is that it's not just the effects on the power grid directly; it's also the effects on satellites, the timing that we get from the global positioning systems which

feeds into the other systems, it's the communication, it's all the things that we rely on. If all of those start to collapse and they start to collapse in sequence, then we are facing I think a kind of a society that we haven't seen for decades or 100 years or sent back to very primitive kind of conditions.

Mr. POSEY. I commend to you the book "One Second After"——

Dr. BAKER. I will——

Mr. POSEY. —and——

Dr. BAKER. Yes.

Mr. POSEY. The consequence, if it takes out enough satellites, you know, you don't have a weather report, you don't have a news report, you don't have a cell phone, you don't have a laptop——

Dr. BAKER. Absolutely.

Mr. POSEY. —you don't have a car that works, you don't have—I mean you're just out of business——

Dr. BAKER. Absolutely.

Mr. POSEY. —and it is very, very, very primitive. And the threat is real, as you mentioned. It's incredibly real.

Dr. BAKER. That's right.

Mr. POSEY. Are any of you aware of any technology to more or less have a super—for lack of a better term—circuit breaker that can detect an EMP threat in advance and shut this system down whether it be on a satellite or on a generator? Are any of you aware of that?

Mr. LORDAN. I'd say the—if you get hit with an EMP, the rise time of that impact is faster than any electronics device could respond to, I assert.

Mr. POSEY. Okay.

Dr. MORGAN. A couple of things. We were sort of disparaging about the technology in some earlier Soviet fighters until we figured out that the reason they were using vacuum tubes rather than solid state was precisely to be EMP-resilient.

We have an annual doctoral qualifying exam in our department and we used a 2X Carrington event—Carrington event was the largest measured solar mass ejection—as the subject for the exam this past year, and the focus was on the resilience of emergency communication. You know, if you're using fiberoptics and you've hardened stuff at both ends, the fiberoptics are going to be resilient to this, so it really is a matter of looking carefully across the system for potential vulnerabilities. And as you heard in the case of the first testimony, if I back off the loading of the transformers, for example, so the cores are not saturated, I'm far less likely to fry them and I can do other things like capacitive coupling and some other——

Mr. POSEY. There is some——

Dr. MORGAN. —so the answer is there are strategies.

Mr. POSEY. There are people who now are working on a high-speed technology to detect it and super high-speed react to it but there just seems to be, believe it or not, no demand for it, which kind of amazes me but——

Dr. MORGAN. Well, to just say again what I said before, which is to get a widespread EMP from a nuclear device, it has to be a high-altitude burst and it—if we have an adversary that engages in a high-altitude burst, I think EMP may be the least of our prob-

lems because I presume it'll be combined with a whole lot of surface burst, which will——

Mr. POSEY. Sure.

Dr. MORGAN. I mean only a major nuclear exchange is likely to lead us to that point.

Mr. POSEY. Thank you, Mr. Chairman. I'm out of time so thank you for your graciousness.

Chairman LOUDERMILK. The Chair recognizes the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. Thanks, Mr. Chair. You know, the purpose of this is we're a very connected society obviously, and that connectedness is great for comfort, for convenience, for efficiency, but it has an obvious downside, which is a potential domino effect of it all failing at once, whether it's a nuclear device, it's cybersecurity, it's space weather, it's just some huge planetary Earth kind of weather thing.

So, Dr. Baker, I want to start with you real quick and then to you, Ms. Bartol, and then I'm going to yield the balance of my time to Mr. Takano.

Given where we are, if you had your wish list, what would be the things we could do to predict better and more quickly the space weather events you talked about to minimize the damage that might come from a big event?

Dr. BAKER. I think what we really need to have is a 24 by 7 very dedicated kind of program to look at the sun from sort of all directions and to be able to, as soon as possible, assess whether the disturbances coming from the sun are going to be harmful or relatively benign. If we could do that, we would then be much better positioned to react appropriately and to probably minimize the impacts.

The difference is that we—right now—light travels at 186,000 miles per second, 8 minutes warning that something is happening on the sun, but the fastest of these events can be at Earth in 12 or 14 hours.

Mr. PERLMUTTER. And you would suggest that we invest some more to avoid what could be——

Dr. BAKER. That's right.

Mr. PERLMUTTER. —potentially unbelievable costs

Dr. BAKER. That's right. I think the——

Mr. PERLMUTTER. Okay.

Dr. BAKER. —investment in such an observing program would be dwarfed by the cost society would face if we don't do those things.

Mr. PERLMUTTER. Okay. Ms. Bartol, what would you suggest that we do today to minimize the potential for cyber attacks that bring down the system?

Ms. BARTOL. We need to educate the society about their behavior on the internet and educate specifically in the case of energy industry the people who work in the utility, from executives to people on the ground, boots on the ground, especially the small utilities that the Chairman discussed. They have one IT guy or maybe a security guy at the same time. It's a matter of expertise; it's a matter of knowledge. There may be technologies and techniques they might not know. So education is huge here.

Mr. PERLMUTTER. I yield the balance of my time to the gentleman from California.

Mr. TAKANO. Dr. Morgan, what are microgrids and would they be useful—a useful tool that could be—that could enable communities to withstand and recover faster from high-impact events?

Dr. MORGAN. A microgrid is a small collection of local generators, perhaps combined heat and power systems, which are interconnected and then also usually connected to the grid. The big difficulty we have with—and so every presentation you go to, you'll see—at DOE, at EPRI, and others, you'll see all this proliferation of new technology on the demand side, that is, on the distribution system side. What those don't typically talk about is who's going to own all that stuff. And most U.S. States have rules that provide exclusive service territories to utilities, which means the only entity that can own one of those things is a utility, and pardon my EPRI friends; I've advised them a lot—I would not rank the distribution utilities as the most innovative firms in the country. And so I think there needs to be some strategy to allow small-scale private players to get—we've deregulated much of the supply side. We need to do a bit more on the demand side to allow small-scale players to come in underneath the distribution system to build these sorts of systems because they can provide very considerable resilience in—for critical social services in the event that the large-scale system goes down.

I'm not talking about getting off the grid. And I'm talking about tariffs that are symmetric so they recognize the cost that you impose on the big system and vice versa. When the United States—when the Congress passed law that said I must—if I build a generator, the utility must interconnect me, that was a federal law and now that's true all across the country. On the other hand, if I try to sell some of that power to Dr. Baker next door, that's in most States not legal yet, and so I don't know if this has got to be solved 50 times for different States or if it could be solved once for the nation as a whole in the same way that interconnection for single generators was solved. But I think it's an issue that would be worth your exploring.

Mr. TAKANO. Yeah, my time is up. I yield back. Thank you. I thank the gentleman from Colorado for yielding.

Chairman LOUDERMILK. Thank you. I recognize Mr. Rohrabacher——

Mr. PERLMUTTER. Mr. Chair, just a second. Did you recognize that Dr. Baker was from Colorado?

Chairman LOUDERMILK. I believe we did in the very beginning, yes.

Mr. PERLMUTTER. Okay. Thank you. Thank you. I meant to mention that. I'm sorry.

Chairman LOUDERMILK. Oh, thank you. I recognize the gentleman from California, Mr. Rohrabacher.

Mr. ROHRABACHER. Thank you very much. And, again, Mr. Chairman, I appreciate your leadership on this issue. This is an issue that is vital to our country's safety and security, and frankly, this is the first detailed hearing I've been to on it. I congratulate you for stepping up and providing that leadership.

And I'd also like to associate myself with Mr. Takano's line of questioning, which was right on target. And—but I would like to disassociate myself with Mr. Grayson's line of questioning.

Mr. GRAYSON. I appreciate that. Feel free to disassociate yourself at any time from any questions I ask. I feel good about that.

Mr. ROHRABACHER. He wanted me to do that to help him in his Senatorial campaign.

The discussion that we're looking at here is, as far as I can see, there's low probability of certain types of disruptions but with high-impact, very high-impact, but then we have other vulnerabilities that you've outlined that have lower impact. Where should our emphasis be? Should it be on this—basically a solar storm in trying to make sure that we are lined up for that and have a few days' notice and then being able to turn off our machines and in the meantime to sort of minimize the effect, or should we be looking at these various things that you're talking about, adding steel so that the terrorist squirrels don't get to us?

Dr. BAKER. Let me first say that I think this is a very active topic of research trying to understand what lower—you know, higher-frequency, lower-impact kind of events are doing to our systems. We can—it's very useful for us to think about the most extreme events and how we would inure ourselves to their effects. If we did that, we'd probably make ourselves better for the lower frequent—for the lower-impact events as well. But right now I think we don't know exactly where the sweet spot is, and investment versus, you know, the cost of doing things versus the impact that we might have.

Mr. ROHRABACHER. Well, we just were treated to some information about possibilities that utilities and that being one of the roadblocks to—and, by the way, it's just not utilities; it's also politics in the local area which determine what the policies of those utilities will be. Let me just ask this. In terms of—aren't we really talking about de-griding the country? Isn't that really the long-term concepts? No, perhaps we have reached a stage where my colleagues on the other side of the aisle have been trying to push me for a long time into basically having independent generation of electricity by solar power and things such as that, individual homes de-grided? Go right ahead, sir.

Dr. MORGAN. I think we're always going to need a grid. I think you're right that there will be much more dispersal of generation but, you know, the sun doesn't shine at night, and at the moment, storage technologies are very expensive, and there are some broader reasons as well that you really want to have a high-voltage backbone. And the wind doesn't blow all the time either. For example, in the Bonneville Power Administration some years ago there was a period of ten days when not a single wind machine put out a single bit of electricity. So you've got to have strategies to deal with that.

On your earlier question, though, what's the appropriate balance between smaller-scale stuff and the very large things? I mean I think you've got to have a bit of both and you've got to figure out how to strike the appropriate balance. You can't go off the deep end and put all your energies into worrying about the rare events that could cause nationwide or large regional blackouts and not worry

at all about local and smaller-scale stuff of the sort that hurricanes or others can do, and so you need a balance.

There's one other thing I might say on that, and that is, given that you don't know which utility is going to get into trouble, there is a problem of sort of the commons. I mean no single—especially for terrorism, no single utility can really justify in economic terms making the investments for something like a transformer stockpile. On the other hand, the nation as a whole ought to have it because there is a good chance that somewhere, sometime we are going to wish we had it.

Mr. ROHRABACHER. Mr. Chairman, let me just note that the storage of electricity is a major part of this whole concept of how we're going to deal with this. There is a lot of research going on right now. There are some people who are working on what could be breakthrough technologies in the storage of electricity, and this, too, might be an interesting discussion for the Committee. Thank you.

Chairman LOUDERMILK. Thank you. We'll keep that in consideration.

I now recognize the gentleman from Ohio, Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman.

Again, I agree this is a very, very important topic and I appreciate our panel being here with us today.

Dr. Baker, you know, in 1989 a geomagnetic disturbance brought on by a solar weather event caused millions of Canadians to lose their power for approximately nine hours. The grid in that situation collapsed within 92 seconds of the geomagnetic disturbance event. If a similar event occurred today almost 30 years later, would there be more of a warning? Would we know about it in advance?

Dr. BAKER. I think what would probably be the biggest difference between now and 30 years ago is how interconnected—Congressman Perlmutter mentioned the interconnectedness of society. I think that we are much more tightly coupled now. The impacts would propagate more—further and I think more rapidly and probably more seriously. And so——

Mr. JOHNSON. So it could be a more negative impact?

Dr. BAKER. It could be a more negative impact by far I believe, and that's one of the things that I guess I've been most struck by in my recent examination of these issues is how interconnected society is and how interconnected our technologies are. We've surrounded ourselves, as we like to say, in a cyber electric cocoon that is——

Mr. JOHNSON. Sure.

Dr. BAKER. —much more tightly coupled now than it was 30 years ago.

Mr. JOHNSON. Yeah, I share your concern. As a 30-year-plus IT professional, I have a great concern about the interconnectivity. There's great benefit to it but there's also tremendous risk associated with it. So in that vein, is there technology available to help us contain or limit the impact and should we be looking at that kind of technology?

Dr. BAKER. I think we should be going into this with our eyes much more open than they are. I think many, many times we de-

velop technologies in one sector without thinking about how they relate to other sectors and how dependent we become. Again, the timing signals that come from the global positioning system are playing into many other kind of technologies, and we at least should be aware of that. I believe we ought to be much more careful about what the interconnectedness that we build into our systems and—now and into the future.

Mr. JOHNSON. Well, yeah, I agree with you. It certainly gives us pause to stop and think. You know, we should do a risk-benefit analysis to determine whether or not the risk of a particular——

Dr. BAKER. Right.

Mr. JOHNSON. —system interconnectivity is an issue or not.

How often do other events affect everyday life like high-frequency radio communications, our space travelers' health, satellite function, and aircraft electronic systems?

Dr. BAKER. I think when you think about the broad sweep of space weather and all those dimensions that you're talking about, it probably affects us, you know, all the time, and on a daily basis there can be things. But when the sun becomes more active especially, then I think that this becomes something that can affect all those sectors and sometimes simultaneously.

So as we talked about before, there's a lot of focus on the most extreme events and the rarity of those extreme events, but as we build these more capable systems, the threshold for effective search go down and I think it becomes not a matter of every ten years or every five years, but it probably becomes almost a daily occurrence that someone somewhere is going to be suffering the effects of the environment on their technological system.

Mr. JOHNSON. Yeah. Well, I mean we saw things like the Carrington event back in the early 1900s or earlier——

Dr. BAKER. Yes.

Mr. JOHNSON. —1900s. Is there technology available today to increase the warning time of those types of events?

Dr. BAKER. Yes. As we talked about, by observing the sun that we could probably have an idea that a solar storm is coming our way. That Carrington event occurred in 1860. The internet of the Victorian age was the telegraph system. That was about the only technology that could really sense the effects of this.

Mr. JOHNSON. Has anything of the magnitude of the Carrington event occurred since then?

Dr. BAKER. I mentioned in my testimony that there was an event that occurred in 2012 that was probably two or three times stronger than the Carrington event, that it missed the Earth by about a week or so, that had that occurred, I had contended—I guess we can debate this point—we'd probably still be picking up the pieces had that event had occurred a week earlier.

Mr. JOHNSON. Is that right? Wow. How concerned are you about an extreme space weather event taking place during our lifetime? And you just said that, 2012, a couple of weeks' difference and we'd be still picking up the pieces. What do you mean by picking up the pieces? What would have been the potential implications of that?

Dr. BAKER. Well, as Dr. Morgan talked about, we don't have a lot of transformers lying around ready to reinstall into our power

grid. We don't have a lot of the kinds of backup systems and so on ready——

Mr. JOHNSON. I don't know. In Marietta, Ohio, the squirrels knockout transformers all the time and——

Dr. BAKER. Yeah, that's right. Yeah. But I believe that, again, if we think about the worst kind of case scenario and how this would propagate through not only the power grid but other aspects of technology, I mean that we would probably still be trying to recover fully from the effects of those kinds of—you know, the incidents of events.

Mr. JOHNSON. Well, it's amazing how many things like this are out there that we—that—I daresay that many people have no clue how precipitously close we are to a disaster of magnanimous proportions and we don't even know about it. It's happening almost right under our noses and we don't know it.

Dr. BAKER. I think that's what's most alarming is the vulnerability that we have and how unaware we typically are about that, yes.

Mr. JOHNSON. Okay. All right. Well, Mr. Chairman, I've exceeded my time. I yield back.

Chairman LOUDERMILK. Well, this is a very important topic, and so we also have a gentleman from California, Mr. Takano, who is not a member of the subcommittee, but we appreciate his interest in being here. He's a member of the committee, and so I recognize you for the final five minutes.

Mr. TAKANO. Thank you, Mr. Chairman. I thank my colleague from California, Mr. Rohrabacher, for commenting—saying something about the topic I brought up, the line of questioning.

Dr. Morgan, am I to conclude that—with my question regarding microgrids that—and the—your comment about the emphasis—the heretofore emphasis on distribution and not enough attention maybe on the other side of the equation on diversifying the generation——

Dr. MORGAN. The reverse?

Mr. TAKANO. Excuse me. Go ahead. Clarify what you're——

Dr. MORGAN. The reverse. We have restructured the supply side. We have not done too much to restructure the demand side, that is the distribution system and the microgrids that might be down under the distribution.

Mr. TAKANO. Thank you. Thank you for clarifying. Okay.

So my question is—and I want to follow up on what Mr. Rohrabacher suggested at the end of his comments about battery technology and—where—how could the federal government—or what would be the appropriate role in terms of emphasizing more research in this area? There's a lot of breakthrough. I just recently visited a vanadium battery company. How could this be—is this a potential game-changer if we were to make breakthroughs in various types of battery technology and how this would help alleviate our vulnerability?

Dr. MORGAN. Yeah, battery technology is important, and of course in California there's actually mandates to try to get some more batteries installed to begin to get practice and to drive things down the experience curve. The—I mean and there are a bunch of emerging new technologies. Jay Whitacre, for example, on my fac-

ulty has built a company called Aquion, which has a very nontoxic battery that's basically you can drink the electrolyte that could be—yeah, it really is. It's just a——

Mr. PERLMUTTER. I'll stick to beer.

Dr. MORGAN. Yeah. But—and the DOE is—has some major research in that space. Actually, if you allow me 30 seconds to come back to the earlier line of questioning——

Mr. TAKANO. Sure.

Dr. MORGAN. —with respect to interconnectedness, solar mass ejections is—are a high-latitude event. That is you'll notice that all of the examples were at, you know, in Canada or in South Africa, but if you have an event like that and it causes a big disruption, the power system is interconnected, so another thing you can do to limit the propagation of a problem is to be concerned about how do you avoid propagating disturbances if you take out, say, the power system across the northern tier of the United States and Canada? How do you avoid that then subsequently propagating through the rest of the Eastern interconnect or the Western interconnect? More likely, the Eastern interconnect given the geology. I'm sorry. Go ahead.

Mr. TAKANO. What can we do more to—I know the DOE supports the battery research, but could we be doing more? And is this a wise place to kind of do more—provide more support?

Dr. MORGAN. Well, I mean I mentioned Jay Whitacre. That work has largely been supported with venture monies, and so you want to make sure that you continue to provide a hospitable environment for those sorts of investments. But I think almost anybody today who has a really good battery idea and has begun to demonstrate it in the laboratory isn't going to have a lot of problems finding substantial capital to build a firm.

Mr. TAKANO. Well, great. But related to the entire topic of today's hearing, better battery storage, energy storage technologies could also be part of a strategy to address——

Dr. MORGAN. Yes. I mean it's clear there is no one-size-fits-all. As we restructure the system, we're going to need a portfolio of strategies and technologies, and support for the critical issues all across that space are important.

The Office of Electricity at the DOE has, for reasons I've never quite understood, long been rather neglected and has been modestly funded, and so that would be one place to start. And I don't know why it is, but OMB has always often sort of neglected it as well. I think that's a mistake and I think that this committee maybe ought to explore that or these committees ought to maybe—subcommittees should explore it a bit more.

Mr. TAKANO. Mr. Chairman, I would endorse that suggestion, also my colleague's suggestion, Mr. Rohrabacher's suggestion about more work on what's going on in the private sector and the public sector in battery storage and energy storage technology.

Chairman LOUDERMILK. I thank the gentleman. And I mean this needs to be an ongoing discussion that we're having.

And again, I thank the witnesses for taking time here today and for the Members being with us. We do have another briefing to get to regarding energy and the threats that we're facing.

So, as we've seen, as America's aging electric grid transitions to the smart grid, we must make sure that we are effectively protecting it, and as we've seen, we've got a long way to go. And as I've heard today, while the grid has been resilient, vulnerabilities remain. Given the importance of the electric grid in everyday life, addressing these vulnerabilities is paramount to ensuring the safety and security of our nation.

To the Members, the record will remain open for two weeks for additional comments and written questions from Members. The witnesses are excused and the hearing is adjourned. Again, thank you.

[Whereupon, at 11:22 a.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Richard Lordan

Questions for the Record

Hearing of the House Science, Space and Technology Committee
Joint Subcommittees on Oversight and Energy

Mr. Richard Lordan

"Examining Vulnerabilities of America's Power Supply"

Final Answers

1. *How long does it typically take to determine the cause of a power failure once it has occurred?*
   a. *What can be the reasoning for needing a longer amount of time to identify the source of power failure? Is that typically seen with larger outages, or are there any other factors?*
   b. *Is there technology available to quickly identify the source of power outages?*

   For transmission system interruptions, a number of factors can lengthen the time required to determine the cause of the power outage. Certain interruption causes are more difficult to identify than others. The physical area comprising the outage influences the time to determine the cause. As the failure area expands, and the number of lines and substations involved increases, the analysis becomes significantly more complicated. Typically the interruption event unfolds very quickly. Analysts must analytically reconstruct the event, by exploring the performance data for each key component to determine what occurred, when it occurred, and why.

   Intelligent electrical devices (IED's) to support faster cause analysis are becoming more prevalent. These technologies are being applied widely across the transmission system. IEDs include synchrophasors, digital fault recorders, and solid state relay reports. The synchrophasors have the ability to monitor the transmission system closely, and document system status very accurately in real time, because all synchrophasors are synchronized to satellite timing.

   For distribution system interruptions, the time to determine the cause requires dispatching a subject matter expert to the location of the outage, and depends on a multitude of variables including the availability of resources and the distance to the location of the problem. On blue sky days, the time is estimated to be 60 minutes after the utility is made aware of the outage. Note that many utilities have what is commonly referred to as a supervisory control and data acquisition (SCADA) system that can notify system operators when certain devices have operated. However, while these systems alert operators to abnormal conditions, a live subject matter expert must travel to the location to visually evaluate and determine the actual cause. Access to readily available subject matter expert impacts the analysis duration.

2. *What kind of impact can a physical assault on a substation have on the larger grid?*
   a. *Do you believe that there are adequate safe guards in place at substation facilities nation-wide?*
   b. *Do you have any suggestions for safe guards that should be implemented?*
   c. *Do you know approximately how often there are attempts of physical harm on substations?*

d. *Has there ever been a successful physical attack on a substation that has resulted in a loss of power?*

The transmission system is designed with sufficient redundancy to serve all customers despite the loss of a single substation, as illustrated by the Metcalf incident of April 16, 2013.

a. As an industry and as a society, we are continuously faced with competition for scarce resources and the need to establish investment priorities. EPRI is committed to enhancing the understanding of the costs and benefits of candidate mitigation strategies to inform utilities, regulators, and other stakeholders faced with the challenge of creating a prudent resiliency strategy.

b. Below are some hardening approaches that *may* be considered by electricity providers for increasing resiliency to electromagnetic pulse. Research is recommended to more accurately determine the effectiveness of these potential countermeasures to ensure prudent resource allocation.

   Hardening for new and existing systems generally focuses on reducing the impact of electromagnetic waves on electronic equipment. Some hardening options include:
   - New control rooms with electromagnetic (EM) shielding in the form of a Faraday Cage are being tested in some locations. To further limit EM access to control rooms, the following may be considered: shielding of cable entrances; limiting the number and location of penetrations; and, implementation of surge protection, filtering and grounding strategies. Other challenges include staff entrances/exits and ventilation ducts.
   - New relay houses which are EMP hardened are being developed and tested by some utilities. These relay houses utilize metal buildings with special consideration to ensure bonding of metal members, improved grounding, and cable entrances.
   - The use of power supply and communication cables with integrated shields, as well as consideration for the grounding strategies for these shields, are being implemented (e.g., individually-shielded twisted pair cables with an overall shield which is grounded).
   - Filtering can be applied at cable entry points to reduce high-frequency conducted energy which can impact the attached electronic activity.
   - Relocation of unprotected, sensitive control equipment to indoor shielded enclosures.
   - Relocation of control cables to a lower EM environment, such as conductive conduit, to reduce induced voltage.
   - The use of fiber optic cables rather than metallic cables for communications. Fiber optic cables have much lower susceptibility to EM impacts.
   - Utilities are engaging original equipment manufacturers (OEMs) to incorporate EM resiliency / hardening into new component design, such as relays and communications systems.
   - Neutral blockers for transformers to reduce the impact of geomagnetic disturbance (GMD) have been implemented. These blockers may aid in the reduction of induced E3 currents. The impact of neutral blockers on system operation requires further analysis.

c. EPRI does not track instances of physical attack on the power delivery system.

d. EPRI does not track outages caused by physical attack on the power delivery system.

3. *How interconnected are the various regional grids, and what does that mean when one region's grid has an outage?*

   a. *What kind of technology is available to stop there from being a domino effect of a power outage from region to region?*

   There are three asynchronous interconnections that comprise the contiguous US electric grid. An interruption in one of these regions will not impact service in another interconnection.

   Within each of these three interconnected regions, the areas are tightly connected to each other, such that an interruption in one area can impact another area (within a single Interconnection). To help limit potential cascading of outages, high voltage direct current (HVDC) lines and substations can isolate disruptions. Additionally, controlled separation methods exist which can limit a cascading event.

4. *What are the different kinds of ways an electromagnetic pulse attack can occur?*

   a. *Are there different kinds of effects from a nuclear weapon detonated on the ground versus a nuclear weapon detonated in the atmosphere? If so, please explain the differences.*

   With respect to the electric delivery system, EMP impacts the system through line of site. Therefore, a high altitude EMP (HEMP) could impact an area of approximately 3000 miles in diameter reaching to the horizon. A ground-based detonation of an EMP would impact an area with an approximate radius of 60 miles. HEMP and EMP produce significantly different impacts with respect to human health and technical areas outside the electric power industry.

5. *EPRI partnered with the Department of Homeland Security's Science and Technology Directorate (DHS S&T) to develop a prototype transformer that could be transported and assembled within a week-called Recovery Transformer (or RecX). To what extent has this project led to additional research and development by industry to further deploy smaller, more mobile transformers?*

   a. *Is there any follow up or next steps envisioned regarding this effort?*
   b. *What additional projects or research efforts, if any, is EPRI currently involved with efforts to help mitigate potential impacts to the electric grid?*

   EPRI appreciates the opportunity to work with the Department of Homeland Security (DHS) on the RecX projects and looks forward to future collaboration with them, as well as other government agencies. The design and deployment of the aforementioned RecX was considered the first important phase of a broader effort. With the efficacy of the RecX now firmly established, the next logical step would be the development of a full deployment strategy. This strategy would determine the appropriate number of spare large power transformers, the allocation of traditional transformers, and recover transformers, the appropriate number and location of storage facilities, and transportation logistics.

6. *From EPRI's perspective, what are the most significant research gaps in safeguarding America's power supply?*

   a. *Where else is there an appropriate role for federal government involvement?*

b. To what extent are federal agencies (including DHS and DOE) leveraging the Electricity Subsector Coordinating Council to help identify, prioritize, and sponsor projects to address these gaps?

With regards to research gaps in *cyber security*, the US Department of Energy released an updated Roadmap to Achieve Energy Delivery Systems Cybersecurity in 2011. As a collaboration between the federal government, utilities, the national labs, and academia, the Roadmap outlines milestones in the area of cyber security research and development. It marks a continued effort by public and private stakeholders to identify steps to build, deploy, and manage resilient energy delivery systems for the electric sector. Each milestone within the roadmap aligns to one of five research and development strategies:

1. Build a Culture of Security
2. Assess and Monitor Risk
3. Develop and Implement New Protective Measures to Reduce Risk
4. Manage Incidents
5. Sustain Security Improvements

EPRI has mapped its cybersecurity research agenda with the Roadmap and with the Department of Energy's Cybersecurity Capability Maturity Model (C2M2).

In consideration of EPRI's opinion of an appropriate role for government to support cyber security, EPRI appreciates the ongoing efforts from the Department of Energy in advancing research across the electric sector. In addition, EPRI supports the Department's role in conducting research, development and demonstrations leading to next generation tools and technologies to enhance and accelerate deployment of cyber security capabilities for the electric sector. The federal government is encouraged to continue to support such opportunities as those outlined in the Department's Cybersecurity for Energy Delivery Systems (CEDS) program, as well as other key areas including information sharing and threat analysis.

Jointly led by DHS and DOE, the mission of the Electricity Subsector Coordinating Council (ESCC) is to initiate executive level dialogue with electric sector chief executive officers and other senior executives on the roles and responsibilities of the industry in addressing high impact cyber risks and potential threats. This includes facilitating the identification and sharing of tools and technologies to improve electric sector security and resilience.

While the establishment of the research agenda within the ESCC is recent, the council has coordinated several efforts in terms of incident response for both physical and manmade emergencies, including cyber security. These efforts have improved the dialogue across industry and government. EPRI supports the ESCC's new research agenda.

With respect to physical and electromagnetic vulnerabilities, EPRI is leading an industry effort to address the key questions to prudently protect the grid. EPRI looks forward to continued collaboration with federal agencies to accelerate this important research. With respect to EMP/IEMI the following research gaps are under evaluation:

- Characterization of EMP/IEMI threats
- EMP/IEMI propagation
- EMP/IEMI vulnerability assessment
- Evaluate EMP/IEMI mitigation approaches
- Modeling of EMP/IEMI electromagnetic environment
- Transformer testing to validate magnetic and thermal models for EMP E3
- Assessment of EMP/IEMI impact on electrical subsystems interacting with Transmission and Substation delivery systems. This work will coordinate and capture analysis by others on generation (centralized and distributed), distribution systems, end-use (load), vehicles, and physical security systems.
- Strength of Insulation with respect to E1 pulse
- EMP E2: calculation of impulses stress and comparison against basic insulation strength (BIL) strength

7. *To what extent is industry receiving adequate information from applicable federal agencies regarding key risks to the electrical grid?*

   a. *What additional information, if any, would be useful to help prioritize risks and develop appropriate mitigation strategies?*

   Federal agencies have been helpful in sharing unclassified information regarding threat characterization and shielding effectiveness. However, through classified research activities, federal agencies and the National Labs have uncovered valuable insights of the evolving threat vectors for physical and electromagnetic attack. This information has helped these agencies focus their next phase of research, namely developing and assessing the effectiveness of candidate mitigation strategies. Should federal agencies be amenable to sharing select details of their higher understanding of the threat to the electric grid, the electric power industry would be able to develop mitigation responses more efficiently and effectively.

8. *In August 2013, EPRI issued a white paper that addresses the potential impacts and mitigation of high-impact, low frequency (HILF) events, such as an electromagnetic pulse (EMP) event. To what extent has EPRI performed, or partnered with industry, any modeling or simulation of the potential impact of these HILF events on wide area or local power systems? If so, what were the results and lessons learned?*

   With respect to EMP/IEMI, EPRI has characterized the threat with respect to amplitude, frequency content, range, and duration. EPRI is preparing a test plan to assess the vulnerability of key components, such as relays, to these threats.

   With respect to physical security, EPRI has characterized the principle threats, initiated ballistics testing of key components, and is in the process of collecting shielding material samples to test shielding effectiveness.

   With respect to resiliency, EPRI is leading an industry effort in partnership with a collaborative industry group. EPRI has developed a framework to guide the research to deploy mitigation countermeasures irrespective of the threat. EPRI has also developed a severe weather guide book to help utilities gather the data necessary to make prudent investment decisions to protect their systems from severe weather.

9. *What types of technologies are currently available to harden critical infrastructure assets, such as large power transformers, from electromagnetic threats, such as EMP or Geomagnetic Disturbance (GMD)?*

    a. *What are the associated benefits and tradeoffs regarding these technologies?*
    b. *Approximately, how much would these preventative measures cost?*
    c. *What challenges exist, if any, regarding evaluation and testing of such equipment (e.g. neutral blocking devices) and assessing feasibility for widespread implementation?*
    d. *To what extent could government agencies help support or facilitate these efforts? Is there an ongoing research effort in the DOE national labs?*

    EPRI is leading an industry effort to address these threats in a measured, logical approach.

    - Characterize each threat, be it EMP, GMD, or Physical Attack. The characterization includes the severity, the likelihood, the duration, warning provided, etc.
    - Through testing, assess the vulnerability of critical components to each of these threats.
    - Calculate the societal impact / cost should the above event occur and the components fail to deter.
    - Through comprehensive literature review, EPRI collects potential countermeasures, either to harden the system, or reduce the area impacted by the outage, or to speed recovery. Each potential countermeasure identified is evaluated for effectiveness and cost. In some cases, new technologies would need to be developed.

    Through this approach, interested parties will better understand the threats, and the cost and effectiveness of mitigation.

10. *To what extent is industry taking action to harden control systems and critical electronics that could be damaged by electromagnetic threats, including potential radio frequency weapons?*

    a. *What are the key barriers for taking additional protective actions?*
    b. *To what extent do estimates exist for the incremental costs that may be required to implement protective shielding and other mitigation equipment?*
    c. *If the threat from EMP is as significant as it sounds, why isn't industry doing more to protect the grid?*

    Industry members are supporting EPRI in research of EMP/IEMI. Also, in select cases, utilities may apply potential countermeasures to learn more about their effectiveness and share the results with the industry. EPRI continues to provide information and technical assistance as it is developed so that utilities and other stakeholders can determine appropriate paths forward in weighing costs and benefits of potential responses to various system threats.

11. *Large power transformers (LPTs) are essential components of the electric grid. The failure of a single LPT can cause a power disturbance and concurrent failure of multiple LPTs could magnify the impact and lead to a highly significant outage.*

    We understand that in 2012 EPRI partnered with DOE, DHS, and the private sector to build and install a recovery transformer that is lighter, smaller, and easier to transport than LPTs.

What were the results from deploying this rapid recovery transformer- referred to as RecX?

a. *What are the lessons learned from the RecX deployment, and in your view, what additional research is necessary in this area?*

The design and deployment of the Recovery Transformer (RecX) has been a success. The goal of the project was to cut the time required to deliver a replacement transformer for two months to one week. The deployment operation test started on March 12, 2013 at a transformer manufacturing plant in St. Louis where three smaller and more easily transportable units were disassembled and loaded onto lowboy flatbed trucks for the 800-mile trip to a substation near Houston. There they were off-loaded, re-assembled and fitted with cooling systems, conservers, and bushings and then connected to the grid. By March 17, the units were fully energized and functional. Two years later, the RecX transformer system remains at PH Robinson Substation, supplying power to CenterPoint customers in the Houston area.

There were numerous lessons learned:

- It is possible to transport and energize a model power transformer in less than one week. This had been considered unthinkable a few years ago.
- The RecX cannot be used as a replacement for all power transformer spares. The RecX does not have all of the functionality of a traditional spare. The RecX should be used in concert with the traditional spares, to quickly restore power as the traditional spares make their way to the site.

Questions submitted by Full Committee Chairman Lamar Smith

1. *Why are neutral ground blocking devices not used across industry?*

EPRI's research to date concludes that geomagnetically induced currents (GIC) blocking devices are not yet ready for broad deployment in transmission systems. Important issues need to be resolved before the devices can confidently be deployed in high numbers.

- Because the blocking device blocks GIC on the transformer where the blocker is deployed, GIC will increase in nearby transformers. Further study is required to determine if implementation of a blocking device on one transformer can make an adjacent transformer more vulnerable.
- When activated, the blocking device adds an impedance to the neutral to ground path for the transformer, which may cause equipment damage in certain conditions, such as a lightning storm.
- Currently available planning models do not have the function to consider GIC blocking devices. Further research is required to understand the real-time operating consequences for the safe and reliable operation of the transmission system in an environment of multiple blocking devices.
- GIC blocking devices are an emerging technology and numerous vendors are pursuing their own unique products. To date, there are no failsafe design standards for the devices. Industry specifications, adopted by manufacturers, for operation under multiple conditions would increase industry confidence in GIC blockers.

2. *What is the government estimate of the percentage of recovery from a HILF event like the solar storm of 2012 from Dr. Baker's testimony or a nuclear EMP?*

   a. *Are there any system-wide technologies that have been implemented that would change that assessment?*

   I am not aware of any estimates or studies of the impact of the event described by Dr. Baker.

3. *Without adequate preparedness and transformer stockpiles in place, how would a nuclear EMP not destroy the power supply to cool nuclear reactors for time periods longer than their back up systems currently account for?*

   The current backup power systems for nuclear plants include emergency diesel generators or combustion turbines and associated electrical equipment. In general, nuclear plants are designed such that emergency generators can supply backup power for 30 days without resupply from offsite. Thereafter, either additional diesel fuel or alternate power sources are assumed to be available maintain backup power.

   As another alternative, recent plant enhancements (particularly "FLEX," a U.S. nuclear industry collaborative approach developed after the Fukushima event in 2011) provide additional margin for extended loss-of-power events (ELAP) events. The FLEX hardware and procedural modifications provide for both onsite and offsite equipment to address extended loss of offsite power events and include the delivery of equipment from two geographically separate regional emergency response centers.

Responses by Ms. Nadya Bartol

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT
SUBCOMMITTEE ON ENERGY

Examining Vulnerabilities of America's Power Supply
Thursday, September 10, 2015

QUESTIONS FOR THE RECORD

Questions for the Record to
Ms. Nadya Bartol, Vice President of Industry Affairs and Cybersecurity Strategist,
Utilities Telecom Council

Questions submitted by Oversight Subcommittee Chairman Barry Loudermilk and Energy Subcommittee Chairman Randy Weber

1. How often is there a cyber-attack or an attempt of a cyber-attack to our national electric grid?

Unfortunately, there is no published data that definitively answers this question. Organizations in all critical infrastructure sectors are under continuous attack from a variety of threats. The Industrial Control Systems (ICS) Computer Emergency Response Team (CERT) in the Department of Homeland Security (DHS) publishes statistics about the number of incidents that ICS CERT responded to and the number of incidents that were reported to ICS CERT (https://ics-cert.us-cert.gov/Other-Reports). Generally speaking, reported incidents usually represent the tip of the iceberg as many attacks (successful and unsuccessful) go unnoticed.

   a. Has that number increased in the past five years?

ICS CERT has published relevant statistics by sector since their 2013 report. I am not aware of authoritative numbers for prior years. In 2013 the number of ICS CERT responses in the energy sector was 145, which constitutes 56% of total responses (257). In 2014, the number of incidents in the energy sector reported to ICS CERT was 79, which constitutes 32% of the total reported incidents (245). Please note that "the number of ICS CERT responses" in the 2013 report and "the number of reported incidents" in the 2014 report may be counting different things. Since the terminology is not consistent between the 2013 and 2014 reports, it is difficult to make any conclusions. Generally speaking, we understand from a number of UTC members that they see an increase in the number of attacks against their networks, although this information is not broken down by enterprise (IT) and operational (OT) networks.

b. How do we monitor potential attacks to the national electric grid?

Numerous government, academia, industry associations or consortia, and private organizations monitor cyber threats to the national grid. These include ICS CERT, the Energy Information Sharing and Analysis Center (E-ISAC), ICS ISAC, internal utility efforts, and a variety of commercial offerings that provide threat indicators and threat information.

c. Has there ever been a successful cyber-attack of the national electric grid? If so, when and what were the consequences of the hack, and who was the adversary?

I am not aware of any information pointing to a successful cyber-attack of the national electric grid. This is assuming that the definition of "successful" is penetration of company networks resulting in a real world event, such as loss of power, injury, or loss of life.

2. Considering the connectivity of regional grids, what is the probability that an effective attack in one part of the country can have a cascading effect on the whole system?

As I noted in my written testimony, today's grid is quite resilient. Since the Northeast Blackout in 2003, utilities have implemented reliability standards and smart grid technologies that should substantially reduce the risk of a similar real world cascading event. These measures will also work to limit the impact of any individual, single point of failure, cyber-related event.

a. Has this country ever seen an example of this kind of attack?

To my knowledge there has not been a successful cyber-attack resulting in a cascading effect on the whole system.

3. Do we know what kinds of adversaries are attempting to hack into our national power grid?

National power grid is not unique in its being attacked by a variety of adversaries. However, information available in the public domain is limited. According to a variety of sources including ICS CERT, well-respected industry surveys and researcher reports, attempts are made by a variety of adversaries including but not limited to nation states, criminal elements, and terrorist groups.

4. What can be done to protect the American people from an adversary attacking our infrastructure?

Protecting from cyber adversaries is a challenging proposition. We can improve our defenses, increase resiliency of our infrastructure, and become more agile in our responses. Protecting from all potential threat vectors is not possible. But we can reduce the risks to our infrastructure. Numerous sources indicate that over 50% of intrusions can be thwarted by improving cybersecurity awareness training of general employees. These are the individuals who use computerized systems to perform their daily duties, not the ones who manage those computerized systems. With respect to the individuals who manage networks and systems, create software, or otherwise have job roles related to networks and systems, a recent study by CyberLab is instructive. This study indicates that 1% of cloud users surveyed in the study are responsible for 75% of the risk generated by the overall surveyed user population (http://enterpriseinnovation.net/article/1-cloud-users-responsible-75-risk-study-1811014142). This 1% of users represents privileged users who have greater access privileges and as a result, when they expose their credentials they create greater risks. Both sets of users need to be educated to improve their understanding of the impact of their actions on the defenses of our national critical infrastructure.

Creating innovative programs for changing regular use behavior and privileged user behavior should become a priority for research and development organizations, and should include multidisciplinary teams of experts including economists, human behavior experts, cybersecurity experts, and others. Furthermore, these programs should include non-academic participants to ensure practicality of the outputs and its applicability to the real world. This is not "basic research," but rather, specific projects that would produce and propagate methods and techniques that can be applied today.

Many strategies, security controls, methods, techniques and technologies are available to improve the cyber defenses of the grid and to reduce the risks to it. Numerous documents by a variety of standards bodies, government agencies, and industry consortia provide a comprehensive list of security controls, mechanisms, and techniques that help design cybersecurity strategies which when implemented appropriately will help reduce cybersecurity risks to our national critical infrastructure. These documents include but are not limited to those published by the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Industrial Society for Automation (ISA), Department of Energy (DOE), DHS, and many others.

As noted in my written testimony, the cybersecurity workforce shortage is projected to be at 1.5 million by 2020. Greater investment in cybersecurity education and training is needed to close this workforce gap and reduce the risks to our infrastructure.

a. What role can the Department of Energy play in developing technology that can protect from cyber threats?

DOE sponsors a variety of cybersecurity research and development projects that have made and will continue to make a huge difference in the cybersecurity posture of the grid. However, very few of those projects focus on how humans use and manage the systems that support the grid. Without humans behaving the right way, the technologies will have a limited impact. To counteract this challenge the Department of Energy can:

- Fund research into the human aspects of cybersecurity
- Ensure that research produces practical results that can be applied and used immediately
- Require that the research is multidisciplinary and includes experts in human behavior, culture change, economics, and other relevant disciplines, in addition to a variety of "technical" experts including those focused on cybersecurity
- Require that research teams include individuals and organizations with experience outside of academia and think tanks with practical experience of working at or with critical infrastructure owner and operator organizations.

5. Does the fact that the "smart grid" relies on two-way communication make the grid more susceptible to cyber-attacks? If so, please explain why.

The answer here is yes and no. Smart grid implementations lead to increased visibility and situational awareness into what is happening on the grid. The grid is more resilient with these technologies than before they were implemented. At the same time, transitioning to the Smart Grid increases the number of potential entry points into the grid that are more accessible than their "dumb" predecessors. In this transition we must continue designing security, deploying software developed using secure development practices, and also have individuals on staff with the understanding of how to continuously monitor and secure these networks.

6. How much personal data will transfer out of a home once the smart grid is implemented and smart electricity meters are installed?

Smart meters do not collect, store, or transmit customer-identifying information – such as names and addresses. Just like analog meters, smart meters collect how much electricity we use. The main difference is that smart meters collect and send to the utility more of that information throughout the day with a greater frequency.

a. How vulnerable is that data to a cyber-attack?

It depends on how the network is designed, architected, and maintained for security. Utilities take protecting this data very seriously.

b. What kind of safe guards are expected to be in place to protect this data from a cyber-attack?

Appropriate safeguards for smart grids are described in the National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628 Revision 1, Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements; Volume 2 - Privacy and the Smart Grid; Volume 3 - Supportive Analyses and References. This comprehensive document describes a broad range of security controls, methods, and techniques including secure design and architecture of the network, encryption of the data, and comprehensive testing of devices before they are installed and integrated into the network. Among other things the document recommends use of both defense-in-depth and defense-in-breadth strategies, defined by the Committee for National Security Systems (CNSS) National Information Assurance (IA) Glossary, Instruction No. 4009 as:

- ***Defense-in-depth: Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.***
- ***Defense-in-breadth: A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).***

NISTIR 7628 is very well known and commonly used among energy utilities in the US and globally.

7. When the smart grid and smart meters are fully installed, will utility companies have the control to turn the power off to individuals' homes?

Utilities are able to turn off power to individuals' homes right now. No change is expected with the transition to the smart grid and smart meters.

a. How will utility companies use the information that is collected by the smart meters?

Utilities will use this data to support business functions, such as improvements in billing and customer service. Examples include consumption data for billing purposes, voltage data for reliability and volt/VAR data and control, and in case of an outage, determining extent of outage and automatically restoring data. Access to this data is and will be restricted to authorized utility personnel.

b. Will the government have any kind of role in utilizing data from the smart meters?

Not to my knowledge.

c. Would a home owner have control on what information is sent to the utility company or government?

In some states consumers have "opt-out" rights, meaning that the utility cannot put a smart communicating meter on their home without their permission.

d. Are you concerned that this introduces privacy and security concerns for American consumers?

No personal data is transmitted via a smart meter.

e. Do you know if this personal data will be encrypted? If not, do you believe that it should be – and why?

Please see answer to question 6b.

8. From what you know, are you surprised by a recent statistic that the nation's electric grid faces physical or online attacks approximately once every four days?
   a. Since that number incorporates physical attacks - do you know approximately how many cyber attacks the nation's electric grid experiences on a daily or weekly basis?

Please see answers to Question 1a and 1c.

9. How are cyber threats to the nation's electric grid being monitored?

Please see answers to Question 1b.

10. A recent CRS report noted that the Industrial Control Systems Cyber Emergency Response Team announced that several industrial control systems had been infected by a variant of a Trojan horse malware program called BlackEnergy in 2014. Can you explain to us how BlackEnergy and other malware like HALVEX or Trojan horse like Sandworm could get into a system and their potential effects?

According to ICS CERT several vendor products have been targeted by those types of malware. This means that there is a risk that this specific malware may be introduced into an electric company environment with the targeted vendor products. However, it should be noted that many electric utilities have robust testing processes that are conducted before introducing any vendor solutions into their operational environments. Conducting such tests increases the probability that the malware is discovered, eradicated and not introduced. ICS CERT also reported that they have not identified any

attempts to damage, modify, or disrupt the control systems where the malware might have ended up (i.e., in a utility environment). ICS CERT also has not confirmed that the intruders accessed additional systems beyond the specific impacted ones.

a. How vulnerable are we to these types of attacks?

It is difficult to tell definitively. Like other industries we will be attacked by a variety of actors through a variety of methods and vectors. Specifically regarding the types of attacks discussed in the ICS CERT announcements, energy companies rely on their vendors, suppliers, and integrators to provide, and ICT systems and services, to support a variety of functions, including managing the grid. The responsibility of mitigating the risk of intrusion is shared among the energy utilities and their ICT vendors, suppliers, and integrators.

b. What can we do to better protect ourselves from these types of intrusions?

Methods and techniques to reduce this particular risk include establishing assurance requirements for acquiring ICT products and services, communicating them among energy utilities and their suppliers, agreeing on the right set of requirements during contract negotiations and monitoring adherence to them throughout the lifecycle. Standards, guidelines, and industry practice documents addressing this particular challenge are available from NIST, ISO, IEC, DOE, and other sources.

UTC recently published a document that lays out basic steps for reducing this particular risk (http://www.utc.org/sites/default/files/public/UTC_Public_files/SupplyChain2015.pdf). Timely access to actionable threat information and appropriate mitigation actions will also help utility companies to better defend their systems and networks from potential compromise, and to respond quickly and appropriately should a compromise occur.

11. What would be the result of a "successful" cyber attack to the national electric grid? How would it impact our economy and society?

It truly depends. If we assume that the definition of "successful" is penetration of company networks, then the result could be anything from nothing noticeable to loss of power, injury, and even loss of life. The impact to the economy and society could be anything from negligible to far-reaching. That all depends on what happens and how quickly the critical infrastructure entities are able to respond, mitigate, restore, and recover.

12. Do you believe that we are adequately safeguarded to protect our power supply from cyber threats?

a. How would you rate the current cybersecurity protections of our nation's electric power grid?

Energy utilities are concerned about cybersecurity threats and are working hard to mitigate them by continuously deploying people, processes, and technology. We have an effective standard that is working well. The NERC CIP standard provides a mandatory baseline for security for registered entities and a gold standard for other utilities that are not regulated by NERC and FERC. We know from our members that their systems and networks attacked numerous times daily and they have to continuously adjust to the evolving threat environment. Our members also continue managing cybersecurity risks while implementing a variety of new technologies that the general public and the regulators want them to implement. We are also moving towards implementing and using risk-based security using a variety of frameworks and standards, including the NIST Cybersecurity Framework and Cybersecurity Capability Maturity Model (C2M2).

13. Does transitioning to the "smart grid" increase the vulnerabilities to the grid?

    a. Is there technology currently available that can be incorporated to the transition that will protect us?

Please see answer to question 5.

14. Just last year, the National Security Agency (NSA) reported that it had tracked intrusions into industrial control systems by entities with the technical capability to take down control systems that operate U.S. power grids, water systems, and other critical infrastructure.
    a. How alarmed should we be by this finding?

Of course we need to be concerned and vigilant. We should also realize that this is a long-term challenge with long-term solutions that involve increasing qualified workforce, changing user behavior, changing software development and system design practices, and applying substantive additional resources to the problem.

15. We have seen in other instances of cyber security breaches that cybercriminals get into a system, learn it, and then wait to perform their cyber attack. Or, the attack may just go unnoticed for months.
    a. How quickly do you think that a cyber attack on the national electric grid could be identified?
    b. What is the likelihood of a cyber attack on the grid going unnoticed for months, or longer?

It is difficult to comment on these questions in the public forum. No study that I know of has been conducted to collect this data. However, Data Breach Investigations Report by Verizon has been tracking those types of statistics for about 10 years.

With respect to general statistics, according to the 2015 Data Breach Investigations Report by Verizon (http://www.verizonenterprise.com/DBIR/), in 2014 less than 25% of defenders covered by the report discovered compromises of their systems within days of the actual compromise. In 60% of cases, attackers were able to compromise an organization within minutes. More than 75% discovered compromises within weeks or months. The Verizon Data Breach Report collects statistics globally from multiple industries. Utilities (including energy companies) represent a small percentage of the data and it is not known what percentage of the data represents the network infrastructure that supports our national grid.

16. What do we need to do as a nation to ensure that these types of intrusions do not occur, or if they occur, they don't have the ability to take down our power supply and critical infrastructure?

- Americans have had to adjust to a new reality since 9/11. We continue to change our behaviors in response to evolving physical threats in our global environment. A similar culture shift is taking place in our utilities cybersecurity environment. We are learning to exercise daily caution when it comes to cybersecurity including things such as recognizing email phishing attempts and other common attacks. To accelerate this process, we need to design and conduct awareness campaigns that show individuals why they should be careful and exactly what they should do and not do when they are conducting their daily on-line activities.

- Greater cybersecurity education and training is needed to increase the supply of cybersecurity leadership and expertise specifically with the knowledge of energy systems and networks.

- New and future technologies that support the grid should be designed, architected, and implemented with security in mind from inception, rather than after the fact.

Questions submitted by Oversight Subcommittee Ranking Member Don Beyer

1. Ms. Bartol, you made a distinction in your response to one of the questions at the hearing between the use of standards for equipment and the use of standards for processes. Would you please expand on that comment? What is the difference and where would you recommend we put our focus to ensure the highest levels of cybersecurity that can withstand the rapid changes we face in protecting our systems from cyber threats?

Standards and conformity assessments for equipment, devices, or specific configurations provide assurance that the item being assessed will act as expected in the specific configuration that it was

tested. While useful, these standards have inherent limitations. Cybersecurity environments undergo continuous changes including people, their behavior, system behavior, configurations, devices themselves, threat vectors, regulations, company policies, and many other factors. Once the item that was assessed is placed in a different environment, reconfigured, or upgraded the assurance provided may no longer be valid.

Standards and conformity assessments for processes provide assurance that an assessed set of processes, (e.g. a company, a department, a product line) performs in accordance to the practice defined in the processes. Process-based practices are designed to adjust to the changing environment through managing risks and modifying specific security controls applied to treat identified risks.

That said, both approaches have value and provide some benefits that the other type does not. We need a combination of these two approaches with the emphasis on a process-based approach first. Why process-based approach first? It is very difficult to produce a robust product without a good process. Process-based standards are more effective at raising the level of minimum practice across the board. They facilitate implementation and continuous improvement of security practices that help develop robust products. However, any standards-based approach needs to be implemented very carefully and deliberately. Standards will impede innovation if the approach they describe is too rigid and too detailed. This is more of a risk with the equipment/device standards but can also be a risk with process-based standards. If a method or technique is mandated at a certain level of detail it may hinder a better and more robust method or technique from being implemented. Such standards are more effective when they are developed by industry practitioners who are intimately familiar with current methods and techniques as well as with their limitations.

Generally speaking, the industry is moving towards holistic risk-based approaches where an organization recognizes its risks and makes security decisions and corresponding investments accordingly.

2. Would you also describe what you think are the primary barriers to cybersecurity information sharing and what recommendations you have to reduce or eliminate those barriers?

The barriers that exist today are well addressed in the two information sharing bills passed by the House of Representatives in 2015 as well as in the Senate Cybersecurity Information Sharing Act (CISA). If CISA is passed and a reconciled bill is signed into law, this challenge will be mostly solved. UTC is a member of the Protecting America's Cyber Networks (PACN) Coalition which is advocating for the passage of the Cybersecurity Information Sharing Act (CISA) by the Senate before the end of the year.

Responses by Dr. Daniel N. Baker

Answers to Questions:

Questions submitted by Oversight Subcommittee Chairman Barry Loudermilk and Energy Subcommittee Chairman Randy Weber

1. How large of an area would a geomagnetic disturbance cover?
    a. What is the largest area that you know of that has been affected from a GMD?

The kinds of geomagnetic disturbances that we most dread would be those that extend to the scale of major regions of the United States. The geomagnetic disturbance of March 1989 blacked out all of the Canadian province of Quebec. It nearly spread to affect all of the northeastern U.S. Models suggest that a major geomagnetic storm could easily affect a broad area such as New England, the Great Lakes region, and the middle Eastern seaboard.

2. How often are severe GMDs expected?

The question of how often severe GMDs will occur is an active area of space physics research. We know that the probability of severe solar storms goes up substantially every 11 years or so in concert with the 11-year sunspot cycle. However, not every cycle necessarily produces extreme coronal mass ejections that strike the Earth. Evidence from the relatively recent record is that every one to two decades the Earth will be hit by quite severe solar storms.

    a. When was the last severe GMD and what was the effect on the nation's power supply?

    In my view, the last quite severe GMD events occurred in 2003. These were the so-called "Halloween" storms of late October and early November. These storms produced dramatic effects both on the Earth's surface and in near-Earth space.

    b. Is it only a matter of time before a severe GMD occurs in our nation?

    Yes, it is not a question of "if" a severe solar storm will hit the Earth, but "when". We must be prepared.

3. How concerned are you about an extreme space weather event – like the Carrington event of 1859 – taking place during our lifetime?

I personally am quite concerned about an extreme event hitting the Earth. My concerns were increased by the experience of July 2012 when a very severe solar disturbance narrowly missed striking the Earth. This showed me (at least) that an extremely powerful disturbance can occur even during a moderately active solar cycle (such as the one we currently are in).

a. Should one occur during our lifetime, what would the extent of the impact look like here on earth?

   The scenarios portrayed for extreme solar events hitting Earth are quite disturbing. There could be nearly instantaneous disruption of radio communication on Earth due to x-ray solar flares. Very quickly thereafter, solar energetic particles could disrupt near-Earth satellite operations. Just a matter of a few hours later, the bulk power grid could be brought to its knees over a broad geographic region. Under the worst of circumstances, vast parts of the nation could be without power for months (or possibly longer). This would mean that water, fuel, food, communication, and basic services would be totally disrupted.

b. What kind of warning would we have for such an extreme space weather event?

   At the present time, we cannot say for sure how much warning of an extreme event there would be. Using science spacecraft and operational satellites, we might get a half day's warning. However, it is more likely that for the most extreme events we would be lucky to get a few hours warning – and it might be much less.

c. What can be done to mitigate the effects of an extreme space weather event?

   Mitigating the effects of extreme space weather is a very challenging matter. It depends very much on how much warning there is and on which technology sector we are talking about. The power grid – with some hours of warning – could plan brown outs and diversions of electricity around certain sectors if warnings were soon enough and accurate enough. Satellite operations could possibly avoid certain maneuvers and could even power down some subsystems under some circumstances. With enough warning, other high-tech sectors could "hunker down" until the worst of the storm had passed. However, realistically one would have to say that during extreme events there would be substantial and long-lasting consequences.

4. How much money does our country spend on the impact of "ordinary" space weather storms?

   This question is being assessed more thoroughly now than it ever has been before. Much money is spent by both military and civilian users to "harden" their systems to space weather in the first place. There is also work by economists to look at day-to-day costs of small and moderate solar and space weather disturbances. I do not have the latest results on this, but will endeavor to get the latest publications. I would expect that several billions of dollars per year get spent dealing with "ordinary" space weather.

a. What would that figure look like for an extreme space weather event?

Our study on the "Economic and Societal Impacts of Severe Space Weather" published by the U.S. National Academies in late 2008 noted that extreme space weather event costs could run to the neighborhood of $2 trillion. This general level of possible economic impact has been largely validated by other recent analyses.

b. How much money does our country spend on preventing and mitigating effects from an ordinary or potentially extreme space weather event?

As noted above, spacecraft designers and operators of ground-based technology systems are well aware of the possible effects of space weather. Thus, most designers and operators spend substantial levels of funds on making their systems more robust. I do not presently know this number with any fidelity, but I am trying to get an accurate estimate.

5. How well do you think that this country addresses the potential threats of geomagnetic disturbance to the grid from an extreme solar weather storm? What could we be doing better to adequately protect Americans?

I am personally disappointed that more attention is not paid to the threats of space weather both by policy makers and technologists. I attach a recent brief paper of mine, published in the journal Space Weather that outlines some of the important steps that can (and should) be taken.

Questions submitted by Full Committee Chairman Lamar Smith

1. Why are neutral ground blocking devices not used across industry?

I believe that more effort is being made to develop (and field) effective neutral blocking devices. I understand that perceived high costs were the reason for not deploying these devices in the past. However, my personal view is that the cost of installing such devices would be dwarfed by the cost to society of an extreme space weather event.

6. What is the government estimate of the percentage of recovery from a HILF event like the solar storm of 2012 from Dr. Baker's testimony or a nuclear EMP?

As noted in answer to Question 4 above, estimates of the cost of power system damage and sustained power outages due to extreme events run to $1-2 trillion.

a. What system-wide technologies have been implemented that would change that assessment?

I would again refer to my attached paper as to what technologies and operational approaches could help mitigate the effects of extreme events.

3. Without adequate preparedness and transformer stockpiles in place, how would a nuclear EMP not destroy the power supply to cool nuclear reactors for time periods longer than their back up systems currently account for?

I do not feel adequately qualified to address this key question. I would hope that one of my fellow panelists could better address the question than could I.

SPACE WEATHER, VOL. 10, S07002, doi:10.1029/2012SW000820, 2012

The Third Electric Infrastructure Security World Summit Meeting

Daniel N. Baker

Published: 12 July 2012

Citation: Baker, D. N. (2012), The Third Electric Infrastructure Security World Summit Meeting, *Space Weather, 10*, S07002, doi:10.1029/2012SW000820.

Almost 150 scientists, engineers, policy makers, and industry leaders from more than 20 countries met at the Electric Infrastructure Security (EIS) summit meeting in London to iron out recommendations on how to potentially protect power grid infrastructure in the event of an extreme space weather event.

Held in the Houses of Parliament on 14–15 May 2012, the EIS summit was intended to find ways to increase cooperation and collaboration among governments and within private industry regarding critical electrical capabilities in cases of extreme space weather. The summit also looks at threats of nuclear electromagnetic pulse (EMP) phenomena. This meeting led to four main recommendations on how to proceed on these broad issues:

1. Establish a severe space weather working group to identify and define the most reasonable extreme space weather event(s) that would serve as the threat analysis baseline for bulk power operators and system engineers to measure against. This group should draw upon ongoing extreme space weather activities in the U.S., in the UK, and elsewhere to define the driving or "forcing" conditions that would be handed over to power industry teams.

2. Identify the critical infrastructures and facilities that must continue to have electric power during extreme space weather events or during EMP attack scenarios. This identification would be spearheaded in the U.S. by the Federal Energy Regulatory Commission and would involve all relevant federal agencies.

3. Establish detailed modeling of the effects and interconnections within a national power grid under the influence of severe space weather (see recommendation 1) or other threats such as an EMP attack. Modeling would be undertaken by companies, system engineers, and operators with the protection of key assets (see recommendation 2) a foremost priority in the scenarios analyzed.

4. Identify techniques and engineering solutions that would keep ground-induced currents from space weather events and from EMP events isolated and away from key infrastructure (blocking solutions). This would require efforts by engineers, transformer experts, and other professionals.

Space weather effects on GPS (Global Navigation Satellite Systems) were also discussed. There is a need to examine the possible effects if a major space weather event were to knock out GPS. Such a scenario leads to myriad questions about nonlinear interconnectedness and feedbacks within a power grid system that may only increase with time. It was stressed that power system designers should undertake future design approaches with "eyes open" concerning unintended consequences of design choices.

This meeting was hosted by James Arbuthnot, a member of Parliament (MP) and the chair of the Select Committee on Defense in the UK. The summit also included a number of dignitaries from the UK government such as Philip Hammond (MP), the secretary of state for defense. The U.S. delegation was headed by Representative Trent Franks (R, Arizona) of the U.S. House Armed Services Committee.

The EIS summits, previously held in Washington, D. C. (2011), and London (2010), present a remarkable opportunity to bring together policy makers, industry representatives, and experts on the science and engineering of electromagnetic threats. The assembled group made it clear that many reports and studies from the U.S. and around the world have undeniably established the threat posed to society by severe space weather and that the time for action has arrived.

Daniel N. Baker *is professor and director of the Laboratory for Atmospheric and Space Physics, University of Colorado Boulder, Boulder, Colo. E-mail: daniel.baker@lasp.colorado.edu.*

Responses by Dr. M. Granger Morgan

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT
SUBCOMMITTEE ON ENERGY

Examining Vulnerabilities of America's Power Supply
Thursday, September 10, 2015

QUESTIONS FOR THE RECORD

Questions for the Record to
Dr. M. Granger Morgan, Hamerschlag University Professor, Departments of Engineering and Public Policy and of Electrical and Computer Engineering, Carnegie Mellon University

Questions submitted by Oversight Subcommittee Chairman Barry Loudermilk and Energy Subcommittee Chairman Randy Weber

1. What are your thoughts on the role Micro-grids might play in making the grid more resilient?
   a. Would direct-current Micro-grids help protect the grid?

There may be economic and efficiency reasons for converting some systems to DC but it is not clear to me that there are any security benefits.

   b. Is there any benefit to mitigating the impact of EMPs or solar flares through DC micro-grids?

The only way to create an electromagnetic pulse (EMP) effects across a wide enough physical area to have serious consequences for the power system is to detonate a high-altitude nuclear weapon. If a terrorist ever secures a nuclear weapon I can't believe they're going to "waste" it trying to induce an EMP. Hence I think the ongoing attention to EMP is misplaced when compared to extreme weather events (e.g., hurricanes, ice storms, earthquakes) that regularly cause big blackouts and solar mass ejections, which have the potential to cause big blackouts.

I presume that EPRI continues to study EMP because people keep asking about it. There is something of a vicious cycle here in that because EPRI studies it, people take it seriously. Yes, if we have a nuclear war, EMP could be a problem. However, in my view, if we have a nuclear war, the problems caused by EMP will pale in comparison to the deaths, physical destruction and radiological contamination even a "small" war would produce.

The situation is quite different for solar mass ejections. While the risk in any given year is low the risks to the power system when a major event occurs could be significant.

Because they would be more spatially compact, micro grids that are isolated from the bulk power system would probably not be very vulnerable. However, I do not see any obvious reason why the vulnerability of a DC micro grid would be significantly different than that posed to an AC micro grid.

Questions submitted by Full Committee Chairman Lamar Smith

1. Why are neutral ground blocking devices not used across industry?

There are at least two reasons. First, given the configuration of the earth's magnetic field, it is only power systems at high magnetic latitudes that are likely to be vulnerable to solar mass ejections, so there is no particular reason why such devices should be used across the southern part of the United States. The second reason is simple economics. These devices cost money, and can somewhat complicate operations, so they are not being used as widely as they probably should be.

What is the government estimate of the percentage of recovery from a HILF event like the solar storm of 2012 from Dr. Baker's testimony or a nuclear EMP?

a. What system-wide technologies have been implemented that would change that assessment?

There may well be government studies of these questions but, if there are, I am not aware of them.

If you have not looked at it, see the study "Impacts of Severe Space Weather on the Electric Grid" by the Jasons available on line at http://fas.org/irp/agency/dod/jason/spaceweather.pdf

2. Without adequate preparedness and transformer stockpiles in place. how would a nuclear EMP not destroy the power supply to cool nuclear reactors for time periods longer than their back up systems currently account for?

Please see my discussion above of EMPs.

The time-scale for deploying replacement transformers is likely to be a few days. While these transformers would have value for minimizing the damage caused by natural causes, such as space weather, they would also have "dual use" value in providing resilience in the event of terrorist acts and acts of war, including EMP.

There may be a number of good reasons to develop strategies to increase the amount of time that back-up systems for present generation nuclear plants can operate without outside power, but, in my view, the possibility of EMPs is not a good reason for doing that.

There are a variety of future more advanced reactor designs that are passively safe and would not require local or grid power to remain undamaged. Unfortunately the United States is not moving with sufficient vigor to conduct research and promote the development and deployment of such systems.

Questions submitted by Oversight Subcommittee Ranking Member Don Beyer

1. Dr. Morgan, you commented on the role of energy storage as part of a portfolio of strategies and technologies we need to manage risks to our electrical infrastructure. Would you please expand on your comments? What would be the value of energy storage in helping us build a more resilient system? And given the interest of the private sector in this space, where do you think federal actions or investments would be most appropriate?

   Let me first clarify a response I gave during the course of the hearing. I indicated that I thought there was a significant amount of private investment money available to support the development of advanced storage technologies and systems. This is true but at the same time once an idea has been shown to be viable there can be big difficulties moving it from the stage of laboratory demonstration and early prototype to the stage of commercial production (i.e., getting it across the so-called developmental "valley of death"). Thus, for example, the commercialization of the technologies that underlie the aqueous hybrid ion battery that I mentioned during the hearing (see: http://www.aquionenergy.com) was very considerably facilitated by some Federal stimulus funding.

   If it can be made cost-effective, storage can be a valuable component to make greater use of low-cost baseload power that can be effectively time shifted from periods of low demand to periods of peak demand. Storage can also be very valuable to smooth out the intermittency and the variability of power generated from solar PV and wind. However, it is always important to "look at the numbers." At least to date the dreams that some people have advanced of using a fleet of battery operated vehicles as a way to store energy for the power system, do not look like they will be particularly attractive to the vehicle owner. Every time one cycles a battery it reduces its useful life by at least a tinny bit. It does not look today as though power companies would be willing to pay vehicle owners enough to offset the cost of that shortening in battery life. Further, our research shows that truly large-scale storage is unlikely to be profitable in competitive wholesale markets in the U.S.

2. Of the many strategies and technologies we could pursue at the federal level to increase our country's ability to withstand and recover from an event, what areas do you think would benefit most from new or additional federal investments?

   I think there are several. First, as I mentioned, there remains a need to develop and deploy a stockpile of emergency replacement transformers. While the risk faced by any single utility or substation is probably quite small the risk across the entire system is significant. Hence, there is a need to spread the risk across our entire society, and that can best be done through some form of government program.

   Beyond this there are a variety of research activities that could result in technologies and strategies to significantly reduce the vulnerability of the power system. One example is better more advanced systems for instrumentation and control of the transmission and distribution system. As I mentioned in my written testimony, the DOE Office of Electricity is doing good work in this area and in my view would benefit from expanded and more secure ongoing funding.

Questions submitted by Rep. Zoe Lofgren

1. The Metcalf attack happened in my district. As you are no doubt aware, this was a very serious incident. Although we were lucky to avoid catastrophic damage, the potential is clear – and not only for the families in the Bay Area, but for the national economy. If Silicon Valley were to go dark, the effects would be felt throughout the country. This attack was a wake-up call as far as the physical security of the electric grid. DOE is now working on a spare transformer stockpile, and FERC has proposed updated reliability standards. If Metcalf happened today, what would be different? Could we prevent it?

   The issue of physical vulnerability has been understood in the power industry for decades. As I explained in my testimony, the Congress was first informed of this vulnerability 25 years ago in a report produced by its own Office of Technology Assessment. In the intervening quarter-century, very little has been done to increase physical protection. One can only hope that the fact that someone has now actually executed an attack at Metcalf will finally result in some action.

   The Department of Homeland Security did build and demonstrate a single replacement transformer, and as the CRS report by Paul Parfomak explains, the industry has taken some steps to try to improve record keeping and facilitate sharing of existing transformer stockpiles, the basic situation remains that we are not building the sort of stockpile that was called for by the 2012 National Academies study. Congress should instruct DOE and/or DHS to do that and should provide the needed funding.

2. What is your assessment of DOE's effort to create a spare transformer stockpile?

   While the DOE Quadrennial Energy Review Notes the importance of such a stockpile, I am unaware of any serious effort by DOE or by DHS to actually develop and build such transformers. See the recommendations on page 2-40 of the DOE's Quadrennial Energy Review that still only talks in terms of studies.

3. According to a March article in USA Today, between 2011 and 2014, electric utilities reported 362 physical and cyberattacks that caused outages or other power disturbances to the Department of Energy. Of those, 14 were cyberattacks and the rest were physical. Given these numbers, do you feel that physical security is being given the appropriate amount of attention?

   No. Because it is "sexy" there is lots of talk about cyber security with respect to the power system, and way too little attention is being given to physical security.

   Take a look at Figure 2-3 in the DOE's Quadrennial Energy Review. You will see that the number of physical attacks during a 5-year period from 2008 to 2012 that actually resulted in any effect on the power system vastly outnumbered cyber events.

   A successful cyber attack on the power system could be inconvenient and might even cause some miner physical damage to the system and an outage that lasted for a few hours or days. A successful physical attack on multiple high voltage power transformers could cause extensive damage and outages that could last for months unless we have a stock of emergency replacement transformers like the one tested in 2012.

Appendix II

Additional Material for the Record

STATEMENT SUBMITTED BY LIEUTENANT COLONEL ALLEN B. WEST

IDEAS CHANGING THE WORLD

Texas is Working to Protect the Electrical Grid Against Natural or Man-Made Electromagnetic Pulse

Statement for the Record

Lieutenant Colonel Allen B. West (U.S. Army, Ret)

President and Chief Executive Officer
National Center for Policy Analysis

"Examining Vulnerabilities of America's Power Supply"

U.S. House Committee on Science, Space and Technology
Subcommittee on Oversight
Subcommittee on Energy

September 10, 2015

Chairman Weber, Chairman Loudermilk, members of the Energy and Oversight subcommittees, thank you for the opportunity to submit written comments about securing the electrical grid against solar storms and man-made electromagnetic pulses. I am Allen B. West, president and CEO of the National Center for Policy Analysis (NCPA). We are a nonprofit, nonpartisan public policy research organization dedicated to developing and promoting private alternatives to government regulation and control, solving problems by relying on the strength of the competitive, entrepreneurial private sector. The NCPA is headquartered in Dallas, Texas.

Having recently moved to Texas, I am proud to report that the state of Texas is showing leadership on this issue by taking action to protect the Texas electrical grid from the damaging effects of a natural or man-made electromagnetic pulse (EMP) that could blackout the entire state for months, with catastrophic consequences. The Texas legislature is moving toward potential legislative solutions, and members of the Executive Branch have met with experts to determine the best course of action to protect the electrical grid in Texas.

EMPs sound like science fiction, but are a real and present danger. EMPs have occurred numerous times with damaging consequences. As far back as 1859, an EMP from a solar storm disrupted telegraph systems throughout America and Europe. In 1921, a solar EMP knocked out railroad signals and switching systems. More recently, in 1989, a solar EMP shut down power transmission in Canada and jammed radio signals throughout North America.

The events of 1859, 1921 and 1989 ought to inform our decisions today. An EMP is like a super-energetic radio wave, so powerful that it can damage and destroy electronic systems within the EMP field. As the world has become more reliant on technology, if a solar EMP of similar magnitude were to occur today, it would potentially cause a protracted nationwide or even global blackout of the electrical grid and other life-sustaining critical infrastructures—including communications, transportation, business and finance, food and water—potentially for months or years.

NASA estimates the likelihood that the Earth will encounter a catastrophic solar storm is 12 percent per decade. This virtually guarantees that we will see a natural EMP catastrophe within our lifetimes or our children's lifetimes. It underscores the vital importance of protecting the electrical grid against solar EMPs.

But solar storms aren't the only sources of catastrophic EMPs. In 2006, Congress created the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. The EMP Commission warned that a nuclear weapon detonated at high-altitude, 300 kilometers above the United States (so high that there would be no blast, fallout, or other effects on the ground from the explosion in the atmosphere) would generate an EMP field over the entire nation. The EMP Commission estimated that a nationwide blackout lasting one year could kill up to 90 percent of Americans by starvation and societal collapse.

North Korea and Iran may have already practiced nuclear EMP attacks by orbiting satellites over the United States, simulating the delivery of an EMP. On a south polar trajectory, the satellites approach the United States from the south, passing over Texas and other states bordering on the Gulf of Mexico. Currently, the United States does not have ballistic missile early warning radars or missile interceptors facing south.

Even if the United States could intercept a warhead disguised as a satellite approaching from the south, the nuclear weapon could "salvage-fuse" by automatically triggering the EMP attack before being intercepted. The Gulf States, including Texas, would be closest to the EMP field, and most at risk.

Furthermore, North Korea and Iran may have also practiced nuclear EMP attacks delivered by short-range missiles. In July 2013, a North Korean freighter transited the Gulf of Mexico with two unarmed, but nuclear capable, SA-2 missiles mounted on their launchers, hidden in the hold. Additionally, Iranian freighters regularly visit their allies in Cuba and Venezuela and have the same potential to carry short-range missiles capable of causing a catastrophic EMP. Again, the Gulf States, including Texas, are most at risk from a ship-launched EMP attack.

Indeed, because Texas has its own electrical grid, and is not part of the Eastern or Western electrical grids that include all the other contiguous states, Texas might be most at risk – and at the same time, the only state in control of its own grid security. An adversary who wants to warn or terrorize the United States might well choose to focus an attack on the Texas grid to demonstrate their power to Washington and the world.

Non-nuclear EMP weapons, called radiofrequency weapons, can also damage or destroy the electrical grid. Terrorists have already employed such weapons in Europe and Asia. Boeing demonstrated such a weapon, called the Counter-electronics High-powered Microwave Advanced Missile Project (CHAMP), which is capable of being delivered by a drone. It is not out of the realm of possibility to imagine a terrorist launching something like a CHAMP from a freighter, or even from Mexico, to deliver a devastating EMP attack on the United States. Texas, once again, is forefront in the danger zone.

Terrorists have figured out that electrical grids are a major societal vulnerability. Terror attacks against the electrical grid have blacked-out 420,000 people in Mexico (October 2013), Yemen's 18 cities and 24 million people (June 2014), 80 percent of Pakistan (January 2015), and most of Turkey (April 2015). Prudence should warn us about the potential for a similar terror attack in the United States. The EMP Commission found that hardening the electrical grid to protect against the worst threat—nuclear EMP attack—would mitigate all lesser threats, including natural and non-nuclear EMP, cyber attacks, physical sabotage, and severe weather.

I am proud of the efforts of Texas state leaders like Representative Tan Parker, Representative Byron Cook, Senator Troy Fraser and Senator Bob Hall, himself an EMP expert, who are working to educate policy makers in Austin about the threat, a service to all Texans who do not want to be in the bull's-eye of an EMP Alamo. Texas Governor Greg Abbott and his administration have an amazing opportunity to take leadership on this important issue. Likewise, there is an important role for your committee and for Congress to take to harden the nation's electrical grid against the dangers of natural and man-made EMPs. The time to act is now.

Thank you for the opportunity to submit these comments. If there is anything the NCPA or I can do to assist you, we are at your service.

STATEMENT SUBMITTED BY DR. GEORGE H. BAKER

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Standard for Geomagnetic Disturbance Operations	**)** **)**	**Docket No. RM14-1-000**

Comments of George H. Baker, Professor Emeritus, James Madison University

Submitted to FERC on March 24, 2014

Pursuant to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking (NOPR) issued on January 16, 2014,[1] Prof. George H. Baker respectfully submits Comments on the Commission's proposal to approve without remand Reliability Standard EOP-010-1 of the North American Electric Reliability Corporation (NERC).

Background of Petitioner

George H. Baker, Ph.D., served on the staff of technical experts for the Congressional Electromagnetic Pulse (EMP) Commission, served in the Defense Nuclear Agency as director of programs for protecting military systems from EMP, and served as Technical Director of the Institute for Infrastructure and Information Assurance at James Madison University. Dr. Baker is a professor emeritus of James Madison University. Currently, Dr. Baker performs EMP, GMD, and RF weapon vulnerability assessments for the United States Department of Defense (DOD).

Summary of Concerns

Based on my work on the EMP Commission, my familiarity with infrastructure vulnerability to the E3 pulse of nuclear EMP,[2] my assessment of the 2003 Northeast Blackout while a professor of critical infrastructure studies, my ongoing assessments of DOD vulnerabilities to both natural

---

[1] *Reliability Standard for Geomagnetic Disturbance Operations*, Notice of Proposed Rulemaking, 141 146 FERC ¶ 61,015 (2014) ("GMD NOPR"), 79 *Federal Register* 3547 (Jan. 22, 2014).

[2] The E3 pulse from nuclear EMP and naturally-occurring GMD have similar effects on the electric grid and telecommunications; both induce harmful currents in long conductors that are grounded at the ends.

and manmade EMP, my participation in emergency planning exercises, and my in-person participation in NERC's GMD Task Force over the past three years, I have concluded that Standard EOP-010-1 is a seriously deficient standard that will not protect the American public from wide-area and long-term electric grid blackout. Standard EOP-010-1 should be remanded by the FERC Commissioners for the following reasons:

1. GMD operating procedures are based on the premise that operators can and will prevent large-scale grid collapse by shedding load. Due to insurance rules, grid operators will be reluctant to shed load to customers, even though load-shedding procedures reduce the probability of grid collapse and damage to EHV transformers. Utility companies know that if customer electric power is lost due to geomagnetic disturbance (GMD), they will not be liable for losses; but if customer power is lost due to intentional human action to de-energize the grid or portions of it, power companies can be held liable. (Ref. Lloyds of London report on GMD effects and liabilities, statements by insurance company representatives at 2012 Electric Infrastructure Security Summit at UK Parliament).

2. The 15-45 minute warning time provided by the ACE satellite or its successor will be inadequate for grid operators to conference in making necessary decisions and then executing required operational procedures. Participants in the 2011 National Defense University-Johns Hopkins University GMD response exercise indicated that they would be hard-pressed even to get all the players to the table within such a short time interval. And, once hit, the grid fails very quickly. We note that, in 1989, during a moderate solar storm GMD, the electric power grid of the entire Province of Quebec went dark in 90 seconds. The August 2003 event evolved over much more slowly (1:31pm – 4:10pm) with much more time available to take action. Nonetheless, even with a course of hours available, power companies were unable to react fast enough to prevent grid collapse.

3. Grid operators will not have adequate information on the state of the grid to implement correct operational procedures. Because most of the grid is not monitored for excess GIC, operators will be "flying blind" with respect to the state of grid, which portions need remedial action, and what actions will be optimal. Information gaps will exist as in August 2003 – where operators were unaware of the initiating tree contact. Sensors needed to monitor GMD/EMP stressors on critical grid components have not been installed. And lack of visibility has led to errors in executing operational procedures that made matters worse.

4. There is no control center with large enough visibility to control operational procedure response on a national scale. Lack of information on neighboring grids impairs proper procedural response. A national control/coordination center does not exist. And there is no single authority over the regional Reliability Coordinators. Because the geographic coverage of solar storm GMD and nuclear EMP can be continental in scale, super-regional control visibility and authority is necessary. At this point, only the federal government, using Presidential authority, can fill this role.

5. Operational procedures have not been adequate to address the more simpler causes of previous large-scale blackouts. Past events provide ample evidence that operational measures are problematic. For instance, operational procedures proved ineffective in preventing the 2003 Northeast blackout that was precipitated by a single failure point involving tree contact with a transmission line. Recent grid models indicate that GMD and EMP will engender hundreds to thousands of failure points. The

complexity and rapidity of grid failure during a Carrington-class event will overwhelm the ability of electric utilities to respond and to prevent grid failure using any suite of operational procedures, no matter how well-conceived and practiced. During Hurricane Sandy, grid physical damage outstripped the effectiveness of procedural protection efforts. Physical damage to grid components will be a factor in GMD/EMP events as well.

6. Unforeseen grid equipment malfunctions have greatly impaired grid operators' ability to respond during major blackouts in the past. Operational procedures during the 2003 Northeast power blackout were greatly impaired by computer control system malfunctions and software problems. Critical grid state monitoring, logging and alarm equipment failed. The control area's SCADA and emergency management systems malfunctioned. The shut-down of hundreds of generators over multiple states was unanticipated as was the failure of tens of transmission lines. Confusion and inoperative control systems lead to many frantic phone calls. Any early failure of major grid components caused by the GMD or EMP environment will impede implementation of subsequent operational procedures.

7. GMD and EMP will affect the communication systems necessary for coordination of operational procedures. Long-line internet and telecommunications networks will experience large overvoltages from GMD and EMP E1/E3 environments, likely causing their debilitation. GMD and EMP also impede signal propagation of HF/VHF/UHF radio systems and GPS systems. Thus grid communication and control systems necessary to execute operational procedures cannot be relied on – just when they are needed the most.

8. It is not possible to anticipate all grid failure point combinations and time sequences during GMD/EMP events in order to adequately plan and exercise GMD/EMP event operational procedures. Normal grid failures are not indicative of GMD/EMP failures. Operators are familiar with single equipment failures but when multiple points fail near simultaneously under GMD/EMP stress and the failures interact and cascade, operators will have difficulty understanding and responding to prevent further damage. In most complex human-machine systems, the interactions literally cannot be seen. Prof. Charles Perrow of Yale defines 'normal accidents' in complex infrastructure systems as involving system interactions that are not only unexpected, but are incomprehensible for some critical period of time. For example, it took an expert NERC investigation team three months to determine the exact combination and sequence of system failures that led to the 2003 blackout.

9. RTOs/ISO's don't have cross-jurisdictional authority to enforce shutdown of neighboring grids, sometimes required to avoid large scale blackouts, as in the August 2003 Northeast Blackout. During that catastrophe, First Energy was asked to shed load by its neighboring grid operators but First Energy declined. According to the NERC after action report, load shedding would have prevented the ensuing Northeast blackout.

10. Draft NERC GMD operational procedures recently submitted to FERC are not comprehensive and not specific. The plans do not apply to generator authorities or load-balancing authorities. The NERC operational procedures also exempt portions of the grid operating below 200KV from operational procedures.

NERC has a pattern and practice of conducting incomplete technical studies and embedding the conclusions in whitepapers then delivered to FERC to justify action or inaction on reliability standards. Key flaws in NERC's technical studies are lack of data collection and exclusion of real-world evidence at odds with NERC's position. With knowledge and perspective from outside of the electric utility industry, as expressed in this comment, I feel compelled to speak out. Because NERC controls the forum and agenda, as it essentially controls the standard development process, NERC's position is difficult to challenge and may even appear to some to be reasonable. But when the United States experiences a wide-area and long-term electric grid blackout, as it surely will should EOP-010-1 be adopted in its present form, any independent inquiry and adjudication would quickly expose NERC's studies and reasoning as technically unsound.

Respectfully submitted by:

George H. Baker
Professor Emeritus
James Madison University
3305 Hemlock Street
Harrisonburg
Virginia
22801