S. HRG. 115–273

EFFORTS TO PROTECT U.S. ENERGY DELIVERY SYSTEMS FROM CYBERSECURITY THREATS

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

APRIL 4, 2017

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
24–979 WASHINGTON : 2018

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

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

COLIN HAYES, *Staff Director*
PATRICK J. MCCORMICK III, *Chief Counsel*
KELLIE DONNELLY, *Deputy Chief Counsel*
ANGELA BECKER-DIPPMANN, *Democratic Staff Director*
SAM E. FOWLER, *Democratic Chief Counsel*
DAVID GILLERS, *Democratic Senior Counsel*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

EFFORTS TO PROTECT U.S. ENERGY DELIVERY SYSTEMS FROM CYBERSECURITY THREATS

TUESDAY, APRIL 4, 2017

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

The Committee met, pursuant to notice, at 10:06 a.m. in Room SD–366, Dirksen Senate Office Building, Hon. Lisa Murkowski, Chairman of the Committee, presiding.

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

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

I want to acknowledge my stand-in Ranking Member, Senator Heinrich. I understand that Ranking Member Cantwell is delayed a little bit coming from the game.

[Laughter.]

Very important.

Senator HEINRICH. I don't know what you are talking about.

The CHAIRMAN. Very important.

I am sure there are those that are happy this morning, and for those of us that love the West Coast and all things West, we are not as excited this morning. But anyway, we will look forward to Senator Cantwell coming later this morning.

We are here today to not talk about basketball, but we are here to examine our collective efforts and those from Congress, the rest of the Federal Government and industry to protect our domestic energy delivery systems from cybersecurity threats.

Here in the United States, we have purposefully built redundant systems to ensure resilience and technological advancements have improved system efficiencies. We have made our devices smarter and connected more of them to the internet, boosting consumer convenience and lowering costs. But as the so-called "internet of things" has become increasingly involved in all phases of energy generation and delivery, we have created even more avenues for cyber intrusion.

This Committee has long recognized that our nation's energy sector is a popular target for bad actors. Everyone from individual hackers to nation-states who wish to do us harm. That is why we took action over a decade ago, through the Energy Policy Act of

2005, to protect the nation's critical grid infrastructure from both physical and cybersecurity threats.

The 2005 law directed the certification of an electric reliability organization, now the North American Electric Reliability Corporation (NERC), to develop and enforce mandatory reliability standards. Congress specifically declined to provide the Federal Energy Regulatory Commission (FERC) with direct authority to establish such standards, instead opting for an industry stakeholder process to assist in formulating these highly complex and technical requirements.

This decision has fostered a robust public/private partnership, and given FERC's current lack of quorum, it perhaps is even more prescient today. I am pleased that NERC's President and CEO, Gerry Cauley, is here to testify this morning.

Last Congress, in the FAST Act, we moved again to protect our energy systems from cyberattack. As enacted, that law includes provisions from this Committee codifying the Department of Energy as the sector-specific agency for the energy sector and providing the Secretary with authority to address grid-related emergencies caused by cyberattacks, physical attacks, electromagnetic pulses (EMP) or geomagnetic disturbances.

We will address the EMP issue, in depth, at a future hearing, but I am looking forward to hearing today from Pat Hoffman, the Acting Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, about the Department of Energy's (DOE) effort to implement its FAST Act authorities.

Finally, while our Committee has spent considerable time over the years examining the threats posed to the nation's grid infrastructure, today we will also assess efforts to secure natural gas pipelines. Given the interdependency of natural gas and electricity, it is imperative that these energy delivery systems are adequately protected. So I look forward to Dave McCurdy's testimony as the President and CEO of the American Gas Association. Mr. McCurdy, I am also curious to know why it is taking so long, particularly, as a former Chairman of the House Intelligence Committee, to get the requisite security clearance from the Energy Department, and we will have an opportunity to chat about that.

In addition, this morning we will hear from Mr. Duane Highley, who is the President and CEO of the Arkansas Electric Cooperative Corporation and the Co-Chair of the Electricity Subsector Coordinating Council (ESCC) which interfaces with the Federal Government on behalf of industry.

We also have Mr. Andrew Bochman, a Senior Cyber and Energy Security Strategist for the Idaho National Laboratory. This is the lab responsible for the Aurora experiment which first demonstrated how a cyberattack could impact physical assets.

We will then hear from Colonel Gent Welsh, from the Washington National Guard, who has done a lot of important work to secure critical infrastructure in that state and develop a cyber workforce.

We all recognize that this is no time for the United States to rest on the question of cybersecurity. The number and scope of attacks is ever-increasing and the resulting harm could be very significant. That is why our Subcommittee, under Senator Gardner's leader-

ship, held a cybersecurity hearing last month and that is why we are broadening the effort here at the full Committee today.

I would like to thank all of our witnesses for joining us this morning, and I look forward to their comments in just a few minutes.

At this time, I will turn to Senator Heinrich for his opening comments.

STATEMENT OF HON. MARTIN HEINRICH, U.S. SENATOR FROM NEW MEXICO

Senator HEINRICH. Thank you, Madam Chairman. As you mentioned, Senator Cantwell is running a few minutes late and asked me to fill in until she arrives.

As a member of the Senate Intelligence Committee, I am acutely aware of the sophisticated threats that our energy infrastructure faces in cyberspace today. Cybersecurity is one of the most serious challenges to our economy and national security that we face as a nation-state. The future of warfare is moving further away from the battlefield each day and closer to the devices and the networks that everyday citizens, as well as the private sector, rely on and depend on.

Protecting our nation from malicious cyber actors requires a very comprehensive approach, and keeping our energy infrastructure secure is absolutely central to that. In January, the U.S. Department of Energy warned that the U.S. grid "faces imminent danger" from cyberattacks.

The Department's Quadrennial Energy Review (QER) warns that a widespread power outage caused by a cyberattack could place at risk the health and safety of millions of U.S. citizens. The QER included a number of policy recommendations for both regulators and Congress. The QER also pointed out that our electric grid has become increasingly reliant on a reliable and secure supply of natural gas, and it is essential to what we do that we do all we can to protect against cyberattacks against natural gas pipelines as well. So I am pleased that Congressman McCurdy will be testifying today on behalf of the American Gas Association to discuss pipeline cybersecurity as well.

Top officials within the intelligence community have testified that energy infrastructure is an enticing target to malicious actors. Those officials have also warned that without action, the U.S. remains vulnerable to cyberattacks that could result in catastrophic damage to public health and safety, economic security and national security.

I am pleased, again, to be an original co-sponsor of Senator King's bipartisan Securing Energy Infrastructure Act, which was the subject of last week's Subcommittee hearing, and I hope we can take action on this bill this year.

Today we are also going to hear from Pat Hoffman, the Acting Assistant Secretary for the Office of Electricity Delivery and Energy Reliability at the Department of Energy. This office, in coordination with our national labs, helps protect our nation's energy infrastructure from a variety of cyber threats.

I am very concerned the President is proposing significant cuts to the Electricity Office's budget that could impair our ability to

meet the challenges foreign actors, and others, present to the security of our nation's energy infrastructure.

Thank you for holding this full Committee hearing today, and I look forward to all of our witnesses' testimony.

The CHAIRMAN. Thank you, Senator Heinrich.

At this time, we will begin with our distinguished panel. I have introduced each of you already, so we will move straight to your comments. I would ask you to keep your comments to five minutes or less. Your full statements will be incorporated as part of the record.

We will begin with Patricia Hoffman, again, the Acting Assistant Secretary for the Office of Electricity Delivery and Energy Reliability at the U.S. Department of Energy, and we will proceed down the line.

Ms. Hoffman, welcome.

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

Ms. HOFFMAN. So, thank you.

Good morning. Thank you, Chairman Murkowski, Ranking Member Cantwell, Senator Heinrich, members of the Committee. Thank you for the opportunity to discuss the continuing threats facing our nation's energy infrastructure and the Department of Energy's role and authorities under the Fixing America's Surface Transportation, or FAST, Act. The Department of Energy is focusing on cybersecurity and resilience of energy delivery systems, and this is one of the Secretary's top priorities.

Our economy, national security, and even the well-being of our citizens depend on the reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability is to strengthen, transform, and improve energy infrastructure to ensure access to reliable and secure sources of energy. The Department is committed to working with our public and private sector partners to protect the nation's critical energy infrastructure, including the electric power grid, from physical security events, natural and man-made disasters and cybersecurity threats.

To address security, it is critical for us to be proactive and cultivate what I call, an ecosystem of resilience, a network of producers, distributors, regulators, vendors and public partners, acting together to strengthen our ability to prepare, respond and recover. We continue to partner with industry, federal agencies, states, local governments and other stakeholders to quickly identify threats, develop in-depth strategies to mitigate those threats and rapidly respond to any disruptions.

DOE plays a critical role in supporting industry functions in several ways. Providing partnership mechanisms that support collaboration and trust, leveraging government capabilities to gather intelligence on threats and vulnerabilities and sharing actionable intelligence with energy owners and operators in a timely manner. We also support energy sector best practices, incident coordination and response and innovation through R&D for the next generation physical and cyber systems.

In the energy sector, the core critical infrastructure partners consist of the Electric Sector Coordinating Council and the Oil and Gas Sector Coordinating Council. Through these partnerships, the energy sector and the government share emerging threat data and vulnerability information.

An example of this type of collaboration is a Cybersecurity Risk Information Sharing Program (CRISP), a voluntary public/private partnership, that is funded by industry, administered by the Electric Sector Information Sharing and Analysis Center and supported by the Department of Energy.

Another example of how the Department supports the cyber posture of the energy industry is through the Department's Cyber Capability Maturity Model, which helps private sector owners and operators better evaluate their cybersecurity capability. This tool allows organizations, regardless of size, type or industry, to evaluate, prioritize and improve their own cybersecurity capabilities.

Beyond providing guidelines and technical support to the energy sector, the Department also supports an R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems.

Intentional, malicious cyber threats challenge our energy systems and are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector. Since 2010, the Department has invested more than $210 million in cybersecurity research development projects that are led by industry, universities and national laboratories. These investments have resulted in more than 35 new tools and technologies.

Threats continue to evolve. The Department of Energy is working diligently to stay ahead of the curve. The solution is an ecosystem of resilience that works in partnership with local, state and industry stakeholders to help provide the methods, the strategies and the tools needed to help protect local communities through increased resilience and flexibility.

To accomplish this we must accelerate information sharing to inform better local investment decisions and encourage innovation and use of best practices to help raise the energy sector's security maturity and strengthen local incident response and recovery capabilities, especially through the participation and training programs, disaster and preparedness exercise.

Building an ecosystem of resilience is, by definition, a shared endeavor, and we must continue to keep a focus on partnerships. This is an imperative.

I thank you for the opportunity for being here today, and I look forward to answering any questions that you may have.

[The prepared statement of Ms. Hoffman follows:]

Testimony of Acting Assistant Secretary Patricia Hoffman

Office of Electricity Delivery and Energy Reliability

U.S. Department of Energy

Before the

Committee on Energy and Natural Resources

United States Senate

April 4, 2017

Introduction

Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure and the Department of Energy's role under the authorities specified in the Fixing America's Surface Transportation – or FAST – Act. At the Department of Energy (DOE), focusing on cybersecurity and the resilience of energy is one of the Secretary's top priorities.

Our economy, national security, and even the well-being of our citizens depend on the reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) – which I oversee in my roles as the Acting Under Secretary for Science and Energy and Acting Assistant Secretary for DOE-OE – is to strengthen, transform, and improve energy infrastructure to ensure access to reliable and secure sources of energy. The Secretary of Energy and DOE are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure, including the electric power grid, from physical security events, natural and man-made disasters, and cybersecurity threats.

Over the past decade, the Nation's energy infrastructure has become a major target of both physical and cyber-attacks. The frequency, scale, and sophistication of cyber threats have increased and attacks can be easier to launch. Cyber incidents have the potential to interrupt energy services, damage highly specialized equipment, and threaten human health and safety. As a result, energy cybersecurity and resilience has emerged as one of the Nation's most important security challenges and fostering partnerships with public and private stakeholders will be of utmost importance in this work.

DOE FAST Act Authority

DOE's role in energy sector security is established in statute and executive action. In 2015, through the FAST Act, Congress assigned DOE as the lead Sector-Specific Agency (SSA) for cybersecurity for the energy sector.

The FAST Act also gave the Secretary of Energy new authority, upon declaration of a Grid Security Emergency by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to

support energy sector preparations for and responses to cyber, electromagnetic pulse (EMP), geomagnetic disturbance (GMD), and physical attack threats.

EMP events are a national concern due to the potential for widespread impact and extended outages from, for example, a high-altitude nuclear burst. To promote government and industry sharing of scientific and testing results, last July, DOE and the Electric Power Research Institute (EPRI) released a Joint Electromagnetic Pulse Resilience Strategy (Joint Strategy). This Joint Strategy is intended to drive efforts to reduce EMP vulnerabilities and improve the response and recovery after EMP events, thus minimizing adverse impacts and improving grid resilience. Following development of the Joint Strategy, both DOE and EPRI committed to developing separate, but coordinated, Action Plans. EPRI's plan focused on industry actions and DOE's on departmental actions to mitigate EMP risks. Although the two Action Plans were developed independently, DOE and EPRI collaborated closely to ensure that the plans complement one another and avoid duplication of effort and implementation of both action plans are underway.

GMDs are naturally occurring phenomena relating to space weather and may have significant impacts on electrical and electronic equipment and systems, including high-frequency radio communications, global navigation satellite systems, long-haul telecommunications/internet exchange carrier lines, and electric power transmission. GMDs can have multiple effects on the electric grid, such as damaged equipment and loss of power over large areas, and can also lead to losses of communications. Significant gaps exist in the understanding of and protection against GMD effects on the electric grid, as well as in optimizing operations to limit GMD effects. Current DOE efforts relate to obtaining better data on GMDs, developing an approach to monitoring the grid and its components for GMD effects, and testing the effectiveness of blocking devices.

Importance of Cybersecurity for Energy Systems and Cybersecurity Threats

In addition to the authorities in the FAST Act related to cybersecurity, we have worked with interagency partners to ensure that our cyber response activities are consistent and integrated with broader national preparedness and incident response efforts. This allows our response to a cyber incident to seamlessly integrate with actions taken to address physical consequences caused by malicious cyber activity.

Principles of cybersecurity often start with computer servers and desktops, the heart of systems generally referred to as "information technology," or IT. As we are all aware, hackers are targeting computing technology and business applications to cause disruptions, obtaining access to email accounts and personal information, exfiltrating data to release to the world at large, and exploiting information for private gain. The energy sector is not immune to such attacks.

In the 2012 Shamoon attack, weaponized malware hit 15 state bodies and private companies in Saudi Arabia, wiping more than 35,000 hard drives of Saudi Aramco, from which the company took more than two weeks to recover. And again in January of this year, Shamoon 2 hit three state agencies and four private sector companies in Saudi Arabia, leaving them offline for at least 48 hours.

While the Shamoon and other similar-style attacks have targeted IT systems, the energy sector is also targeted because of the assets they control and the value they represent. Accordingly, this has also increased interest in vulnerabilities of the "operating technology," or OT, of energy delivery systems and other critical infrastructure as well. OT systems consist of industrial control systems (or ICS), programmable logic controls, and its associated supervisory control and data acquisition software (known as SCADA). The heavy use of OT systems has made electric utilities, oil and natural gas providers, hydro and nuclear facilities, and water utilities prime targets for OT-related cyber-attacks. The disruption of any one of these is not only inherently problematic, it also hampers the ability to respond to any type of emergency event.

In December 2015, the first known successful cyber-attack on power grid OT took place in Ukraine. Over 225,000 residents were left without power for several hours in the coordinated attack, and a second attack occurred in December 2016 that left portions of Kiev without electricity. These two cyber-attacks demonstrated the real world, physical impacts that can occur through cyber means.

Ecosystem of Resilience

To address these challenges, it is critical for us to be proactive and cultivate what I call an ecosystem of resilience: a network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover. We continue to partner with industry, Federal agencies, states, local governments, and other stakeholders to quickly identify threats, develop in-depth strategies to mitigate those threats, and rapidly respond to any disruptions.

DOE plays a critical role in supporting industry functions in several ways: providing partnership mechanisms that support collaboration and trust; leveraging government capabilities to gather intelligence on threats and vulnerabilities, and share actionable intelligence with energy owners and operators in a timely manner; developing supportive tools that encourage cybersecurity best practices in the energy sector; developing tools and capabilities to conduct risk analysis; supporting energy sector incident coordination and response; and, supporting innovation and R&D for next-generation physical-cyber systems.

Importance of Partnerships

The Department of Energy has collaborated with the energy sector for nearly two decades in voluntary public-private partnerships that engage energy owners and operators at all levels – technical, operational, and executive, along with state and local governments – to identify and mitigate physical and cyber risks to energy systems.

These partnerships are built on a foundation of earned trust that promotes the mutual exchange of information and resources to improve the security and resilience of critical energy infrastructures. These relationships acknowledge the special security challenges of energy delivery systems and leverage the distinct technical expertise within industry and government to develop solutions.

The security and integrity of energy infrastructure is both a state and Federal government concern because energy underpins the operations of every other type of critical infrastructure; the economy; and public health and safety. The owners and operators of energy infrastructure, however, have the primary responsibility for the full spectrum of cybersecurity risk management: identify assets, protect critical systems, detect incidents, respond to incidents, and recover to normal operations.

When the lights go out or gasoline stops flowing in pipelines, the first responder is usually not the state or Federal Government but, rather, industry or local government. This is why public-private partnerships regarding cybersecurity are paramount – they recognize the distinct roles and capabilities of industry and government in managing our critical energy infrastructure risks.

In the Energy Sector, the core of critical infrastructure partners consists of the Electricity Subsector Coordinating Council (ESCC), the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and the Energy Government Coordinating Council (EGCC). The ESCC and ONG SCC represent the interests of their respective industries. The EGCC, led by DOE and co-chaired with DHS, is where the interagency, states, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures that we're working together in a whole-of-government response.

As defined in the National Infrastructure Protection Plan, the industry coordinating councils or "SCCs" are created by owners and operators and are self-organized, self-run, and self-governed, with leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.

The SCCs, EGCC, and associated working groups operate under the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a mechanism for industry and government coordination. The public-private critical infrastructure community engages in open dialogue to mitigate critical infrastructure vulnerabilities and to help reduce impacts from threats.

Strengthening Energy Sector Cybersecurity Preparedness

As the Energy SSA, DOE works at many levels of the electricity, petroleum, and natural gas industries. We interact with numerous stakeholders and industry partners to share information, discuss coordination mechanisms, and promote scientific and technological innovation to support energy security and reliability. By partnering through working groups between government and industry at the national, regional, state, and local levels, DOE facilitates enhanced cybersecurity preparedness.

Cybersecurity Risk Information Sharing Program

It is necessary for partners in the Energy Sector and the government to share emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyber-attacks more rapidly. An example of this type of collaboration is the Cybersecurity Risk Information Sharing Program (CRISP), a voluntary public-private partnership that is funded by industry, administered by the Energy Sector Information Sharing and Analysis Center (E-ISAC), and supported by DOE in both intelligence analysis through DOE's Office of Intelligence and Counterintelligence and from an R&D standpoint by DOE-OE. One of DOE's National Laboratories – the Pacific Northwest National Laboratory – is a key partner for the E-ISAC in accomplishing the goals of the CRISP program.

The purpose of CRISP is to share information among electricity sector partners, DOE, and the Intelligence Community to facilitate the timely bi-directional sharing of unclassified and classified threat information to enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the Intelligence Community to better inform the energy sector of the high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental United States electricity customers.

Cybersecurity Capability Maturity Model

Another example of how DOE supports the cyber posture of the energy industry is DOE-OE's Electricity Subsector Cybersecurity Capability Maturity Model (C2M2) to help private sector owners and operators better evaluate their cybersecurity capabilities. The C2M2 evaluation allows organizations – regardless of size, type, or industry – to evaluate, prioritize, and improve their own cybersecurity capabilities.

DOE and the oil and natural gas (ONG) subsector collaborated extensively to develop a C2M2 version specifically for them. The model was tested and refined for the subsector through pilot evaluations across upstream, midstream, and downstream ONG companies.

Owners and operators across the subsector are utilizing these best practices. The C2M2 evaluation workshops facilitated by the American Gas Association are a strong example of their use.

Since the C2M2 program's inception in June 2012, more than 1,100 C2M2 toolkits have been distributed, many to domestic energy sector companies. The tool enables voluntary, consistent measurement of the maturity of an organization's cybersecurity capabilities. This is a comprehensive and credible approach that energy sector companies can use to improve their cybersecurity posture. In addition to the electricity and ONG versions, a sector agnostic C2M2 version has been created for industry at large.

As we move forward, we continue to engage stakeholders from both the electricity and ONG subsectors to leverage insights gathered from industry to further enhance the C2M2 model.

National Association of Regulatory Utility Commissioners Primer

DOE-OE also works to provide guidance to the Nation's policy makers on improving their cybersecurity. As a recent example, DOE-OE and the National Association of Regulatory Utility Commissioners (NARUC) sponsored the third edition of a cybersecurity primer for regulatory utility commissioners. This document was published in January of this year and is publicly available on the NARUC Research Lab website, benefitting not only regulators, but state officials focused on the sector as well.

The updated cyber primer provides best practices, access to industry and national standards, sample questions, and easy reference materials for Commissions in their engagements with utilities to ensure their systems are resilient to cyber threats.

We are continuing to work with the NARUC Research Lab to support regional trainings on cybersecurity throughout the year, with the goal of building commissioner and commission staff expertise on cybersecurity so they ensure cyber investments are both resilient and economically sound.

Coordinating Cyber Incident Response and Recovery

Cyber Incident Coordination

The emergency authorities established under the FAST Act enable the Secretary to undertake certain actions within the context of a Grid Security Emergency. These actions require a swift and coordinated response in collaboration with industry partners to secure critical energy infrastructure and to support response and restoration efforts.

In the event of a significant cyber incident, a national Cyber Unified Coordination Group (UCG) would be activated. The Department of Homeland Security's National Cybersecurity and Communications Integration Center, or NCCIC, would be designated as the Asset Response Lead, the National Cyber Investigative Joint Task Force, or NCIJTF, would be designated as the Threat Response Lead and the Cyber Threat Intelligence Integration Center, or CTIIC, would be responsible for leading intelligence support. Under the UCG, DOE, in its role as the energy sector SSA, would be responsible for leading sector coordination and enabling sector specific technical assessments and assistance.

We continue to work closely with our public and private partners to ensure that our response and recovery capabilities fully support and bolster the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with the SCCs to synchronize DOE and industry cyber incident response playbooks.

Cyber Exercises

DOE-OE also engages directly with our public and private sector stakeholders to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. Innovation and

preparedness are vital to grid resilience. This past December, DOE and the National Association of State Energy Officials co-hosted the Liberty Eclipse Exercise in Newport, Rhode Island, which focused on a hypothetical cyber incident that cascaded into the physical world, resulting in power outages and damage to oil and natural gas infrastructure.

The event featured 96 participants from 13 states, and included representatives from state energy offices, emergency management departments, utility commissions, as well as Federal partners, such as FEMA, and private sector utilities and petroleum companies.

In addition to building up participant knowledge of the cyber threat and the roles and responsibilities of the government in a cyber incident, it brought stakeholders from all aspects of the energy emergency management spectrum together to further build relationships and share expertise.

As a result of this event, a number of states are now looking to update their energy assurance and incident response plans to include more robust coordination of cyber incidents in the energy sector.

Accelerating Game-Changing Cyber Research, Development, and Deployment

Beyond providing guidance and technical support to the energy sector, DOE-OE also supports an R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems. Intentional, malicious cyber threat challenges to our energy systems are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control and OT systems is much different than that of typical IT systems. Power systems must operate continuously with high reliability and availability. Upgrades and patches can be difficult and time consuming, with components dispersed over wide geographic regions. Further, many assets are in publicly accessible areas where they can be subject to physical tampering. Real time operations are imperative and latency is unacceptable for many applications. Immediate emergency response capability is mandatory and active scanning of the network can be difficult.

DOE-OE's Cybersecurity for Energy Delivery Systems (CEDS) R&D program aligns activities with Federal and private sector priorities, envisioning resilient energy delivery control systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

The CEDS R&D program is designed to assist the energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. DOE-OE co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber-incident for our present and future energy delivery systems.

Since 2010, DOE-OE has invested more than $210 million in cybersecurity research, development, and demonstration projects that are led by industry, universities, and the National Laboratories. These investments have resulted in more than 35 new tools and technologies that are now being used to further advance the resilience of the Nation's energy delivery systems.

Closing

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

Building an ecosystem of resilience is – by definition – a shared endeavor, and keeping a focus on partnerships remains an imperative. DOE will continue its years of work fostering these relationships and investing in technologies to enhance security and resilience, ensuring the electric power grid continues to be able to withstand, respond, and recover quickly from all threats and hazards.

The CHAIRMAN. Thank you, Ms. Hoffman.

Next we will turn to Mr. Gerry Cauley, welcome.

STATEMENT OF GERRY W. CAULEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. CAULEY. Thank you and good morning, Chairman Murkowski, Ranking Member Cantwell and Senator Heinrich and members of the Committee. Thank you for conducting this timely hearing to assess the progress and challenges of securing the power grid which is critical to our nation's security and well-being. The threat of cyberattacks by nation-states, terrorist groups and criminal actors is at an all-time high.

In December 2015, a cyberattack in the Ukraine left over 225,000 customers without power for several hours. This indicates that nation-state adversaries have the tools and clearly now the will to disrupt the grid of another nation.

More recently in the U.S., although no part of the grid was affected, we saw a million electronic devices all part of the internet of things, captured and used in a denial of service attack disrupting major internet service providers.

We've seen increases in ransomware, data theft and other criminal activities across all sectors of our economy.

NERC's role is to assure the reliability and security of the bulk power system through mandatory standards, compliance monitoring and enforcement and reliability assessments. Our independent board and staff are unaffiliated with system owners and operators.

FERC approves NERC's standards and enforcement actions in the U.S. and has authority to direct NERC to develop new or revised standards.

As a nation, we share an interconnected grid with our neighbors which is why NERC is international in scope, spanning the United States, Canada and Mexico.

Our cyber standards are written with inputs from the best experts in industry and provide a strong foundation for security practices.

NERC and its eight regions also have cyber experts, who conduct hundreds of site visits every year to assess security controls. We're finding that power companies take cybersecurity very seriously with strong attention at the top from CEOs and boards.

Grid control cyber assets communicate over private networks, including fiber, microwave and lease circuits. They are isolated from business systems and from the public internet.

Utility personnel are screened and well-trained. Companies are using advanced security services from third party providers to maintain the latest threat information.

Most importantly, power companies know they must continuously monitor and detect suspicious activity, isolate malware and destroy it before an attack happens, commonly known as the "kill chain."

As flexible and risk-based as our standards are, I firmly believe we cannot win a cyber war with regulations and standards alone. Industry must be agile and continuously adapt to threats. To do

that, we need robust sharing of information regarding threats and vulnerabilities.

NERC operates the Electricity Information Sharing and Analysis Center. Our role is to assimilate intelligence, to share trusted information with industry and the government and to recommend specific actions.

One of our most effective tools in this effort is the Cybersecurity Risk Information Sharing Program, as mentioned by Ms. Hoffman. Developed by the Department of Energy, CRISP has been adopted by NERC and deployed across wide areas of the U.S. grid to continuously detect malicious activity and share that information with industry.

NERC can also issue formal alerts to industry at three levels of urgency, two of which require responses.

NERC conducts an annual grid assurance, grid security conference and training events and frequent classified briefings.

We also conduct a continent-wide cyber and physical security exercise, called GridEx, with over 4,000 participants from industry and government across North America engaged for two days responding to a simulated massive attack on our grid.

To date, there's not been a single cyberattack in the U.S. resulting in customer outages. This is an exceptional record and is due, in large part, to the vigilance of NERC, industry and our government partners; however, we will never be complacent. The risk is very real, and we have to work hard every day to stay ahead of our adversaries.

I'll close by mentioning a few challenges ahead: securing millions of electronic devices being installed on distributed energy systems and behind the mirror; ensuring the security chain within our—security of our global supply chain; building a more robust public/private model to coordinate strategy and resources between the government and industry; expanding the sharing of classified information; filling a growing gap in cyber workforce; coordinating across critical infrastructures like telecom, finance and gas; and investing in grid resilience, including strategic reserves.

I thank you for the time this morning, and I look forward to your questions.

[The prepared statement of Mr. Cauley follows:]

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

Before the Senate Committee on Energy and Natural Resources
"Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats"

April 4, 2017

Introduction

Good morning Chairman Murkowski, Ranking Member Cantwell, members of the committee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). NERC's mission is to assure the reliability and security of the bulk power system (BPS) in North America. The threat of cyber attacks by nation states, terrorist groups, and criminals is at an all-time high. Now more than ever, grid security is inextricably linked to reliability. The North American BPS is among the nation's most critical infrastructures. Virtually every critical sector depends upon electricity. The BPS is also one of the largest, most complex systems ever created. It is robust and highly reliable. Nevertheless, conventional and non-conventional factors do present risks to the BPS. I am pleased to speak with you today about NERC's responsibilities for grid security.

Summary

The security landscape is dynamic, requiring constant vigilance and agility. NERC assures grid security through a comprehensive series of complementary strategies involving mandatory standards, information sharing, and partnerships. NERC's mandatory critical infrastructure protection standards (CIP standards) are a foundation for security practices. They provide universal, baseline protections. Due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Vigilance also requires the agility to respond to new and rapidly changing events. Accordingly, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) serves as the information sharing conduit between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to maintain "ground truth" during rapidly evolving security events. The E-ISAC also plays a key role in cross-sector communications. Together, mandatory standards, coupled with effective mechanisms to share information, provide robust and flexible tools to protect the BPS. NERC works closely with the Electricity Subsector Coordinating Council (ESCC) to further the public private partnership so important to addressing security.

About NERC

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

NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC performs a critical role in real-time situational awareness and information sharing to protect the electricity industry's critical infrastructure against threats to the BPS. NERC's area of responsibility spans the continental United States, Canada, and Mexico. Our jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

Critical Infrastructure Protection Standards

With oversight by FERC, NERC is responsible for developing and enforcing mandatory reliability and security standards for the BPS. These standards provide a common, universal foundation for security. They are robust and comprehensive, covering a wide range of priorities and threat vectors.

More than a decade ago, Congress had the foresight to anticipate the emerging risk posed by cyber security threats to the BPS. The Energy Policy Act of 2005 expressly states that reliability standards extend to "cybersecurity protection." NERC's CIP standards are developed by registered entities through an open, transparent stakeholder process, subject to approval by NERC's Board of Trustees and FERC. In addition, FERC can order NERC to develop a standard and has done so on topics such as geomagnetic disturbances, physical security, and supply chain cyber security risk.

Currently, NERC is implementing the fifth version of the CIP standards which include the following 11 topics addressing cyber and physical security:[1]

Cyber System Categorization – Identifies and categorizes bulk electric cyber systems and their associated cyber assets (CIP-002-5.1a). This categorization is used as a basis for determining the level of controls applicable to those systems in the rest of the CIP cyber security standards.

Security Management Controls – Specifies consistent and sustainable security management controls (CIP-003-6). This standard also identifies the security controls for those systems identified as "low impact" under CIP-002-5.1.

Personnel and Training – Requires that personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. (CIP-004-6).

Electronic Security Perimeters – Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter (CIP-005-5).

[1] To view NERC CIP standards, see http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United%20States.

Physical Security of Bulk Electric System (BES) Cyber Systems – Requires a physical security plan in support of protecting BES cyber systems (CIP-006-6).

Security System Management – Specifies technical, operational, and procedural requirements in support of protecting BES Cyber Systems (CIP-007-6).

Incident Reporting and Response Planning – Specifies incident reporting and response requirements (CIP-008-5).

Recovery Plans for BES Cyber Systems – Specifies recovery plan requirements in support of the continued stability, operability, and reliability of the BES (CIP-009-6).

Configuration Change Management and Vulnerability Assessments – Prevents and detects unauthorized changes to BES cyber systems by specifying configuration change management and vulnerability assessment requirements (CIP-010-2).

Information Protection – Prevents unauthorized access to BES cyber system information by specifying information protection requirements in support of protecting BES cyber systems against compromise (CIP-011-2).

Physical Security – Requires identification and protection plans for certain "grid-critical" transmission stations and transmission substations, and their associated primary control centers (CIP-014-2).

In addition to these 11 currently enforceable standards, NERC is currently developing a new standard pursuant to FERC directive to address supply chain cyber security risk.

Cyber Security Supply Chain Management (Under Development) – Requires entities to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with BES operations (CIP-013-1).

Electricity Information Sharing and Analysis Center

NERC's CIP standards provide a universal foundation for security practices. Yet security cannot be achieved through these standards alone. Because of the emerging and dynamic nature of malicious cyber threats, reliability assurance also requires constant situational awareness, real time communication, and prompt emergency response capabilities. The E-ISAC provides these services and supports these industry capabilities.

Operated by NERC, in collaboration with the Department of Energy (DOE) and the ESCC, the E-ISAC is the central information sharing hub for the electricity sector. E-ISAC services enable industry to defend against and respond to cyber and physical security threats, vulnerabilities, and incidents through the exchange of timely, actionable information. The E-ISAC also promotes cross-sector communication through work with DHS and other agencies. In order to further enhance cross-sector collaboration in light of electric and natural gas interdependencies, the E-ISAC has partnered with the Downstream Natural Gas ISAC (DNG ISAC). Security is a global priority, and because NERC is an international organization, the E-ISAC works with Natural Resources Canada and Public Safety Canada to provide cross-border

outreach and collaboration. Under a recently-signed memorandum of understanding with Mexico, we are pursuing similar relationships with Mexican authorities.

The E-ISAC:[2]

- Identifies, prioritizes, and coordinates the protection of critical power services, infrastructure service, and key resources;
- Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices;
- Provides rapid response through the ability to effectively contact and coordinate with asset owners and operators, as required;
- Authors alerts to industry ranging from advisory notices to essential actions requiring recipients to respond as defined in the alert;
- Provides and shares analysis, which includes capturing and correlating trend data for historical analysis, and sharing that information within the sector;
- Receives incident data from private and public entities;
- Assists DOE, FERC, and the Department of Homeland Security (DHS) in analyzing event data to determine threats, vulnerabilities, trends and impacts for the sector, as well as interdependencies with other critical infrastructures (this includes integration with the DHS National Cybersecurity and Communications Integration Center (NCCIC));
- Analyzes incident data and prepares reports based on subject matter expertise in security and the BPS;
- Shares threat alerts, warnings, advisories, notices, and vulnerability assessments with the industry;
- Works with other ISACs to share information and provide assistance during actual or potential sector disruptions whether caused by intentional, accidental, or natural events;
- Develops and maintains an awareness of private and governmental infrastructure interdependencies;
- Provides an electronic, secure capability for the E-ISAC participants to exchange and share information on all threats to defend critical infrastructure;
- Participates in government critical infrastructure exercises; and
- Conducts outreach to educate and inform the electricity sector.

In addition to these activities and services, the E-ISAC has partnered with DOE on the Cybersecurity Risk Information Sharing Program (CRISP). Managed by the E-ISAC, CRISP uses innovative technology and leverages DOE's analytical capabilities. CRISP provides timely bi-directional sharing of unclassified and classified threat information and develops situational awareness tools to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure.

[2] See https://www.esisac.com/.

NERC Alerts

NERC also employs an alert system designed to provide concise, actionable security information to the electricity industry. NERC staff with appropriate security clearances often work with cleared personnel from federal agencies to communicate unclassified sensitive information to the industry in the form of NERC Alerts. As defined in NERC's Rules of Procedure, alerts are divided into three levels:

- Level One – Industry Advisory: Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- Level Two – Recommendation to Industry: Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the alert.
- Level Three – Essential Action: Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the alert.

NERC determines the appropriate alert notification based on risk to the BPS. Generally, NERC distributes alerts broadly to users, owners, and operators of the North American BPS using its Compliance Registry. Entities registered with NERC are required to provide and maintain updated compliance and cyber security contacts. NERC also distributes the alerts beyond BPS users, owners, and operators to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., Balancing Authorities, Transmission Operators, Generation Owners, etc.). Alerts are developed with the strong partnership of federal technical organizations, including FERC, DOE National Laboratories, DHS, and BPS subject matter experts. Since 2009, NERC has issued 41 cyber-related alerts (37 Industry Advisories and 4 Recommendations to Industry). Those alerts covered items such as Sabotage events, Aurora, Stuxnet, Night Dragon, and the reporting of suspicious activity. In 2016, NERC issued two Level Two alerts – the first related to the cyber security event in Ukraine and another concerning distributed denial of service attacks involving compromised Internet of Things[3] devices. Responses to alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders.

The NERC alert system is working well. It is understood by industry, handles sensitive information, and communicates this information in an expedited manner. The information needed to develop the alert is managed in a confidential manner. Information sharing through the E-ISAC is the greatest asset we have to combat emerging threats to cyber security and help ensure the reliability of the BPS.

[3] The Internet of Things (IoT) refers to devices and sensors connected to the Internet such as security cameras, alarm systems, printers, or light switches. IoT devices typically use default passwords and are highly vulnerable to subversion by threat actors.

GridEx

Consistent with our mission to promote a strong learning environment, NERC hosts a biennial grid security exercise – GridEx – which simulates widespread, coordinated cyber and physical attacks on critical electric infrastructure. Led by the E-ISAC, NERC conducted GridEx III on November 18–19, 2015.[4] GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise and a separate executive tabletop session featuring 32 industry executives and senior officials from federal and state governments. All told, more than 4,400 individuals from 364 industry, law enforcement and government organizations across North America participated in GridEx III.

The objectives of GridEx III were to:

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

GridEx III provided participants with the opportunity to exercise their incident response procedures during large-scale security events affecting North America's electricity system. The large-scale cyber and physical attack scenario was designed to overwhelm even the most prepared organizations. Participating organizations were encouraged to identify their own lessons learned and share them with NERC. NERC used this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS. Planning for GridEx IV in November 2017 is well underway.

GridSecCon

Consistent with promoting a learning environment and information exchange, NERC hosts the annual Grid Security Conference (GridSecCon). This widely attended conference brings together cybersecurity and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity sector. While the specific agenda varies from year to year, general objectives include:

- Promoting reliability of the BPS through training and industry education;
- Delivering cutting-edge discussions on security threats, vulnerabilities, and lessons learned from senior industry and government leaders; and
- Informing industry with security best-practice discussions on reliability concerns, risk mitigation, and physical security and cybersecurity threat awareness.

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

Ukraine

Cyber attacks on three distribution utilities in Ukraine on December 23, 2015, garnered significant attention. The Ukrainian incidents affected up to 225,000 customers in three distribution-level service territories and lasted for several hours.[5] A team from the United States, which included experts from DOE, DHS, the Federal Bureau of Investigation and NERC, assisted the government of Ukraine in gaining more insight into the event.[6] The events in Ukraine are a reminder that cyber threats are real and that constant vigilance is needed to protect the reliability of the North American grid. At the same time, it is important to note that the operational and technical aspects of the North American BPS are different from those of the Ukrainian system. Other differences include the U.S. industry's mandatory and enforceable cyber security standards, including security management controls and authorized personnel and training controls; network segmentation; and the use of licensed anti-virus software, among other things.

Conclusion

Reliability is NERC's mission, and grid security is inextricably linked to reliability. To date, there has not been any loss of load in North America that can be attributed to a cyber attack. At the same time, the security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber threats through a comprehensive range of complementary strategies. Mandatory CIP standards provide a universal foundation for security. Through the E-ISAC, NERC provides situational awareness, and sharing of timely, actionable intelligence with industry and government. Strong public private partnerships are key to successful information sharing within the electricity sector and across sectors. NERC remains keenly focused on our mission to assure reliability of the BPS.

---

[5] "Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case," SANS Industrial Control Systems and E-ISAC, March 18, 2016.

[6] See ICS-CERT report at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

The CHAIRMAN. Thank you, Mr. Cauley.

We will next turn to Mr. Duane Highley, the President and CEO of the Arkansas Electric Cooperative Corporation.

STATEMENT OF DUANE D. HIGHLEY, PRESIDENT AND CEO, ARKANSAS ELECTRIC COOPERATIVE CORPORATION

Mr. HIGHLEY. Thank you.

Good morning, Chairman Murkowski, Ranking Member Cantwell, Senator Heinrich and members of the Committee. Thank you for the invitation to testify today. I'm speaking on behalf of Arkansas Electric Cooperative Corporation where I serve as CEO and the National Rural Electric Cooperative Association which represents 900 not-for-profit consumer-owned utilities serving 42 million people in 47 states.

I also serve as one of three co-chairs of the Electric Subsector Coordinating Council, or ESCC, a CEO level, public/private partnership serving as our subsector's principle entity in coordinating with our senior government counterparts on policy level issues. The 30 CEOs on our council meet regularly with senior officials from the White House, Department of Energy, Department of Homeland Security, Federal Energy Regulatory Commission, Federal Bureau of Investigation, et cetera.

The electric sector, like other critical sectors, is now at the front lines of international warfare. We're under constant cyberattack. Many of those attacks are sponsored by foreign enemies and nation-states.

Though the recently updated Quadrennial Energy Review recommends protecting the electric sector as a national security asset, it's important to remember that most of the critical infrastructure is owned and operated by private industry. So, for that reason, we must have timely access to actionable information obtained through the defense and intelligence gathering capabilities of our government. We have to work together to protect the grid.

Our traditional design of the electric grid relies on defense in depth to maintain reliability. We designed the grid to survive significant natural disasters with minimal interruption and generally quick recovery. That same redundancy makes the grid very resilient to intentional cyberattacks.

The electric sector is also the only sector with mandatory enforceable reliability and cybersecurity standards developed through NERC. We have to meet these standards and verify compliance through audits conducted by NERC's regional entities or face fines and penalties, potentially as high as $1 million per day per violation. And we take those standards very, very seriously.

That said, just relying on defense, in depth and mandatory standards is not enough. That's why we're developing real time communication environment for sharing threat information between government and industry.

Real time sharing is great but both parties have to play. I can share with you examples of times in the past when we became aware that our government counterparts knew about a developing threat, but were unable to share it because of the classified nature of the threat itself. Often we've learned of threats from private sec-

tor sources well before our government counterparts chose to share them with industry.

One of the primary initiatives of the Electric Subsector Coordinating Council is to work together to improve information sharing in both directions, government to industry and industry to government.

I believe that we've developed a mutual trust relationship and we've obtained some security clearances but not enough across the sector and not enough at a higher level of clearance, and we have contributed to the development of and deployed tools such as DOE's cybersecurity capability and maturity model, the Electric Information Sharing and Analysis Center, the E-ISAC, the Cyber Risk Information Sharing Program, or CRISP, in partnership with DOE and the national labs.

These tools, clearances and briefings have helped, but we can still do more. We have to work together and we have to be able to trust one another to communicate threat information in real time.

I'm pleased to report we've already met with Secretary Perry at DOE and leadership at the White House and FERC in the transition, and I'm confident in their commitment to maintain the momentum of the prior Administration in supporting, funding and staffing our many developing projects.

In particular, we're very pleased at the response of DOE for greater assistance to smaller electric systems such as cooperatives and municipals. Last year DOE provided funding to the trade associations to assist their member utilities in improving cyber and physical security. The co-ops have used these funds to create the Rural Cooperative Cybersecurity Capabilities Program, or RC3, to assist the smaller utility systems.

ESCC has also recently developed a Cyber Mutual Assistance Program modeled after existing mutual assistance programs where utilities mobilize staff across the country to help restore service after a disaster. The Cyber Mutual Assistance Program provides a steady cadre, a ready cadre, of IT staff to assist in restoration of critical systems, if needed. We already have 93 member systems, including 18 cooperatives, on board. So now, 80 percent of all utility customers in the United States are covered by this program.

In summary, the electric sector has mandatory enforceable cybersecurity standards and redundant design providing defense in depth to protect us. But that's not the entire answer to defending against an ever-changing threat.

To bridge the gap, we need an ongoing dialogue and ever more open information sharing, finding ways to provide more and higher level security clearances to our staff who are at the front lines, rapidly declassifying and sharing threat information and jointly developing new solutions to protect against this threat.

I look forward to your questions.

[The prepared statement of Mr. Highley follows:]

Testimony of Mr. Duane D. Highley

President and CEO of the Arkansas Electric Cooperative Corporation (AECC)

to the Committee on Energy and Natural Resources

U.S. Senate

April 4, 2017

Duane Highley, President and CEO
Arkansas Electric Cooperative Corporation
April 4, 2017 Testimony

Introduction

Chairwoman Murkowski, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify before you on this very important topic, it is an honor. I am here today to testify on behalf of the Arkansas Electric Cooperatives Corporation (AECC) and the National Rural Electric Cooperative Association (NRECA) about efforts to protect U.S. energy delivery systems from cyber security threats. First, a little background about myself and those I am representing today prior to getting into how we guard against and recover from energy disruptions utilizing private-public partnerships, processes, and regulations.

As an engineer with 34 years of experience in a sector that many call the most critical of the critical, I continuously strive along with other owners and operators in the sector to ensure reliable, resilient and affordable power so that our communities and neighbors can depend on the light switch in their homes and businesses.

I serve as President and CEO of AECC, a not-for-profit power supply system serving 17 distribution systems, which in turn serves over 1 million Arkansans. I report to a democratically-elected board consisting of the customers we serve. AECC was created in 1949 and provides power for more than 500,000 farms, homes and businesses served by our 17 electric distribution cooperative owners. AECC relies on a diverse generation mix to serve its members, including hydropower, natural gas, coal, biomass, wind and solar.

In addition, I also serve as President and CEO of Arkansas Electric Cooperatives Inc. (AECI), which provides construction, right-of-way, and electrical products to utilities across the U.S. AECI's subsidiary ERMCO is one of the largest manufacturers of distribution transformers for utilities nationwide. AECI's newest subsidiary Today's Power Inc. (TPI) develops utility-scale, community solar projects and produces do-it-yourself solar kits to enable household distributed generation.

The electric cooperatives of Arkansas are members of the National Rural Electric Cooperative Association (NRECA), a service organization for over 900 not-for-profit consumer-owned electric utilities serving 42 million people in 47 states. Electric cooperative service territory covers 75 percent of the nation's land mass and includes over 19 million businesses, homes, schools, churches, farms, irrigation systems, and other establishments in 2,500 of 3,141 counties in the U.S. NRECA's membership includes 65 generation and transmission (G&T) cooperatives, which provide wholesale power to distribution co-ops through their own generation or by purchasing power on behalf of the distribution members. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent on the market.

As member-owned, not-for-profit utilities, distribution cooperatives and G&Ts reflect the values of our membership, and they are uniquely focused on providing reliable energy at the lowest reasonable cost. We have to answer to our owners and justify every expense to them. There is never any debate as to whether a proposed project will benefit our shareholders or our customers, because they are one and the same.

I also serve as one of the three co-chairs who jointly lead the Electricity Subsector Coordinating Council (ESCC), a public/private partnership of the type outlined in the National Infrastructure Protection Plan (NIPP) for critical infrastructure owners and operators to serve as the sectors' principal entity with the government on policy-level security issues. Though membership of these councils vary dramatically across the critical infrastructure sectors, in the electric sector the council is composed of 30 utility and trade association CEOs, representing all segments of the electricity industry, and it engages regularly with its government counterparts, including, senior Administration officials from the White House, Department of Energy (DOE), Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the Federal Bureau of Investigation (FBI) and others as needed.

Cyber Security in the Electric Sector

Protecting the nation's complex, interconnected network of generating plants, transmission lines, and distribution facilities which make up the electric power grid to ensure a supply of safe, reliable, secure and affordable electricity, is a top priority for electric co-ops and other segments of the electric power industry.

Often news headlines about cyber or physical threats to the electric grid focus on far-fetched scenarios or sensationalized claims. However, though there are real and legitimate threats to the grid, the scenarios most often put forth for public consumption are rarely reflective of the real threat environment but rather disproportionally emphasize the highest consequence scenarios that are the least likely to occur. Many of the more dramatic scenarios would constitute acts of war on the United States that would directly impact more than just the electric sector. In addition, these news headlines don't take into account our expert operator actions and plans that each and every day work to ensure reliable and resilient electricity.

Defense in Depth

We didn't originally design the electric grid to defend against intentional physical or cyber attacks nor acts of war, but fortunately our normal preparations against severe weather and equipment failure serve us well in limiting the potential impact of intentional actions. This approach to protecting critical assets is known as defense-in-depth. To protect against extreme weather events, vandalism and major equipment failure, a high level of redundancy is built into the power supply system. The grid is designed to reliably deliver the highest possible summer or winter peak load demand even when our most critical facilities are out of service – that is our standard. Because of this we have withstood intentional attacks such as the 2013 California substation and Arkansas transmission line attacks with no loss of customer service, despite severe damage to our infrastructure.

The grid is incredibly resilient – imagine the worst ice storm – thousands of poles and wires down – and even in these severe cases service is usually restored in days or at most a couple of weeks – longer outages are extremely unlikely. From drafting plans, to coordinating with our partners, private sector and government alike, to assessing and mitigating risks including building in a multitude of redundancies, we are continuously working to ensure outage times are minimal if and when they do occur.

The electric power industry continuously monitors the bulk electric system and responds to events large and small. Consumers are rarely aware of these events primarily because of the sector's routinely planning, coordinating, and responding to take care of them. In the cases where an event impacts the consumer, these same activities, in addition to the decades of lessons learned from supplying power, have helped ensure there are hazard recovery plans in place for working within the sector and with government counterparts to get the power back on.

Again, defense in depth and system redundancies are helping electric utilities to keep the grid reliable and secure. This will continue to be our first and best defense to any event.

Value in Partnerships & Information Sharing

As mentioned earlier, the ESCC serves a vital role in efforts as a place for the sector to work with government to coordinate policy-level efforts to prevent, prepare for, and respond to, national-level incidents affecting critical infrastructure. The major trade associations and industry work together with government to improve cyber security through the ESCC.

These efforts by industry CEOs from all segments of the electricity sector and their government counterparts include: planning and exercising coordinated responses; ensuring that information about threats is communicated quickly among government and industry stakeholders; and deploying government technologies on utility systems that improve situational awareness of threats.

At the most recent meeting of the ESCC, the government and private sector worked on a number of issues including: transition planning; identifying R&D needs; fostering a better understanding and protection of our mutual dependencies through cross sector engagement including joint exercises and sharing information; a cyber mutual assistance program, and gaining a better understanding of the Fixing America's Surface Transportation (FAST) Act's provisions and implementation.

In addition to pulling industry leadership together with government leadership throughout the year and all of the hard work they do, the ESCC also serves an advisory role with the Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC collects and promptly disseminates threat indicators, analyses and warnings from a variety of private sector and government resources to assist electric sector participants in taking protective action. The information is handled confidentially and distributed through North American Electric Reliability Corporation's (NERC) secure portal directly to industry asset owners and operators.

The E-ISAC also manages the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership co-funded by the Department of Energy (DOE) and industry that seeks to facilitate timely bidirectional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry with near real-time exchange of machine to machine information. This is a great example of efforts to bridge the divides between classified space and sharing actionable, relevant information with private industry.

We appreciate efforts of the new administration in meeting with ESCC leadership recently to work on the transition and ensure our existing partnership and associated initiatives continue to advance without any loss of momentum. We stand ready and intend to continue our work with our government counterparts, across sectors and with each on ensuring a secure, reliable and resilient grid from all-hazards.

It Takes a Toolbox: Additional Tools and Resources

When it comes to cyber security a toolbox with many different tools, resources and options allowing flexibility is necessary – there are no "silver bullets". For the electric sector this includes, but is not limited to: cyber assessments; guidance; tools and resources for small and medium entities; Cyber Mutual Assistance programs; as well as a national industry playbook.

Examples of Cyber Assessments: The industry has decades of experience working together to protect our shared infrastructure and is constantly reevaluating threats and taking steps to protect the system as well as plan for its recovery. Electric cooperatives make protection and security of their consumer-members' assets a high priority. NRECA, their member cooperatives, industry partners and government agencies work closely to develop effective approaches to protecting the electric system. One example is the Cybersecurity Capability Maturity Model (C2M2) a public-private partnership effort that supports the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework by assisting organizations – regardless of size, type or industry – to evaluate, prioritize, and improve their own cyber security capabilities. This tool was customized for electric utilities through the creation of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

Example of Guidance: To further bolster the efforts of ES-C2M2 for electric cooperatives specifically, NRECA's Business and Technology Strategies (BTS) developed a "Guide to Developing a Cyber Security and Risk Mitigation Plan" which includes tools and processes cooperatives (and other utilities) can use today to strengthen their security posture and chart a path of continuous improvement. All co-ops participating in NRECA's Regional Smart Grid Demonstration used these tools to develop a smart grid cyber security plan. The continued engagement on development and improvement to cyber security programs and tools – combined with access to actionable relevant information, both classified and unclassified – is vital when it comes to security postures in critical infrastructures.

Tools and resources for small and medium entities: The DOE's Office of Electricity Delivery and Energy Reliability provided funding to NRECA and the American Public Power Association to implement programs that will help utilities improve their cyber and physical security capabilities. In June 2016, NRECA used this funding to create the Rural Cooperative Cyber Security Capabilities Program (RC3). The RC3 Program is designed to assist cooperatives in developing cyber resiliency and security programs. RC3 funding is primarily focused on assisting small- and mid-sized cooperatives with smaller information technology staff, but all of the products and materials developed in RC3 will be available to help all cooperatives. In addition to developing tools and resources RC3 will provide training and guidance to assist cooperatives in assessing their cyber security risks, enhancing their cyber

security capabilities to prevent and mitigate cyber incidents, and implementing cyber security best practices.

Cyber Mutual Assistance programs: The electric sector, including cooperatives, have a unique and effective approach to emergency management and disaster recovery as they have a lot of experience. Following a disaster, cooperatives will rapidly deploy support staff and equipment to emergency and recovery zones to assist sister cooperatives. To help with this process there are Mutual Assistance Agreements, signed by the vast majority of NRECA member electric cooperatives, which formalize the arrangements that have historically been made informally among cooperatives to help each other when disaster strikes. Cooperatives help each other and other electric utilities as needed. Co-ops often work through their statewide organizations, which helps lead coordination efforts to identify in-state and cross-state needs and resources. This culture of mutual assistance can be found across the industry and is being applied to the implementation of the ESCC's recommendation for the formation of a Cyber Mutual Assistance (CMA) Program, a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies. The CMA program is still young but already has 93 members, including 18 cooperatives, participating. What this means is that in the U.S. there are approximately 118 million electricity customers, approximately 80% of all U.S. electricity customers, who are currently served by utilities that participate in CMA.

ESCC Playbook: Most events impacting electric power supply tend to impact a community or a region – not the bulk power system as a whole. However, planning for response and recovery at a national level for widespread events is necessary in a world where terrorists and nation states have an eye toward harming our critical infrastructure. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry is greatly enhancing our nation's ability to defend, protect against and recover from threats to our systems. The ESCC Playbook provides a framework for senior industry and government executives to coordinate response and recovery efforts and communicating to the American public when such a situation arises. The Playbook has been tested and will be an evergreen document that can be updated by industries when lessons are learned from an exercise or real world experiences.

However, it is important to note, that with a national level event, while our society depends on electricity to function, our electricity systems are reliant on other systems including transportation systems for our fuel, water systems for cooling, and telecommunications for operations. When dealing with national events coordination across all these systems is imperative.

Mandatory and Enforceable Standards

To maintain and improve upon the high level of reliability consumers expect, electric cooperatives work closely with the rest of the electric industry, the NERC, the DHS, the DOE, and the FERC on matters of critical infrastructure protection – including sharing needed information about potential threats and vulnerabilities related to the bulk electric system.

Approximately 60 generation and transmission and 60 distribution cooperatives must comply with some portion of NERC's reliability standards based on the criticality of the bulk electric system assets they own and operate. Since 2007, when NERC standards (reliability and cyber security) become mandatory, electric cooperative representatives have participated in numerous NERC standard development activities and those cooperatives with compliance responsibilities have been working to both comply and to demonstrate compliance through scheduled NERC audits. When covered entities are found to have violated cyber security and/or other NERC standards, they can be subjected to fines as high as one million dollars per day per violation. Sizable fines have been levied when entities have been found in violation and as a utility CEO I can tell you that we take compliance with the NERC standards very seriously.

The NERC standards development process begins with input from industry experts. After approval by industry, the NERC Board of Trustees is asked to approve the standards, which, if approved, are then submitted to FERC for their approval. Upon FERC approval, the standards become mandatory and enforceable. The electric utility industry recently developed standards on physical security and geomagnetic disturbances (GMDs) and continues to revise and develop additional cyber security and GMD standards. NERC also has an "alert system" that provides the electric sector with timely and actionable information when a standard may not be the best method to address a particular event or topic.

How Congress Has Helped

In the last Congress, legislation was passed that assists efforts in securing the grid – thank you.

As mentioned previously, the Fixing America's Surface Transportation (FAST) Act was enacted last year, P.L. 114-94, with a number of helpful provisions including:

- A plan for the Department of Energy to create a plan for a strategic transformer reserve program which assists in all-hazard recovery planning for large scale events;
- Clarification of roles and authorities when there is an imminent threat to the bulk power system as well as identifying DOE as the official lead Sector-Specific Agency (SSA) for cyber security for the energy sector – it was already the SSA for the sector but this was appropriately clarified to include cyber;
- FOIA exemptions for "critical electric infrastructure information" (CEII) submitted by industry to the FERC and other federal agencies.

Also enacted into law in the first half of the 114th Congress was the Consolidated Appropriations Act of 2016, P.L. 114-113, which included long-sought legislation to promote robust, multidirectional voluntary information-sharing about cyber security threats between and among federal agencies and critical infrastructures, including the utility industry.

As the implementation of these new laws is ongoing, it is difficult to demonstrate their importance when it comes to grid security. However, from an industry perspective these were

necessary and important steps forward in clarifying roles, protecting information and planning for all-hazard recovery scenarios – all vital to the reliability of electricity.

How Congress Can Help

An example of where government can improve information sharing with industry is the December 2015 Ukraine event. While the content of the classified and unclassified information from the government was very helpful, the timeliness of getting specific, actionable information to industry must be improved so that we can respond as quickly as possible.

Critical infrastructure owners and operators understand that the biggest threats tend to be those that are hardest to identify – the insider threat. We urge Congress to consider legislation giving the FBI the statutory authority to assist industry with fingerprint-based, criminal and terrorist database background checks for industry-determined personnel that perform critical functions. This would assist industry in further mitigating risks in a way we cannot accomplish at the local and state levels.

Additionally, though we are the only critical infrastructure with mandatory and enforceable standards - developed by NERC, approved by FERC and applicable Canadian governmental authorities - the issue of liability after a cyber event creates serious concerns for the sector. In particular, we are deeply concerned that no matter what steps are taken, our members could face costly and unnecessary litigation in state or federal courts after a cyber event that would serve no purpose. Though the language of the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (the "SAFETY Act") statute, as well as its Final Rule, have always made clear that the protections offered by the law apply to cyber events, in practice there has been some hesitancy on the part of industry to utilize the SAFETY Act to protect against federal claims arising out of cyber attacks due to the requirement that the attack be deemed an "act of terrorism" by the Secretary of Homeland Security before liability protections become available. A legislative clarification that explicitly allows the Secretary of Homeland Security to declare that a "qualifying cyber incident" triggers the liability protections of the SAFETY Act, thereby removing the need to link a cyber attack to an "act of terrorism", would likely go a long way. While state liability actions would remain a concern, the industry and vendors of cyber security technologies and services will be much more likely to use the SAFETY Act program with these clarifications. This would fulfill the law's original intent of promoting the widespread deployment of products and services that can deter, defend against, respond to, mitigate, defeat, or otherwise mitigate a variety of malicious events, including those related to cyber security.

It is important to avoid a one size fits all strategy. For example, security issues relevant for an entity on the bulk electric system may be very different from another entity due to geography, engineering architecture and redundancies among other differences, just as security issues relevant for the bulk electric system are not necessarily equivalent to issues facing the local distribution system. As such, funding streams from the Office of Electricity Delivery and Energy Reliability for programs like NRECA's RC3 to help small and medium cooperatives should be protected.

Conclusion

Thank you for holding today's hearing on this very important issue. I am proud of the efforts of our sector and hope that my testimony helps the Committee to better understand a few of the many activities and collaborative efforts of our industry and our federal government partners. We share your goal of protecting the nation's critical infrastructure from cyber threats and appreciate your efforts to address this important national security issue.

Cooperatives believe building and investing in partnerships will be vital as the industry navigates this dynamic environment. We are implementing a coordinated and collaborative effort across the electricity sector to respond to threats and to vigilantly modify our tactics as needed to keep pace with these threats.

In closing, I thank you again for inviting me to testify today and I look forward to your questions.

The CHAIRMAN. Thank you, Mr. Highley, we greatly appreciate that testimony.

Next we turn to Congressman Dave McCurdy, the President and CEO of the American Gas Association. Welcome, Congressman.

STATEMENT OF HON. DAVE McCURDY, PRESIDENT AND CEO, AMERICAN GAS ASSOCIATION

Mr. MCCURDY. Thank you, Chairman Murkowski, Senator Heinrich and members of the Committee. As the Chairman indicated, I am here as the CEO of the American Gas Association (AGA). I'm also the former Chairman of the House Intelligence Committee and former CEO of the Electronic Industries Alliance. I also served on the board of the Software Engineering Institute and co-founded the Internet Security Alliance in partnership between the electronic industry's alliance and CyLab at Carnegie Mellon University. So, I have to say, I've been engaged in internet policy since before it was called cybersecurity.

AGA represents more than 200 local energy companies that deliver clean natural gas to more than 72 million customers. Natural gas meets more than one-fourth of the United States' energy needs and is the foundation fuel for a clean and secure energy future.

Alongside this opportunity natural gas offers comes serious responsibility to protect pipeline systems from cyberattacks. Technological advances have made natural gas utilities better able to serve our customers; however, there is a recombinant challenge with a more connected industry, as we become a target for increasingly sophisticated cyber adversaries.

Natural gas utilities meet that threat via a commitment to security, skilled personnel, technological advances and partnership with the Federal Government.

I'd like to highlight four critical areas related to pipeline and energy sector cybersecurity.

First, natural gas utilities understand and take very seriously cyberattacks and cyber threats. This drives us to employ the best technology and personnel available to protect our systems and the customers that we serve. This obligation starts at the top. AGA member utility executives assign the AGA commitment to cyber and physical security demonstrating their dedication with a call to action to ensure natural gas pipelines remain resilient to cyber and physical security threats.

Second, energy security interdependence. Recently the electric sector has increased the use of natural gas for power generation. With that comes a greater need for coordination. Natural gas utilities focus on safe and reliable gas delivery and they utilize a variety of assets in contractual plans to secure that reliability. We welcome electric generation customers, but stress the gas/electric interdependency policy should preserve and enhance, not decrease, natural gas system reliability for all customers, both gas and electric. In this regard, the importance of having adequate gas pipeline infrastructure must not be overlooked.

And third, we need to maintain our existing security partnerships. Gas utilities maintain a pipeline security partnership with our statutory partner, the Transportation Security Administration. Industry also works closely with DOE, as we've heard from Ms.

Hoffman and Gerry Cauley. These vital, non-regulatory partnerships are cooperative and support a more effective risk management approach to security. Further, disturbing the continuity of our security partnerships by reshuffling pipeline security authorities will not make us safer. It will simply add uncertainty to the mix.

And last, as we've heard, public/private collaboration is paramount. Industry needs better government cyber threat data delivered in real time, quicker dissemination of classified threat information and a closer working relationship with sector agencies, law enforcement and the intelligence community.

And finally, we should reform how industry leaders receive security clearances, as the Chairman and others have mentioned. For me, this is not a mere talking point. Despite my military, congressional and intelligence experience and currently holding a DoD clearance, I have not received a DOE security clearance, SCI, that I applied for over a year ago to be able to sit in on some of the discussions that we have at the ESCC and other areas, and I am the leader of the Natural Gas Sector for this industry.

America's natural gas delivery system is the safest, most reliable energy delivery system in the world. Security is woven into the natural gas utility culture and our members apply a portfolio of tools to stay ahead of cybersecurity threats. One of our most important tools is partnership with the Federal Government.

Chairman, thank you for the opportunity to testify. I look forward to the exchange of ideas.

[The prepared statement of Mr. McCurdy follows:]

The Honorable Dave McCurdy
President and CEO
American Gas Association

Testimony before the Senate Committee on Energy & Natural Resources "Protecting the U.S Energy Delivery Systems from Cyber Threats"

April 4, 2017

Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee, I am Dave McCurdy, President and CEO of the American Gas Association. Also relevant to this hearing, I am a former Chairman of the House Intelligence Committee and have been heavily involved in computer, software, and internet policy since before it was called "cybersecurity." Also relevant in my background, I served on the Board of the Software Engineering Institute and in 2001 co-founded the Internet Security Alliance, a partnership between the Electronic Industries Alliance and the CyLab at Carnegie Mellon University. Thank you for inviting me to share my perspectives on critical infrastructure cybersecurity.

The American Gas Association, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 72 million residential, commercial and industrial natural gas customers in the U.S., of which 94 percent — over 68 million customers — receive their gas from AGA members. Today, natural gas meets more than one-fourth of the United States' energy needs. Natural gas is the foundation fuel for a clean and secure energy future, providing benefits for the economy, our environment, and our energy security. Alongside the economic and environmental opportunity natural gas offers our country comes great responsibility to protect its distribution pipeline systems from cyberattacks.

Technological advances over the last 20 years have made natural gas utilities more cost-effective, safer, and better able to serve our customers via web-based programs and tools. Unfortunately, the opportunity cost of a more connected and more efficient industry is that we have become an attractive target for increasingly sophisticated cyber terrorists. This said, America's investor-owned natural gas utilities are meeting the threat daily via skilled personnel, robust cybersecurity system protections, an industry commitment to security, and a successful ongoing cybersecurity partnership with the Federal government.

When this hearing is complete, I hope the committee will have a strong understanding of at least four critical realities related to energy sector cybersecurity generally and pipeline transportation security and cybersecurity specifically.

- **Industry Commitment**. Natural gas utilities and our partners across the energy sector – from the CEO level on down – are exceptionally aware of cyberthreats and the potential consequences of a successful cyber attack. This awareness requires us to be vigilant and drives us to employ the best systems and personnel available to protect our business and operating systems, but more importantly, the millions of customers we have a duty to serve.
- **Energy Sector Coordination**. The business model for natural gas utilities is centered around the safe and reliable delivery of natural gas to their customers; therefore, the continued availability of abundant and affordable natural gas supplies, and the safe and reliable transportation of such gas supplies is of primary importance to their businesses and their regulatory obligations to serve. It is thus critically important that policy discussions surrounding gas-electric interdependency/coordination, address the reliability of both the gas and electric systems in a coordinated manner.
- **Maintain Existing Security Partnerships.** Gas utilities maintain a longstanding and effective pipeline transportation security partnership with the Department of Homeland Security (DHS), specifically the Transportation Security Administration (TSA). The industry also works closely with the Department of Energy (DOE) on general energy sector physical and cybersecurity. These non-regulatory security partnerships are built on cooperation, mutual trust, and most importantly the recognition that a top-down cybersecurity regulatory regime would be counterproductive to industry security. Simply put, our adversaries move faster than any regulatory checklist so it's better to partner on protecting our systems than to rely on static compliance programs. Further, reshuffling our government cybersecurity partners will also not make us any safer. Granting DOE additional authority over pipeline transportation systems security virtually guarantees unnecessary program overlap with existing TSA programs. Shifting the entire pipeline transportation security regime from TSA to DOE ignores the pipeline expertise and industry knowledge TSA has built over a decade of partnership, a program that would have to be rebuilt at DOE.
- **Public-Private Collaboration**. The single most important aspect of cybersecurity policy remains effective government-private sector partnership. In order to better protect our systems, industry needs better cybersecurity information from our government partners delivered in real-time; quicker dissemination of classified threat information; and a closer working relationship with not only our sector specific agencies (TSA and DOE), but the law enforcement and intelligence community so we can leverage their unparalleled knowledge and capabilities. Finally, we need to reform the process by which industry leaders receive security clearances. [*A personal point of privilege: Despite my long history of service in the government intelligence space, and despite my existing Department of Defense security clearance, I still have not received a DOE security clearance. I applied well over a year ago.*]

COMMITMENT TO SECURITY

AGA member utility executives have signed onto the *AGA Commitment to Cyber and Physical Security* (Commitment) (see Appendix A), formally demonstrating their dedication to ensuring natural gas pipeline infrastructure remains resilient to the growing and dynamic cyber and physical security threats faced by the industry. The Commitment was developed at the direction of the AGA Board with full CEO support. As outlined in the Commitment, AGA member utilities are dedicated to proactively collaborating with Federal and State governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving their security posture and the industry's longstanding record of providing natural gas service safely, reliably and efficiently across America.

Security awareness is part of the natural gas utility culture and daily practice. The Commitment identifies a consensus by AGA members of actions and accompanying elements that help enhance the resilience of a company's gas operations to security threats. The Commitment further acknowledges that the method and timing of implementing such actions may vary with each operator, taking into consideration individual environments, identified risks, and what has been deemed reasonable and prudent by their state regulators or governing bodies. AGA member utilities recognize the significant role that state regulators or governing bodies play in supporting and funding these actions. As such, effective, performance-based implementation is beyond prescriptive, "check-the-box" compliance.

STRATEGY – REMAIN ON THE OFFENSIVE

Natural gas utilities and pipelines actively engage in cybersecurity risk management. Our primary objectives are to minimize cyber vulnerabilities and increase the natural gas operator's ability to detect malicious cyber traffic, mitigate potential impact, and implement security measures that ensure the safe and reliable delivery of natural gas to customers is not disrupted. Cybersecurity effectiveness in the natural gas industry is maximized by the diversity of protective measures industry-wide that achieve the same overall objectives.

In general, natural gas operators across the industry use the "resiliency in depth" strategy to protect their networks. This strategy begins with corporate cybersecurity governance consisting of policies, standards and guidelines designed to protect critical operations networks, which may include industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA). SCADA consists of software and hardware for system operations and may be applied differently across the industry. Some operators use SCADA only to monitor critical data from sensors, while others use SCADA additionally for system control. Basically, SCADA sends compiled data to a central computer for a human operator to analyze to determine if signals need to be sent out to control field equipment and pipeline conditions. The introduction of SCADA technology to natural gas operations significantly increased natural gas delivery efficiency, reliability, and safety. Industry operators recognize the application of ICS has inherent cyber vulnerabilities, and they identify, evaluate, and manage these risks accordingly. Natural gas utilities and pipelines apply a portfolio of tools, policies, procedures, and practices to manage cybersecurity vulnerabilities and stay ahead of threats. The ultimate objective: Remain on the offensive.

As the Committee knows, there is no single best practice for cybersecurity protections among natural gas utilities, let alone across the energy sector. More to the point, the diversity of operations and SCADA applications across the industry adds to overall sector security because there is no security benefit in identical operating environments. Operators implement security programs and actively engage in voluntary actions to help enhance the security of the nation's 2.5 million miles of natural gas pipeline, which span all 50 states with diverse geographic and operating conditions.

AGA members utilize a number of available security standards, models, guidelines, and information sharing resources (Appendix B), including, but not limited to: (1) National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, (2) Department of Energy *Cybersecurity Capability Maturity Model* (C2M2), (3) Department of Homeland Security *Industrial Control System Computer Emergency Readiness Team* (ICS-CERT), (4) TSA *Pipeline Security Guidelines*, and (5) North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. Cybersecurity cannot effectively be treated as a static threat. As cybersecurity risks and threats change, so do vulnerabilities. As such, ongoing implementation of new tools and capabilities is vital to adapting to the dynamic cyber environment.

In addition, AGA gas utilities and transmission companies participate in the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC), enabling them to share real-time threat intelligence and pertinent information to help them keep their systems secure. Other information sharing entities in which AGA member utilities participate include State Fusion Centers, other ISACs (e.g., Electricity ISAC, Oil & Natural Gas ISAC, Multi-State ISAC, Financial ISAC, Industrial Control System ISAC), and cross-sector information sharing initiatives (e.g., TSA Alerts, USCYBERCOM, DOE Situational Awareness Reports, government intelligence community Joint Analysis Reports, Railway Alert Network, and the Interstate Natural Gas Association of America (INGAA) ThreatConnect program.

Beyond technology, standards, and tools, cybersecurity program effectiveness starts with employee training and awareness of cybersecurity risks and how they may be used by adversaries to gain unauthorized access to networks. Natural gas utilities dedicate substantial resources to reinforcing cybersecurity hygiene awareness at all levels of the corporate structure – from the field employee to the board room. Natural gas utilities also conduct social engineering penetration assessments of their employees to identify those individuals who may require increased cybersecurity awareness training.

FEDERAL & STATE GOVERNMENT ROLES

Pipeline Security Regulatory Authority

The *Aviation & Transportation Security Act of 2001* gave the Department of Homeland Security (DHS) security authority over all modes of transportation, including modes under the purview of the Department of Transportation. Specific to pipeline security, oversight was given to the Transportation Security Administration (TSA), and TSA has been partnering with natural gas

pipelines for over a dozen years. This partnership has been fostered by onsite audits conducted by TSA, conferences jointly sponsored by TSA and industry operators, open communication and exchange of smart practices, and voluntary sharing and analysis of emerging security challenges. Through a multi-year effort and comprehensive forums, TSA developed the *TSA Pipeline Security Guidelines* (Guidelines) in coordination with the pipeline industry. These Guidelines were released in late 2010 (re-released in 2011 to incorporate the National Terrorism Advisory System) and are presently under revision to address lessons-learned and ongoing changes to the cyber threat landscape. The Guidelines have been widely adopted by industry since initial completion in 2009. AGA member gas utilities implement these Guidelines as applicable to their individual environments.

TSA's strategic decision to partner with industry instead of regulate has created a constructive and open relationship with natural gas utility partners that has advanced security beyond a solely compliance mindset. Compliance does not equate to security, and TSA understands this. By working closely with industry for over a decade, TSA has a developed thorough understanding of pipeline operations. Additionally, TSA and the Department of Transportation (DOT) have a Memorandum of Understanding to coordinate pipeline safety and pipeline security, which further enhances TSA's role in coordinating and promoting security throughout the sector.

DHS Cyber Vulnerability Assessment of ONG Value Chain

In February 2013, Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," was issued. Per the requirement in Section 9, DHS conducted cyber vulnerability assessments of all the critical infrastructure sectors, including the Oil and Natural Gas (ONG) sector to identify U.S. cyber-dependent critical infrastructure "where a cyber incident could reasonably result in catastrophic regional or national effects." Based on an evaluation of the threats and the mechanisms in place that enhance ONG resilience, DHS concluded ONG did not belong on the Section 9(a) list.

In conducting the assessments, the ONG sector worked with DHS to identify business functions and associated value chains along the commodity path from well-head to end-user. Functions with a cyber-component, regardless of housing on the enterprise network or the operating network, were identified and a series of cyber-provoked scenarios were discussed along with how consequences would measure up to the criteria proposed by DHS.

From a cyber design perspective, natural gas functions are divided across an enterprise network (which handles emails, billing, invoices and basic corporate data and information) and an operations network (which includes control system, SCADA, and pipeline monitoring). These two networks are isolated from each other, employ firewalls and layer other tools and mechanisms to improve the prevention, detection and mitigation of cyber penetration. Further, the inherent design of high pressure and low pressure gas delivery systems is mechanical by nature. Modern infrastructure has control systems to help operate and monitor pipelines and pipeline components to move the product in a reliable, efficient and effective manner. Operators manage the internal pressure of the delivery system by controlling the amount of natural gas entering and leaving the system. The process of increasing or decreasing pressure happens

relatively slowly in a natural gas system because of the compressible nature of the gas. This compressibility lessens the immediacy of a potential cyber attack's impact and increases the probability of detection. Layered onto this control system architecture are mechanical overpressure protection devices, which serve as a safeguard to prevent internal gas pressure from threatening a pipeline's integrity. Pipeline safety regulations and standards require that back-up systems CANNOT be affected by the same incident that compromises the primary control system; thus, fail-safes and redundancies must be independent of the cause of the primary mechanism's failure.

Sector Specific Agencies

The Homeland Security Presidential Directive 7 (HSPD-7) of 2003 identified critical infrastructure sectors and Federal government agencies/offices to serve as Sector Specific Agencies (SSAs) responsible for implementing the National Infrastructure Protection Plan framework and guidance as tailored to the specific characteristics and risk landscapes of each sector to which the SSA is assigned. Natural gas utilities and pipelines fall under the purview of at least two SSAs, i.e., DHS TSA[1] as the SSA for pipelines (identified as a mode of transportation) and DOE as the SSA for energy. The DHS Office of Infrastructure Protection may be an additional SSA depending upon the business functions of the company.
In its role as the SSA for the Energy Sector, DOE has worked closely with government and industry partners to develop cybersecurity practices, tools, and guidelines that address relevant cybersecurity risks and threats. Much of this work has been and continues to be done in collaboration with the two Energy Subsector Coordinating Councils (SCCs) and the Energy Government Coordinating Council (GCC). The Electricity SCC and the Oil & Natural Gas SCC (ONG SCC) comprise the Energy SCCs and represent the interests of their respective industries. The Energy GCC represents government at various levels – Federal, State, local, territorial, and tribal. Through the partnership created under the NIPP framework, SCC and GCC partners work together towards the ultimate end-goal of protecting and securing the American energy system.

Other Federal government entities with pipeline cybersecurity interests and with which natural gas utilities and pipelines coordinate include the DHS Infrastructure Security Compliance Division, United States Coast Guard, and the Federal Energy Regulatory Commission. Additionally, natural gas utilities and intrastate pipelines are subject to State government actions.

PROACTIVE INITIATIVES

Natural gas utility security challenges, like the threat environment in which they operate, are constantly changing. To address these challenges and to predict future challenges, AGA and its member utilities have an array of strategically planned initiatives to educate, coordinate, and motivate industry resilience. Leading challenges include sector interdependencies, supply chain integrity, Internet of Things, and the convergence of physical and cybersecurity. Initiatives

[1] The Department of Transportation and DHS are directed by HSPD7 to collaborate on all matters relating to transportation security and transportation infrastructure protection.

include partnering within the Energy Sector, with other interdependent sectors, and with government partners. Programs already referenced include development of the DNG ISAC and the *Commitment to Cyber & Physical Security*. Additional initiatives include active engagement with the revisions to the *TSA Pipeline Security Guidelines* and to the *NIST Cybersecurity Framework*, Downstream Energy Coordination, educational activities with State regulators, assistance with industry-wide implementation of the DOE ONG C2M2, identification of leading cybersecurity threats to natural gas utilities, topical workshops, cybersecurity tabletop exercises, and senior executive engagement. Details for each follow.

- **AGA Commitment to Cyber and Physical Security:** The *AGA Commitment to Cyber and Physical Security* (Commitment), which was approved by the AGA Board in October, 2016, outlines industry's continued commitment to improving security through voluntary actions and closely aligns with the *TSA Pipeline Security Guidelines (2011)* and the *NIST Cybersecurity Framework (2014)*. The Commitment demonstrates to interested stakeholders that industry is voluntarily taking actions to identify, protect, detect, respond, and recover from a physical or cybersecurity attack. At the direction of the AGA Board, AGA has moved forward with collecting letters of commitment from AGA member company executives. AGA has been commended by DHS, DOE, TSA, and DOT for this effort.
- **Downstream Natural Gas Information & Analysis Center (DNG ISAC):** The DNG-ISAC supports natural gas operators with cyber and physical security alerts of greatest relevance to natural gas operations. Participation includes AGA member gas utilities, the Canadian Gas Association, and the Interstate Natural Gas Association of America. This provides all natural gas distribution and transmission companies in the U.S. and Canada unfettered access to real time actionable information, security alerts, and analysis to enable them to better secure their cyber and physical assets.
- **Updating 2011 Transportation Security Administration (TSA) Pipeline Security Guidelines.** The *2011 TSA Pipeline Security Guidelines* (Guidelines) is a collaboration of TSA, pipeline operators (including AGA), and other government entities with an interest in pipeline security. It has been five years since the release of the Guidelines, and TSA and stakeholders are once again partnering to review and ensure the Guidelines are up to date and an effective pipeline operator security resource.
- **NIST Cybersecurity Framework.** Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," directed the National Institute of Standards & Technology (NIST) to develop a cybersecurity framework applicable to all 16 critical infrastructure sectors. Natural gas utilities and pipelines committed to the collaborative development of this framework. Released in February 2014, the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) is essentially a maturity model intended for voluntary adoption by critical infrastructure owner/operators. Additionally, DOE and industry partners (including ONG) collaborated to develop the *Energy Sector Cybersecurity Framework Implementation Guidance*, which relies on existing sector-specific standards, tools, and processes to help industry characterize, enhance, and communicate their cybersecurity posture using the NIST Cybersecurity Framework. TSA collaborated similarly with sector partners (including pipelines) to develop the *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*. In January, 2017 NIST released

an updated Cybersecurity Framework and pipelines are once again engaged to ensure the revisions build upon the current wide-spread acceptance and adoption of the Cybersecurity Framework.

- **Downstream Energy Coordination.** AGA leads the downstream energy coordination initiative on behalf of the ONG SCC in partnership with the ESCC. Oversight is provided by a prominent gas/electric utility CEO. This initiative focuses on the interdependency of natural gas and electric utilities to plan for and respond to major incidents, better understand and protect mutual dependencies, share information, and improve cross-sector situational awareness. This coordination has led to opportunities for cross-subsector education and information exchange to the benefit of government and industry stakeholders.
- **Activity with States.** Recognizing the significant role state regulators or governing bodies play in supporting and funding of cybersecurity actions of natural gas utilities, industry operators are engaging with State-level leadership. The National Association of Regulatory Utility Commissions (NARUC) developed a reference guide, "Cybersecurity for State Regulators," a primer that explains cybersecurity basics and includes questions State regulators and utilities may use to engage in partnerships. AGA encourages gas utilities to use this primer to reach out to State regulators.
- **Regional Cybersecurity Assessment Workshop.** AGA is in its third year of sponsoring regional cybersecurity assessment workshops with the objective of assisting member companies with evaluating the maturity of their cybersecurity programs through facilitated application of the DOE ONG Cybersecurity Capability Maturity Model (ONG C2M2). Participating companies leave the workshop with an assessment of their overall corporate cybersecurity capabilities and identified areas for further consideration and planning.
- **Cyber Threat Analysis Guidance.** The AGA Cyber Threat Analysis initiative identified leading cybersecurity threats to natural gas utilities; developed a resource tool detailing each threat, associated threat vectors, consequences, threat elements, and mitigation measures; and culminated in a workshop that brought together cyber and operations professionals representing three dozen natural gas companies to discuss the potential impact of these threats on their companies' operations infrastructure.
- **Topical Workshops & Tabletop Exercises.** AGA continues to present timely, well-attended topical workshops on areas of interest and opportunity for advancing natural gas utility cybersecurity programs. Recent workshops include *Cyber Risk Taxonomy*, *ONG C2M2 Lessons Learned*, *Shodan & Metasploit Overview*, and *Insider Threat*. AGA also hosts multi-dimensional tabletop exercises that touch on a variety of business functions upon which natural gas operations rely, including gas control, operations, telecommunications, cyber, physical security, and electricity. The last exercise scenario was developed with input from DHS ICS-CERT and the DOE Idaho National Laboratory.
- **Senior Executive Engagement.** Biennially, AGA presents the *Energy Delivery Cybersecurity Executive Summit* bringing together leading executives from across the Nation with a stake in natural gas energy delivery, including electric, oil, telecommunications, and finance. The objective of the Summit is to engage government and private sector leaders to discuss cyber interdependencies, increase awareness of shared

vulnerabilities, and continue our commitment to effective, coordinated strategies. The 2017 event will be co-sponsored by the Canadian Gas Association and held in conjunction with *NERC GridEx IV* to maximize cross-border and cross-sector coordination.

NATURAL GAS & ELECTRIC POWER GENERATION INTERDEPENDENCY

The growing interdependencies between the natural gas and electricity subsectors are well-recognized. The increased use of natural gas for power generation is due to many factors, including – environmental regulations, abundant and affordable fuel, and significant increase in domestic production. This interdependency has effectively expanded the customer base of our nation's natural gas delivery portfolio that has required a new level of physical, operational, legal, and regulatory understanding between the two industries. The natural gas and electric industries have been working together to increase the understanding of each other and to address challenges by increasing coordination and communication regarding understanding the natural gas value chain, natural gas contractual obligations, physical natural gas system operations and limitations, natural gas limiting regulations, natural gas emergency service priority requirements,[2] and the need to coordinate cybersecurity resiliency efforts.

America's natural gas production, transmission, storage, and distribution systems support the most flexible and resilient natural gas market in the world. The U.S. pipeline and storage network is highly reliable, the result of accessible production from virtually all major North American gas producing regions and delivery via an integrated pipeline transportation network. The business model for natural gas utilities is centered around the safe and reliable delivery of natural gas to their direct-use customers.[3] Therefore, the continued availability of abundant and affordable natural gas supplies, and the safe and reliable transportation of such gas supplies is of primary importance to their businesses and their regulatory obligations to serve. It is thus critically important that discussions surrounding gas-electric interdependency, as well as our national policy, address the reliability and resiliency of both the gas and electric systems, while recognizing the differences between the industries.

Reliability of natural gas service and system resiliency is a priority for both the natural gas and electric industries. This is particularly important for natural gas utilities because they have state regulatory mandates or obligations to serve firm, or core, customers (generally residential and small commercial) which requires them to reliably meet the natural gas supply needs of these customers at just and reasonable rates, terms and conditions of service. To fulfill this public service obligation, gas utilities develop comprehensive plans and manage assets, operations and contractual portfolios that include physical natural gas supply arrangements, natural gas transportation, and natural gas storage. Natural gas utilities plan their supply portfolios and build their system deliverability to ensure reliable service to these firm customers and others on a

[2] For gas-fired generators located on natural gas utility systems, it is important to note that gas curtailment priorities are state-specific determinations. For gas-fired generators served directly off an interstate pipeline, there are interstate pipeline tariff provisions that set forth transportation service priorities.

[3] Not discussed in depth here, natural gas pipelines also are subject to pipeline safety regulations, which address the resilience and reliability of the pipeline infrastructure.

"design day" (or a forecasted peak day load based on historical weather conditions). The methodologies for design day determination vary among gas utilities, but are based typically upon the principle of maintaining service to these firm customers on the coldest days of winter.

Through this planning, natural gas utilities build systems and enter into contractual arrangements seeking to ensure continuous gas service operations throughout each year. Planning includes contingencies to address physical operational service disruptions in various scenarios, as well as other circumstances, such as extreme weather events and planning system resiliency against cyber threats – all of which may impact or disrupt natural gas service. An important component for gas service reliability regards the planning and development of needed infrastructure. Adequate and reliable infrastructure is a critical component of a healthy and liquid natural gas market. As more power generation moves to the use of natural gas for fuel, certain regions of the country, particularly the Northeast, will need additional infrastructure to serve this new load. But each region of the country has a unique energy portfolio, and the timing of infrastructure development will be regionally-dependent.

Natural gas utilities also provide reliability by contracting at the highest level of service reliability offered by the pipeline – generally at a firm service level. While unusually severe weather events have the potential to disrupt the natural gas system, the loss of pipeline transportation and storage services that are contracted for on a firm basis have been rare. During periods of high usage and system constraints, prevalent on the coldest winter days, natural gas systems may call upon customers that have contracted for lower priority services, such as interruptible service, to decrease or cease gas usage temporarily, upon which these customers generally have planned to switch to a back-up fuel, such as fuel oil. The tradeoff for these customers is a discounted rate for the natural gas delivery service, compared with firm service rates, and parties enter into these contractual arrangements with prior knowledge. To ensure reliability in periods of extreme weather constraints and other events, natural gas utilities routinely plan and contract for firm contracting levels for both natural gas commodity supplies as well as the transportation of such supplies on gas pipeline systems. Thus, if natural gas-fired power generators have decided to contract for interruptible transportation service on gas pipeline systems, they may find that interruptible transportation capacity is unavailable during severe weather or other outage events because the available pipeline capacity is being used by higher priority firm transportation service customers. In some circumstances, in order to provide additional firm services to customers, gas system operators may need to develop and construct additional infrastructure.

During coordination efforts to address the needs of the gas and electric industries, it has been emphasized that many gas services are offered and/or can be designed to help meet the needs of gas-fired generators. In seeking natural gas service reliability for their own circumstances, gas-fired power generators can learn from the natural gas utility planning and contracting model to assess their needs and pursue firm services as well as new or different services on gas pipeline systems that may not be currently available. In some cases, the provision of such services may require an appropriate expansion of natural gas infrastructure to meet the needs of gas-fired generation. However, AGA stresses that it is important that such gas services preserve reliability for all of the customers on the gas system and are aligned with the market

incentives for gas-fired generators to enter into contracts for those services, when needed, without the creation of cross-subsidies.

In considering the broad issues of how to achieve greater coordination between the natural gas and electricity markets, AGA believes that policies should be guided by the following principles:

- The overall goal of gas-electric coordination policies should be to preserve and, where appropriate, enhance reliability for all customers, both gas and electric:
- Gas and electric stakeholders must collaborate to meet this overall objective;
- Policymakers and industry leaders should ensure the policies they pursue address the reliability of both gas and electric systems in a coordinated manner, not one at the expense of the other;
- National policy cannot be made in isolation; there are a number of different considerations – including energy, environment, economics, national security and consumer interests;
- Policies should reflect variations in reliability issues at the regional level in terms of infrastructure, scope and timing. Priority should be given to those regions where the need is most urgent; and
- Policy initiatives should recognize ongoing regional efforts to address reliability issues, draw on stakeholders' existing knowledge of regional operations and promote continued collaboration among all stakeholders on a regional basis.

IN SUMMARY

America's natural gas delivery system is the safest, most reliable energy delivery system in the world. Industry operators recognize the application of industrial control systems has inherent cyber vulnerabilities, and they identify, evaluate, and manage these risks accordingly. Security awareness is woven into the natural gas utility culture, and natural gas utilities and pipelines apply a portfolio of tools, policies, procedures, and practices to manage cybersecurity vulnerabilities and stay ahead of threats. Of these, the most important cybersecurity mechanism is the existing cybersecurity partnership between the Federal government and industry operators.

TSA, the regulator for pipeline security, has been partnering with the industry for over a dozen years. TSA's strategic decision to partner instead of regulate has created a constructive and open relationship with natural gas utility partners that has advanced security beyond a solely compliance mindset. Further, pipelines are subject to DOT pipeline safety regulations, which are intended to address the resilience and reliability of the pipeline infrastructure. Natural gas utilities' risk management takes into consideration upstream feeds, downstream customers, contractual agreements, and State service priority plans.

Building on the partnership model, natural gas utilities and pipelines work closely with its leading SSAs, i.e., TSA and DOE. In its role as the SSA for the Energy Sector, DOE actively engages with government and industry partners to develop cybersecurity practices, tools, and guidelines

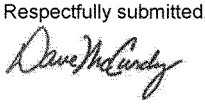
that address relevant cybersecurity risks and threats. The partnership with DOE continues to be effective in identifying and solving constantly changing pipeline security challenges.

Additionally, AGA and its member utilities have an array of strategically planned initiatives to educate, coordinate, and motivate industry resilience through partnerships within the Energy Sector, with other sectors, and with government partners. This is particularly important given the growing interdependencies between the natural gas and electric industries, which has effectively expanded the customer base of our nation's natural gas delivery portfolio but not without accompanying challenges. The natural gas and electric industries have been working together to address such challenges, and more remains to be done. Given that the business model for natural gas utilities is centered around the safe and reliable delivery of natural gas to their customers, it is critically important that discussions that surround gas-electric interdependency/coordination as well as our national policy address the reliability of **both** the gas and electric systems in a holistic coordinated manner for the benefit of the energy consumer and our nation's economy.

Attached to this testimony are following additional supplemental materials:
1. AGA's Commitment to Cyber and Physical Security
2. Natural Gas Cybersecurity and Standards Portfolio

Thank you for the opportunity to provide this additional testimony for the record.

Respectfully submitted,



President and CEO
American Gas Association

AGA's Commitment to Cyber and Physical Security

AGA and its members are dedicated to help ensure that natural gas pipeline infrastructure remains resilient to growing and dynamic cyber and physical security threats. We are committed to proactively collaborating with federal and state governments, public officials, law enforcement, emergency responders, research consortiums, and the public to continue improving our security posture and the industry's longstanding record of providing natural gas service safely, reliably and efficiently across America.

AGA and its operators implement security programs and actively engage in voluntary actions to help enhance the security of the nation's 2.5 million miles of natural gas pipeline, which span all 50 states with diverse geographic and operating conditions. The Department of Homeland Security Transportation Security Administration (TSA) has oversight for security of pipelines (including natural gas distribution and transmission), and as such, has developed the *TSA Pipeline Security Guidelines*. AGA member gas utilities and transmission companies are implementing these guidelines as applicable to their individual environments. Additionally, AGA members are utilizing a number of available security standards, models, guidelines, and information sharing resources, including, but not limited to: (1) National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, (2) Department of Energy Cybersecurity Capability Maturity Model (C2M2), (3) Department of Homeland Security Industrial Control System Computer Emergency Readiness Team (ICS-CERT), (4) TSA Pipeline Security Smart Practices Observations, and (5) TSA Intermodal Security Training Exercise Program (I-STEP). In addition, AGA gas utilities and transmission companies will be part of the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC) by 2017.

Below are voluntary security actions that are being taken by AGA or individual operators to help ensure the secure operation of natural gas pipeline infrastructure. AGA and its operators recognize the significant role state regulators or governing bodies play in supporting and funding these actions. It is the consensus of AGA members that the actions and accompanying elements listed below enhance the resilience of a company's gas operations to security threats. However, the method and timing of implementation of these actions will vary with each operator. Each operator evaluates, and implements as appropriate, these actions taking into account individual environments, identified risks, and what has been deemed reasonable and prudent by their state regulators or governing bodies.

IDENTIFY

1. Establish ownership, sponsorship, organizational roles and responsibilities for corporate security programs
2. Conduct criticality assessments to identify critical facilities
3. Identify critical cyber assets
4. Define security roles, responsibilities, and lines of communication
5. Intelligence gathering and information sharing

PROTECT

1. Review security plans and procedures
2. Implement access controls
3. Implement personnel training and awareness program(s)
4. Develop & implement maintenance program(s)
5. Incorporate security into system designs
6. Establish cybersecurity controls for procuring systems and services

DETECT

1. Implement intrusion detection and monitoring
2. Perform background investigations
3. Conduct periodic vulnerability assessments
4. Establish procedures for receiving and handling threat intelligence to improve detection capabilities

RESPOND/RECOVER

1. Develop communication procedures for security events
2. Conduct periodic drills and exercises
3. Plan and prepare for the restoration of systems, facilities, and assets
4. Establish redundancies for resilience
5. Establish procedures for responding to threat information and actual events

NATURAL GAS CYBERSECURITY GUIDELINES & STANDARDS PORTFOLIO

Gas utilities and transmission operators apply a myriad of cybersecurity standards, guidelines, and regulatory practices, and tools developed by industry and government entities in their cybersecurity portfolio, as applicable to their individual security environments. These include, but are not limited to:

- American Chemistry Council, *Guidance for Addressing Cyber Security in the Chemical Industry*
- *AGA Commitment to Cyber and Physical Security* (2016)
- *AGA Cybersecurity Procurement Language Tool*
- *AGA Report 12 – Part I, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan*
- AGA and Interstate Natural Gas Association of America (INGAA), *Security Practices Guidelines Natural Gas Industry Transmission and Distribution*, (2008)
- American National Standards Institute (ANSI)/International Society of Automation (ISA)-95.00.01-CDV3, *Enterprise-Control System Integration Part 1: Models and Terminology*, (2008)
- ANSI/ISA0-99.00.01-2007, *Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models*, (2007)
- ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- American Petroleum Institute (API) & National Petrochemical & Refiners Association (NPRA), *Security Vulnerability Assessment Methodology for the Petroleum & Petrochemical Industries*
- API, *Security Guidelines for the Petroleum Industry*, (2005)
- API, *Standard for Third Party Network Connectivity*, (2007)
- API Standard 1164, *Pipeline SCADA Security*, (2009)
- Center for Internet Security *Critical Security Controls (formerly SANS Top 20 Critical Security Controls)*
- Department of Energy (DOE) ONG Cybersecurity Capability Maturity Model (ONG C2M2)
- DOE *Energy Sector Cybersecurity Framework Implementation Guidance*, (2015)
- DOE Office of Cyber Security, Computer Incident Advisory Capability
- DOE, *21 Steps to Improve Cyber Security of SCADA Networks*
- *DOE Cybersecurity Procurement Language for Energy Delivery Systems*, (2014)
- DHS Control Systems Security Program, *Cyber Security Evaluation Tool* (CSET)
- DHS Chemical Facility Antiterrorism Standards, (2007)
- DHS, *National Infrastructure Protection Plan*, (2013)
- DHS, National Cyber Security Division (NCSD), *Catalog of Control Systems Security: Recommendations for Standards Developers*, (2010)
- DHS NCSD, *Cyber Security Procurement Language for Control Systems Security*, (2009)
- DHS Transportation Security Administration (TSA), *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*, (2016)
- *DHS Cybersecurity Questions for CEOs*
- DHS Industrial Control Systems Cyber Emergency Response Team Recommended Practices
- International Organization for Standardization (ISO) and International Electrochemical Commission (IEC), *17799/27001/27002, Information technology - Security techniques - Code of Practice for Information Security Management*
- INGAA, *Control System Cyber Security Guidelines for the Natural Gas Pipeline Industry*, (2011)
- National Association of Regulatory Commissioners Primer, *Cybersecurity for State Regulators* (2017)
- National Institute of Standards and Technology (NIST) SP 800 series
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-82, *Guide to Industrial Control Systems*
- NIST *Framework for Improving Critical Infrastructure Cybersecurity*, (2014)
- North American Electric Reliability Corporation (NERC), NERC-CIP Standards
- TSA *Pipeline Security Guidelines*, (2011)

The CHAIRMAN. Thank you, Congressman McCurdy.

Next, we turn to Mr. Andrew Bochman, who is with us today from Idaho National Labs.

Thank you.

STATEMENT OF ANDREW A. BOCHMAN, SENIOR CYBER AND ENERGY SECURITY STRATEGIST, IDAHO NATIONAL LABORATORY

Mr. BOCHMAN. Good morning, Chairman Murkowski, Ranking Member Heinrich, or depending upon her proximity, Cantwell, and distinguished members of the Committee, I thank you for holding this hearing and inviting Idaho National Laboratory's, or INL's, testimony on the protection of our energy delivery systems.

I am INL's Senior Cyber and Energy Security Strategist. In this capacity, I provide guidance to DOE, and INL leadership on matters related to protecting national energy infrastructure against mounting cyber and physical threats. I am here today to share impressions on the state of cybersecurity in the energy sector and provide an update on DOE and national lab actions.

I just returned from a USAID-funded trip to Estonia where I joined a team of U.S. state-level energy regulators, led by the National Association of Regulatory Utility Commissioners, or NARUC. We provided cyber training to Black Sea energy regulators, including commissioners from Ukraine, target of two outage-causing cyberattacks.

The possibility of similar attacks or worse on U.S. energy infrastructure has been much on the minds of DOE, INL and some of your colleagues, including Senator King and co-sponsors Risch, Heinrich, Collins and Crapo. Last year they drafted the Securing Energy Infrastructure Act, and just last month, Senators Cantwell and Wyden wrote a letter to President Trump urging him to maintain, as 2015's FAST Act codified, DOE primacy over grid security matters.

Concern for such an attack on U.S. energy infrastructure is well warranted. I pause at five reasons. Number one, the aforementioned successful attacks on foreign transmission and distribution energy infrastructures. Two, the now daily drumbeats of damaging cyberattacks on U.S. Government and private sector systems. Three, profound shortage of skilled industrial control system security professionals. Number four, manufacturer's zeal to embed new technologies in industrial systems and our eagerness for sound business reasons to buy and install these products in energy infrastructure. And lastly, five, while we make incremental improvements on defense, our attack surface and the attacker's ability to exploit it, are expanding at a much, much faster pace.

Cyber risk futurists, myself included, are experiencing a palpable sense of foreboding that our nation's current security activities will not yield the transformational changes that we need; however, some significant improvements are in the offing. DOE's Office of Electricity Delivery and Energy Reliability, or OE, INL and our peer national laboratories are working via multiple policy and programmatic pathways to make a difference. Here are six, high impact examples.

Number one, DOE's Cyber Threat Intelligence and Information Sharing Program, you've heard it referenced previously, CRISP, is currently in place at dozens of large U.S. utilities and efforts are underway to substantially improve both the timeliness and the helpfulness of the security warnings they receive.

Two, INL and industry partners are on the homestretch of a threat-informed, engineering-centric assessment and mitigation activity at a large U.S. utility. We call this approach, Consequence-driven, Cyber-informed Engineering, or CCE. It clarifies and prioritizes the way we look at high consequence risks within control systems environments.

Methodology lessons harvested from this pilot will be shared with other partners to expand the nation's ability. And I'd like you to remember this phrase, "to engineer out the cyber risk from our most critical energy infrastructures."

Number three, INL assists DOE with initiatives to make grid systems more resilient against geo-magnetic disturbance and electromagnetic pulse events.

Four, with the substantial expansion of the industrial control system security workforce as a goal, INL and its partners, Pacific Northwest National Lab (PNNL) and Sandia, U.S. universities and commercial training partners are teaming to create curricula to make this happen as quickly as possible.

Five, OE's Infrastructure Security and Energy Restoration Organization, ISER, is the seat of the Department's sector specific agency authority. INL and PNNL are supporting the build out of ISER's cyber incident response and coordination capabilities in conjunction with DHS, NERC's Electricity Information Sharing and Analysis Center and other grid security stakeholder organizations.

And lastly, per the 2013 Executive Order on improving critical infrastructure cybersecurity, INL supports ISER as it convenes the energy sector's Section Nine energy companies. Among several capabilities requested so far, is a multi-lab environment where energy sector systems can be analyzed from a threat informed cybersecurity vantage point with specific mitigation actions shared securely among the lab's equipment suppliers and asset owners and operators as well.

I'll leave off there.

Thank you very much for inviting me to testify today. And I look forward to your questions.

[The prepared statement of Mr. Bochman follows:]

STATEMENT OF

MR. ANDREW A. BOCHMAN, SENIOR CYBER AND ENERGY STRATEGIST
NATIONAL & HOMELAND SECURITY

IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON ENERGY AND NATURAL RESOURCES

APRIL 4, 2017

Mr. Andrew A. Bochman, Senior Cyber and Energy Strategist, Idaho National Laboratory National and Homeland Security Division

U.S. Senate Hearing to receive testimony on examining efforts to protect U.S. energy delivery systems from cybersecurity threats

Chairman Murkowski, Ranking Member Cantwell, and distinguished members of the Committee, thank you for holding this hearing and inviting Idaho National Laboratory's testimony on the protection of our energy delivery systems. This topic is highly relevant, and your attention to this issue will have a long-term impact on our energy, economic, and national security. I am the Senior Cyber and Energy Security Strategist at Idaho National Laboratory, also known as INL, and in this capacity I provide guidance to the Department of Energy (DOE) and laboratory leadership on matters related to protecting the nation's energy infrastructure against mounting cyber and physical threats. These threats include both the current threats of which the nation is aware, and future threats that we envision and anticipate. I am honored to participate and request that my written testimony be made part of the record.

As one of DOE's national laboratories, INL is missioned to be a leader in technology research, development, demonstration, and deployment for critical infrastructure protection. As such, INL is at the forefront of U.S. and international control systems cybersecurity and grid resilience research. The laboratory also supports DOE in developing and implementing initiatives to research, develop, and test new methodologies and technologies to increase the reliability and protection of energy infrastructure. These initiatives are essential as industry evolves to the Smart Grid; add new energy sources, storage, and consumers; and encounter potentially high consequence impacts from the effects of Geomagnetic Disturbance (GMD), Electromagnetic Pulse (EMP), and other natural and man-made phenomena.

I just returned from a trip to Estonia, sponsored by the United States Agency for International Development, where I joined a team of U.S. state-level energy regulators, led by the National Association of Regional Utility Commissioners (NARUC). This team provided training for Baltic & Black Sea energy commissioners on cybersecurity issues. As you may know, Estonia is one of the first countries to suffer a large scale cyberattack against its critical government and commercial infrastructures. Estonia is located within a region where several other countries were victims of cyberattacks on critical infrastructure. Recently, INL provided experts on the U.S. delegation that assessed the cyberattack on the Ukraine power grid. As a result, INL assisted the SANS Institute with issuing a summary report on the attack and subsequent recommendations for further protections.

The possibility of attacks like these or worse have been the focus of DOE, INL, and some of your colleagues. Senators Cantwell and Wyden, who in a March 14 letter to President Donald Trump, urged the President to maintain, as codified in the Fixing America's Surface

Transportation Act (Public Law 114-94), DOE's primacy over grid security matters. And earlier, heightened concerns over cyberattacks on energy systems motivated Senators King and co-sponsors Senators Risch, Heinrich, Collins and Crapo to draft S. 79, the Securing Energy Infrastructure Act.

The average person may wonder: "Why all this activity now?" I would state that it is being driven by what has happened in the past, and the daily reports of successful cyberattacks on U.S. government and private sector systems. Also, and in particular it is about what cybersecurity experts see looming in the future. In the interest of efficiency and reliability, manufacturers and utilities exhibit a zeal to embed automation and autonomy technologies in industrial products, a trend which goes by the name Industrial Internet of Things (IIoT), and an eagerness to install these products in energy infrastructure. This means that, despite the cybersecurity community's best reactive efforts, attackers are going to penetrate energy systems, and utilize the complexities of "bolt on" cybersecurity measures to develop more attack path options than ever before. Cyber risk futurists, myself included, are experiencing a palpable sense of foreboding, never more so than when I study the current state of cyber measure/countermeasure activities.

Even while acknowledging all of this contextual background, I can assure you that in my role with DOE, I daily gain confidence in our capability and capacity to overcome this condition and resolve significant energy infrastructure cybersecurity challenges. DOE, INL and our peer national laboratories are working these challenges via multiple strategy, policy and programmatic pathways. Though not exhaustive, I will describe a few of the relevant and impactful examples in which INL is serving DOE as a strategic and technical leader in the protection of the nation's energy infrastructure:

- DOE's Office of Electricity Delivery and Energy Reliability (DOE-OE) cyber threat intelligence and information sharing program, Cybersecurity Risk Information Sharing Program (CRISP) is currently in place at dozens of U.S. utilities. INL is a part of the efforts to substantially improve both the timeliness and effectiveness of the security warnings utilities receive. Also, the DOE-supported California Energy Systems for the 21st Century (CES-21) program's Machine-to-Machine Automated Threat Response (MMATR) project has strong potential to accelerate alerts for specific categories of threat information to near-real time.

- DOE-OE is investing over $15M in improved power grid testing capability to provide modern, more robust research on technologies intended to protect substations and power transmission systems from both physical and cyber threats. Industry also is investing in this capability by adding equipment for further research as part of CES-21, and the DOE Grid Modernization Laboratory Consortium (GMLC) and Cybersecurity for Energy Delivery Systems (CEDS) programs. These investments enable cooperative cybersecurity research with universities and industry. Recent examples include cyber vulnerability discovery research with the University of Louisiana Lafayette on an electric vehicle charging station and development of cyber protection devices with auto

manufacturers.

- The DOE Office of Nuclear Energy (DOE-NE) initiated research projects focused on nuclear energy cybersecurity. These projects conduct research that is producing the scientific data which will be used as the basis for future cost effective cybersecurity technologies and practices. These projects will enhance cybersecurity within our current and future nuclear power plant fleet, research reactors, future reactor designs, and nuclear fuel cycle facilities. These collaborative research projects include INL, three other national laboratories (Sandia National Laboratories, Pacific Northwest National Laboratory, and Brookhaven National Laboratory), the Electric Power Research Institute (EPRI), and several universities (including competitive awards granted at North Carolina State University, the Ohio State University, and Tulsa University). DOE-NE also has awarded three Phase I and one Phase II nuclear-cybersecurity grants within the DOE Small Business Innovative Research Program.

- In the spirit of Senator King's Securing Energy Infrastructure Act, INL and industry partners are near completion with a threat-informed, engineering-centric assessment and mitigation activity at a very large U.S. utility. The lab calls this approach Consequence-driven Cyber-informed Engineering (CCE). The methodology reprioritizes the way the nation views high-consequence risks within control system environments. Lessons harvested from this initial pilot will be shared with research partners to greatly expand the nation's ability to "engineer out the cyber risk" from our most critical energy infrastructure networks and systems. Further reduction of risk can be achieved with government, research and industry working toward a common goal complemented by investments in over-the-horizon research and development.

- INL supports the North American Electric Reliability Corporation and its biennial multi-sector North American Grid security exercise, GridEx. The lab provides extremely realistic "inject" artifacts that show energy systems operating incorrectly due to cyberattacks. INL experts routinely participate in many other national exercises, including the recent Cascadia Rising.

- Recent INL investments include more than $5M over the last two years in cybersecurity equipment, laboratories, and research related to energy security issues. Research topics address a wide range of energy-cyber relevant topics, such as: vehicle cybersecurity for battery charging; vehicle command and control communication protocols; vehicle-to-vehicle automation communications; threat actor analyses; grid cybersecurity; geomagnetic disturbance (GMD) and electromagnetic pulse (EMP) threats; infrastructure interdependency analyses; futuristic cyber-resilient systems and architectures; cyber reverse engineering; and cyber forensic tools. Aligned with these internal investments, the State of Idaho recently approved up to $90M for two new research facilities on the INL campus. One of those facilities, the Cybercore Integration Center, will support INL and Idaho universities' cyber and information sciences research, education and training

for DOE, other government, universities and industry.

- DOE-OE's Infrastructure Security and Energy Restoration (ISER) organization is the seat of the department's Sector Specific Agency (SSA) authority for all hazards, including cyber, to energy infrastructure. INL and PNNL are supporting the buildout of ISER's Incident Response & Coordination capabilities in conjunction with the Department of Homeland Security, North American Electric Reliability Corporation's Energy Information Sharing and Analysis Center (E-ISAC) and other grid security stakeholders.

- Lastly, INL supports ISER as it convenes the energy sector's Section 9 energy companies. These companies were previously identified in the 2013 Executive Order on Improving Critical Infrastructure Cybersecurity as providing "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effect on public health or safety, economic security, or national security." In addition to incident response capability, there is a call for a multi-lab environment where energy sector systems, both legacy and next generation, can be analyzed from a threat-informed cybersecurity vantage point. These analyses will result in specific mitigation actions shared securely, among national labs, equipment suppliers, and asset owning utilities.

Before closing, I would like to emphasize a couple of DOE and INL grid protection leadership principles shared during prior testimony from INL representatives. Specifically:

- Technology advances for automation and digital control are inherently embedded into our energy infrastructure. The opportunity to go back decades to implement large-scale manual control and response is unfeasible relative to the benefits from diversifying our energy supply with renewables, providing service and reliability into rural regions, and managing costs by balancing supply and loads.

- Cyber authorities, system defenders, and research efforts are spread across multiple government, academic, and industry organizations. Access to this dispersed, advanced control systems security talent is limited and does not facilitate response in a coordinated and integrated manner to prioritize resources on high-consequence vulnerabilities. DOE, INL and other national laboratories identified this challenge and are making great strides in assembling and implementing long-term leadership and research plans to address the highest consequence scenarios. Also, these plans will build the expertise and experimental infrastructure to deliver sustainable, long-term capacity, and solutions.

- While the nation is catching-up with incremental improvements to harden defenses and better detect and respond to a cyberattack, the national laboratories will make progress to identify and focus protections on the few areas where engineering and business

decisions have exposed infrastructure to the highest national security risks. These areas of risks are where INL can re-design and develop engineered barriers or cyber-informed human responses as last lines of defense to remove the possibility of a significant consequence.

- At INL, we believe that unexplored options exist for taking consequences off the table. To this end, INL is accelerating our implementation of a transformative methodology called "Consequence-driven Cyber-informed Engineering" that seeks and identifies high-consequence risks within the cybersecurity-industrial control systems environment. This process starts with identifying the highest impact, most severe consequences and then discovers the best process design and protection approaches for engineering out the cyber risk.

Thank you very much for the opportunity to provide testimony on this critical issue. INL is proud to take on this challenge and has much respect and gratitude for the similar resolve and commitment from you, DOE and our collaborative partners to protect our energy systems. Thank you for inviting me today to testify, and I look forward to your questions.

The CHAIRMAN. Mr. Bochman, thank you.

We are also able to welcome this morning Colonel Gent Welsh with the Washington Air National Guard. We appreciate your service.

STATEMENT OF COLONEL GENT WELSH, COMMANDER, 194TH WING, WASHINGTON AIR NATIONAL GUARD

Colonel WELSH. Thank you.

Madam Chair Murkowski, Ranking Member Cantwell, Senator Heinrich and members of this Committee, my name is Colonel Gent Welsh. I'm the Commander of the 194th Wing for the Washington Air National Guard, the Air National Guard's 89th Wing and the first cyber wing in the air guard. Thank you again for the honor to participate in such a crucial conversation today.

A quick disclaimer. Please note that I appear before the Committee today in a National Guard Title 32 status. Although I've served as a National Guard Officer for more than 23 years, my testimony today has not been reviewed or approved by anyone at the United States Air Force or the Department of Defense.

As you know, the front lines of the next conflict are not overseas in some country folks can't find on a map, they are right here, right now, every day at the doorstep of every owner and operator of our nation's critical infrastructure.

Developing a plan to best secure our critical infrastructure is challenging, primarily because more than 85 percent of our critical infrastructure to include our electrical grid, our water sources and our health care system, is owned by the private sector. As you know, the private sector doesn't always consider government a valuable partner.

In Washington State, we believe we've broken that mold. Major General Bret Daugherty, the Adjutant General in our state, is also the Governor's Homeland Security Advisor and head of all emergency management efforts. These positions give him tremendous convening authority within the state to pull people together. And with the leadership of Senator Cantwell and members of our House delegation, such as Representatives Kilmer and Heck, we're able to get a variety of stakeholders around the table routinely to include public and private owners and operators of critical infrastructure to discuss and prepare for a catastrophic cyber event.

As everyone on this Committee knows, when something does happen, it's going to happen in a state, and we've made our agency a key player in our state in the security and critical infrastructure.

We're fortunate that our state law provides our agency with policies and authorities that provide resources before and after a cyber event. We have more than 600 cyber professionals that work in the Washington National Guard at our disposal. And because we conduct continual outreach efforts, both private and local governments know what we can offer. And that's critical. The private sector has to understand and know the government can provide something tangible and resources of value if you want their true cooperation. That's why policy authorities and capabilities matter. If government has clear policies and plans for either resources or outside assistance, that makes a decision for private industry to work with government easier.

Washington is proof the government and private industry can not only get along, we can actually work together and very well. The Washington National Guard considers Pacific Northwest National Laboratory, the Idaho National Laboratory and several major utility companies, strong partners. The same could be said for Microsoft, Boeing and other Washington State corporations.

Our efforts began five years ago when we formed an integrated project team within state government to fully develop the first ever, significant Cyber Incident Response Plan for the state. I'm talking about the state, not just state government networks. We've truly led this nation and positioned Washington in many ways as a national thought leader in critical infrastructure cybersecurity at the public level.

Since then, we've continued to work with our state critical infrastructure sectors to exercise and refine our plan. I'd be remiss not bragging about the more than 600 cyber professionals in our organization. Several assist in our local utility companies, the Snohomish County Public Utilities District, with a critical cyber assessment back in 2015. Their work was beyond successful and was incredibly enlightening.

Since then, we've had a steady stream of visitors to include the former Secretary of Defense, Ash Carter, who wanted to learn more about how cyber partnerships work in Washington State.

It starts with the power of the citizen airman and soldier, our typical solider and airman participates one weekend a month and two weeks a year. Outside of that obligation they have full-time jobs, many working in the IT or critical infrastructure sectors.

They bring in a remarkable understanding of their private sector's needs and their capability shortfalls. They also bring in credibility with these organizations as National Guard members. They are folks that understand government and private industry, and they're able to bridge those gaps and that's a tremendous combination.

Looking forward, we're hopeful to bring a cyber schoolhouse to Washington State that allows us to train members of critical infrastructure sectors alongside our National Guard members. Those are the folks that are on the front lines these days in this environment.

Sharing information and best practices among those tasked to defend this nation within the private sector is how we'll be more resilient to a significant cyberattack.

And for those on the panel, I'm going to go off script for a second. We've solved some of the security clearance issues in our state, and I'd be happy to share some info on that.

Again, I'd ask that you review my submitted testimony for further information and certainly thank you for the opportunity to appear in front of this Committee from the other Washington.

And my sympathies for the Gonzaga Bulldogs because I'm a Washingtonian.

Thank you.

[The prepared statement of Colonel Welsh follows:]

TESTIMONY of

Colonel Gent Welsh
Commander, 194th Wing, Washington Air National Guard

BEFORE THE

Senate Committee on Energy and Natural Resources
U.S Senate

April 4, 2017

TESTIMONY BY

COLONEL GENT WELSH
COMMANDER, 194th Wing, WASHINGTON AIR NATIONAL GUARD

Madam Chair Murkowski, Ranking Member Cantwell and members of the Committee, my name is Colonel Gent Welsh. I'm the Commander of the 194th Wing for the Washington Air National Guard. Thank you for the honor to participate in such a crucial conversation.

Please note that I appear before the Committee today in a National Guard, Title-32 status. Although I have served as an Air National Guard officer for more than 23 years, my testimony has not been reviewed or approved by anyone in the United States Air Force or the Department of Defense.

I don't need to convince you that our nation currently faces sobering threats in the cyber realm. You've heard the alarming statistics on the number of daily attacks on our critical infrastructure to include the energy and financial sectors, our military, and other entities across the public and private spectrum. We know that as a nation, we desperately need more cyber warriors, more cyber collaboration and more cyber training. We know that the consequences of inaction will bring disaster. And we know it's not a question of 'if,' but 'when.'

Media reports concerning our national vulnerability to a significant cyber-attack often refer to a "Cyber 9/11." The media didn't invent that rhetoric – it's been discussed in the halls of Congress, as well. In early 2012, Senator Joe Lieberman rose to the Senate floor to declare "Mr. President, I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber-attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens. Would-be enemies probe the weaknesses in our most critical national assets – waiting until the time is right to cripple our economy or attack a city's electric grid with the touch of a key. The system is blinking red. Yet, we fail to connect the dots – again."

According to the *National Security Strategy* of May, 2010, "Cybersecurity threats truly represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale."

Madam Chair and members of the committee, the front lines of the next conflict are not overseas in some country most folks can't find on a map. They are right here, right now at the doorstep of every owner and operator of our nation's critical infrastructure.

And the Washington National Guard, under the leadership of Major General Bret Daugherty, the Adjutant General (TAG), is doing everything possible to address this growing threat.

For the past five years, we've been tirelessly working on efforts to better secure critical infrastructure in our state from the consequences of a devastating cyber attack. In Washington

state, our Adjutant General is also the Governor's Homeland Security Advisor and the overall head of Emergency Management efforts. These positions give him incredible "convening authority" to pull people together and enable serious conversations and planning efforts concerning a significant cyber attack. In our state, through these convening authorities, and with the help of Sen. Cantwell and members of our House delegation like Representatives Kilmer and Heck, we're able to get industry, state and local governments, owners and operators of critical infrastructure, the National Guard, and the educational services sector all together regularly in a room to make steady progress on mitigation, preparation, response and recovery efforts in cyber. These four phases may sound familiar to you because they are the four phases of Emergency Management as outlined in the National Response Framework. It's important to highlight that our state treats cyber threats like any other threat we plan and prepare for.

It takes more than simply acknowledging that someday we might see a significant cyber event that hits us like 9/11 did. If you haven't already, I'd highly recommend you download and read through the Executive Summary of the 9/11 Commission Report. It's both a fascinating and tragic read at the same time.

At its core, it acknowledges that we knew there was a problem. We were aware that Al Qaeda had interest in commercial aviation, and we weren't able to do anything about it until it was too late. The 9/11 Commission Report also highlighted four failures.

The first was imagination. I'm sure you've heard, "Failure of Imagination."

But did you realize that there were three other failures? They include policy, capabilities, and management.

If you take that same 9/11 Commission Report and replace the word 'airplane' with 'cyber,' it's scary and striking at the same time. Doing so makes it crystal clear that we face the same four failures – imagination, policy, capabilities and management – in our cyber preparation just as we did prior to 9/11.

As I mentioned, we're addressing these failures as quickly as we can in Washington state. And we appreciate your help – the fact that you're here and we're talking about this topic addresses the failure of imagination.

While it's recognized at the national level that a significant cyber attack could occur domestically in the future, the true failure of imagination lies within the unaddressed gap that exists between the rhetoric surrounding the nature of the cyber threat and our actual resource capacity to respond and recover from an attack. Federal efforts have principally emphasized efforts to prevent cyber attacks, rather than anticipate response considerations. Since 2000, federal government strategies have consistently emphasized the importance of information sharing, partnerships, analysis and warning capabilities, and coordinating efforts in cyberspace among relevant entities to minimize the impact of incidents. While these information sharing and coordinating mechanisms are vitally important, they have done little to anticipate and develop actual response capacity that would be needed post-attack. In remarks before Congress in October 2013, Charley English, the director of the Georgia Emergency Management Agency,

stated, "while the pre-event aspects of cybersecurity maintain a high level of importance, so too will the post-event considerations."

I'd like to also address the policy, capabilities and management failure pieces from a cyber perspective.

The US Department of Homeland Security designates 16 different sectors as critical infrastructure. Some of these are obvious – like the power and water sectors. Others are things you might not immediately think of, like dams (and we have a lot of those), healthcare and public health, agriculture and food, and critical manufacturing. In Washington state alone, we have operations in every one of these sectors. Before 9/11, the federal government had never fully put these sectors together and hadn't put policies and actions in place to better secure these sectors. Why? Likely because more than 85 percent of our national critical infrastructure is owned by the private sector.

That can make securing our critical infrastructure sometimes difficult and requires a very high level of trust and cooperation with the private sector. That trust isn't always easy to build – especially when you're dealing with cyber. There is an on-going national debate on how the government can work better together with the private sector. And in Washington state, we like to think we've developed the mold. In our state, the Washington Military Department has become a key player in the cyber discussion relating to securing critical infrastructure in this state. And by doing so – we're able to address some of the failures I mentioned earlier. We're fortunate that state law provides us with the policy and authorities. We have the capabilities through the more than 600 cyber professionals that work in the Washington National Guard. And we have the outreach mechanisms to touch not only the private sector but also the ability to leverage existing emergency management relationships and evangelize on cyber all the way down into our local governments.

This has helped Washington state secure the cooperation and support of the private sector. We have numerous private and semi-privately owned organizations that we now consider strong partners – to include Pacific Northwest National Laboratory and Idaho National Laboratory. We're also working closely with several utility companies. These partners are making instrumental contributions to our efforts to enhance national security.

The cooperation and support of the private sector is necessary to be successful at any level in cyber security as it relates to critical infrastructure. The private sector will need help when something bad finally happens, whether that's a conduit for information sharing or assistance in requesting federal resources. A major cyber event won't just have digital consequences. Consequences will manifest themselves in the physical space very quickly and create a complex issue to manage.

With all of that said, to get true cooperation with the private sector, government must be able to offer something tangible and something of value. When we look at cyber, we have to have something the private sector needs in exchange for meaningful and purposeful cooperation and outreach. That's why the discussion before about policy, authorities and capabilities matters. If government has clear policies and plans for either resources or outside assistance, that makes the

decision to work with government easier. This process is no different than how we work with the private sector during any other emergency or disaster.

An additional tangible resource we've been able to assist the private sector with is security clearances. The Adjutant General, in his role as Homeland Security Advisor, is able to sponsor folks for clearances based on their potential requirement to have access to classified information. This is a huge benefit to industry and is a confidence building mechanism in terms of public-private information sharing partnerships. In terms of threats, we'd love to know what industry is looking at, and they certainly want to know what we're looking at.

While we've only been at this for five years, they've been incredibly busy. In 2012, we formed an Integrated Project Team within state government to develop the first ever significant cyber incident response plan for the state. This plan goes beyond state agencies to include the whole state. After building the plan, we began a significant process to exercise it, not only at the local level but nationally. Our efforts in this area have truly led the nation and positioned Washington in many ways as the national thought leader in cyber security. From 2014 to now, we have continued to work with our state critical infrastructure sectors to refine our statewide plan, and have involved the private sector both in our planning process and exercises. We know we still have a lot of work to do, both in integrating all 16 sectors of critical infrastructure into the process and in developing the right mechanisms within government to address emerging cyber threats. We did a lot of work after 9/11 in the physical security space across all 16 sectors and now we're attempting to do that in cyber.

Here's where I get to brag a little more about our folks. We have more than 600 cyber professionals in the Washington Military Department between the Air and Army Guard, and our State Guard. After news spread about the assessment our folks accomplished at Snohomish County Public Utilities District back in 2015, we have had a steady stream of visitors who want to learn more about Washington state's secret sauce in how cyber cooperation works. What makes this success possible is what we call the power of the Citizen Airman and Citizen Soldier. Remember our typical Soldier and Airman drills one weekend a month and two weeks a year. Outside of that obligation, they have full time jobs. Our cyber folks' day jobs are out there in these very same industries, many working in sectors of critical infrastructure. They bring in a remarkable understanding of the private sector's needs as well as their capability shortfalls. They also bring credibility in dealing with these organizations. Our folks are not full time career government employees doing industry outreach. These are truly folks that understand government and understand private industry because they work in it every day and are able to bridge gaps. What a combination! Just last year, we hosted a visit from former Secretary of Defense Carter where he highlighted our efforts working with critical infrastructure as a national model.

Looking forward, securing Washington's cyber critical infrastructure is General Daugherty's top priority in cyber. We've developed a five year strategic plan that guides this agency in all of our cyber interactions. We are continuing our meaningful outreach work with actual sectors of critical infrastructure. We're working resource typing. That means working with DHS and FEMA on developing specifications for actual cyber response teams that can be deployed to help industry, the same way we resource type any other response asset. I'm not sure it would surprise

this committee, but as of today, there is not a single cyber resource type within DHS or FEMA that allows a state to request cyber response assistance from the federal government or even state to state using existing emergency management processes.

We're also working with our Congressional delegation to bring a cyber schoolhouse to Washington state that allows us to train members of the critical infrastructure sectors alongside our national guard members. Sharing information and best practices among those tasked to defend this nation with the private sector is how we'll be more resilient to a significant cyber attack in the future. Cyber resilience requires a disciplined and team engagement.

And finally, we continue to bring in cyber force structure to the Washington National Guard. Our past efforts are bearing fruit in that Washington is viewed as a place to invest additional resources at the national level.

We believe our work is a model for other government organizations and have four key recommendations for the federal government to consider to supplement and support our work:

- Develop federal governance and policy that sets forth a clear process to provide critical resources both before and following a cyber event that help harden our critical networks, and respond/recover from the follow-on consequences of a cyber attack;
- Don't treat cyber differently and use existing emergency management processes to respond/recover from a significant cyber attack. Encourage each state to identify a key official to lead cyber efforts and provide that individual with convening authority or the ability to pull various sector leads together to develop meaningful solutions and strategies;
- Ensure joint research efforts between the states and federal government continue. Washington state is seeing tremendous success through our partnerships with PNNL and INL; and
- Provide for a Cyber Schoolhouse that allows for the sharing of knowledge and expertise among National Guard and civilian critical infrastructure partners, with the ultimate goal of developing a Center of Excellence for those defending this nation.

Thank you again for the opportunity to appear here today and share some of our efforts out in the "other" Washington!

SUPERSTORM SANDY: IMPLICATIONS FOR DESIGNING A POST-CYBER ATTACK POWER RESTORATION SYSTEM

National Security Perspective

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

SUPERSTORM SANDY: IMPLICATIONS FOR DESIGNING A POST-CYBER ATTACK POWER RESTORATION SYSTEM

Paul Stockton

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

This National Security Perspective contains the best opinion of the author at time of issue. The views expressed in this study are solely those of the author and do not necessarily reflect the opinions, practices, policies, procedures, or recommendations of the US Department of Homeland Security or any other US government agency or of JHU/APL sponsors.

NSAD-R-15-075

Contents

Abstract

Sophisticated cyber attacks on the electric grid will create power restoration challenges starkly different from those in Superstorm Sandy or other previous outages in the United States. Nevertheless, rather than build a separate restoration system for cyber events, electric utilities and their government partners should explore how they can leverage existing mutual assistance agreements and other mechanisms to meet the challenges of the cyber era.

This study summarizes restoration challenges posed by Sandy and contrasts them with those that would be produced by a cyber attack on the grid. The study then examines the implications of these disparate challenges for the electricity industry's mutual assistance system and proposes potential steps to build an "all-hazards" system that can account for the unique problems that cyber attacks will create. The study also analyzes support missions that state and federal agencies might perform in response to requests for assistance from utilities and analyzes how to build a cyber response framework that can coordinate such requests. The study concludes by examining how utilities might prepare in advance for post-cyber attack opportunities to strengthen the architecture of the grid in ways that are not politically or economically feasible today.

Executive Summary

The electric power industry and its public sector partners are rising to meet a new challenge in cyber resilience. Thus far, their efforts have concentrated on protecting the grid and making it less susceptible to attack. Those efforts are vital and must continue. However, given the increasing severity of the cyber threat, utilities and their partners must also accelerate progress in another dimension of resilience: improving plans, capabilities, and coordination mechanisms to restore power and reestablish the integrity of grid control systems if cyber defenses fail.

This study discusses opportunities to accelerate power restoration after a sophisticated cyber attack on the US grid. As a starting point, the study examines how utilities restored power so effectively after Superstorm Sandy and analyzes the problems that utilities confront in building an equivalent restoration system to respond to sophisticated cyber threats. The study also examines the starkly different requests for government support for restoration that might result from a cyber attack. In addition, the study derives lessons learned from Sandy for coordinating such assistance so that it actually serves utilities' priorities—as opposed to being in the way.

After Sandy, power was restored remarkably quickly because so many utilities across the United States pitched in to help. State and federal agencies aided this flow by responding to industry requests for transportation aircraft and other support capabilities. An equivalent restoration system, tailored to meet the challenges of cyber attacks rather than storms, is essential to build resilience against potential adversaries who are aggressively mapping the US power grid and hiding malware within it.

However, adapting the current restoration system for post-cyber attack operations will entail major challenges. During Sandy, utilities sending assistance to the impact zone were secure in the knowledge that they were safely beyond the reach of the storm. No power company will be beyond harm's way during a nationwide cyber attack. To help restore power when many utility chief executive officers (CEOs) will worry that their companies are next in line for attack, mutual assistance agreements may need to overcome powerful disincentives to provide scarce restoration capabilities. Utilities can leverage exercises such as GridEx to develop specialized agreements and support protocols that can meet these challenges, just as they are doing now for coordinated physical attacks on the grid and other man-made threats.

Differences among the industrial control systems (ICSs) utilities use to manage their operations pose an additional problem. During Sandy, restoration crews arriving from the West Coast could directly contribute to repair efforts of Consolidated Edison and other companies in the stricken region because restringing power lines and other restoration tasks are similar from one utility to the next. Much greater variation exists across ICS software, applications, and system designs. Restoring these operational technology (OT) systems after a cyber attack requires specialized utility-specific training. The electricity sector and its contractors might want to explore cross utility pilot programs to determine how best to overcome these training challenges and whether such programs might be scaled up to help meet regional restoration needs. The sector might assess whether existing standards and interoperability initiatives are sufficient to mitigate the cross utility challenges that would be presented by restoration tasks. The sector might also identify which restoration tasks can be performed with less specialized knowledge so that it can focus cyber mutual assistance on providing those functions, allowing more highly trained personnel in a stricken utility to concentrate on ICS remediation.

The utility-specific nature of these OT systems will also limit the ability of government agencies to assist power restoration. State National Guard units offer the most promising potential source of support. Guard personnel performed crucial road clearance and other operations to assist grid repair crews after Sandy. Now, a growing number of State Guard

organizations and Department of Defense (DOD) contractors are partnering with their local utilities to train personnel to support post-cyber attack power restoration. These efforts should be evaluated for their cost effectiveness to determine whether they can be expanded nationwide.

Whether US Cyber Command (USCYBERCOM) should be structured to augment this support is less clear. The command has a growing cadre of cyber protection teams with ICS remediation skills. However, these teams' primary focus in an attack will be to protect DOD networks and functions. As occurred during Sandy, the president could direct the DOD to make power restoration a top priority, especially when defense networks remain secure and cyber protection assets are readily available for support missions. Yet, the authorities under which USCYBERCOM would help utilities remediate their OT systems remain uncertain, as do the specific functions that utilities would want USCYBERCOM to perform. Cyber Guard and other exercises could examine and further clarify whether and how USCYBERCOM might assist such power restoration operations.

Restoration after Sandy benefited from a strong foundation to coordinate federal assistance to states and their utilities, undergirded by the *National Response Framework* (NRF). The equivalent document for the cyber realm—the interim *National Cyber Incident Response Plan* (2010)—would almost surely prove inadequate just when the United States needed it most. An especially critical shortfall of the interim plan: it provides state governors with only a minimal role in guiding cyber response efforts, even though state National Guard organizations will likely play an increasingly significant role in supporting power restoration and other response operations. The core principles of the NRF (including its reliance on governors) should be leveraged to build a new national framework for cyber response, including an effective process for requesting assistance. The cyber response framework should complement and be integrated with other public and private sector initiatives to strengthen power restoration capabilities, especially the playbook initiative led by the Electricity Subsector Coordinating Council (ESCC). The framework should also account for cyber response tasks that go beyond those required for natural hazards, including attributing a cyber attack to those responsible for launching it.

The electricity subsector and its partners should also explore how the grid might be reconstituted once utilities have completed initial power restoration operations in an event. A cyber attack that successfully disrupts subsector functions and services may open the door to changes in the grid architecture that are too technically difficult, expensive, or politically impractical to adopt today. In addition to aggressively accelerating current efforts to strengthen grid resilience, utilities and their partners should begin developing options to reconstitute the post-attack grid before an attack occurs, so that these options will be readily available in the new political and resilience funding environment that a major outage could create.

The first section of this study summarizes restoration challenges posed by Sandy and contrasts them with those that would be created by a sophisticated cyber attack on the grid. The second section examines the implications of these disparate challenges for the electricity industry's mutual assistance system and proposes potential steps to build an "all-hazards" system that can account for the unique problems that cyber attacks will create. The third section analyzes support missions that state and federal agencies might perform in response to requests for assistance (RFAs) from utilities. The fourth section analyzes how to build a cyber response framework that can coordinate RFAs and help integrate power restoration support. Finally, the fifth section examines the phasing of power restoration efforts over the longer term, including post-cyber attack opportunities to strengthen the architecture of the grid in ways that are not politically or economically feasible today.

The Power Restoration Challenge

Lessons Learned from Superstorm Sandy

Sandy packed a one-two punch for electric infrastructure. On the night of October 29, 2012, Sandy made landfall near Atlantic City, New Jersey, as a post-tropical cyclone. Over the next three days, the impacts of Sandy could be felt from North Carolina to Maine and as far west as Illinois. With an unprecedented storm surge in the affected areas, there was especially severe damage to the energy infrastructure. Peak outages to electric power customers occurred on October 30 and 31 as the storm proceeded inland from the coast, with peak outages in all states totaling over 8.5 million, as reported in the Department of Energy (DOE) Situation Reports. Much of the damage was concentrated in New York and New Jersey, with some customer outages and fuel disruptions lasting weeks.[1] The second punch landed on November 7, 2012, as a nor'easter impacted the Mid-Atlantic and Northeast with strong winds, rain and snow, and coastal flooding. The second storm caused power outages for more than 150,000 additional customers and prolonged recovery.[2]

The combined damage to critical electricity substations, high-voltage transmission lines, and other key grid components was massive—as would be expected from the second-largest Atlantic storm on record.[3] Some major utilities in the region suffered from gaps in their preparedness to conduct repair operations on the scale that Sandy required.[4] Overall, however, utilities restored power with remarkable speed and effectiveness in most areas hit by the superstorm. Despite the vast number of grid components that needed to be repaired or replaced and the fallen trees and other impediments that restoration crews encountered, within two weeks of Sandy's landfall, utilities had restored power to 99 percent of customers who could receive power.[5]

The mutual assistance system in the electric industry was the linchpin for this success. Although the linemen and other power restoration personnel in utilities across Sandy's impact zone performed admirably, no single utility retains the restoration capabilities needed to repair the damage caused by a storm on that scale. Achieving such restoration preparedness would be extraordinarily expensive. Moreover, given the rarity of such catastrophic events, the amount of money required to enable a utility to restore power on its own would be difficult to justify as a prudent expense to state public utility commissions (PUCs), shareholders, or elected officials responsible for approving such expenditures.[6] Instead, utilities have built a highly effective voluntary system of

[1] US Department of Energy, Office of Electricity Delivery and Energy Reliability, *Overview of Response to Hurricane Sandy-Nor'easter and Recommendations for Improvement* (Washington, DC: US Department of Energy, February 26, 2013), 2, http://energy.gov/sites/prod/files/2013/05/f0/DOE_Overview_Response-Sandy-Noreaster_Final.pdf.

[2] Ibid., 4.

[3] US Federal Emergency Management Agency (FEMA), *Hurricane Sandy FEMA After-Action Report* (Washington, DC: US Federal Emergency Management Agency, July 1, 2013), 4, https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf.

[4] The Moreland Commission to Investigate Public Corruption, *Moreland Commission Report on Utility Storm Preparation and Response: Final Report* (New York: Moreland Commission, June 22, 2013), http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/MACfinalreportjune22.pdf; and Danny Hakim, Patrick McGeehan, and Michael Moss, "Suffering on Long Island as Power Agency Shows Its Flaws," *New York Times*, November 13, 2012, http://www.nytimes.com/2012/11/14/nyregion/long-island-power-authoritys-flaws-hindered-recovery-efforts.html?_r=0.

[5] US Department of Energy, *Overview*, 4. For a detailed breakdown of restoration time lines, see Rae Zimmerman, "Planning Restoration of Vital Infrastructure Services following Hurricane Sandy: Lessons Learned for Energy and Transportation," *Journal of Extreme Events* 1, no. 1 (2014): 1450004-1–1450004-38.

[6] On cost recovery constraints associated with investments in power system resilience and restoration operations, including labor force levels and standby equipment, see Edison Electric Institute, *Before and after the Storm: A Compilation of Recent Studies, Programs, and Policies Related to Storm Hardening and Resiliency, Update* (Washington, DC: Edison Electric Institute, March 2014), 13–15 and 19–26, http://www.eei.org/

mutual support, whereby utilities that are not at risk of being struck by a hurricane or other hazard can send restoration assets to those that are. The overall restoration capacity of the industry is immense; the mutual assistance system enables utilities to target support when and where specific utilities request aid.

Sandy highlighted the effectiveness of this system. Tens of thousands of mutual assistance personnel, including linemen, engineers, vegetation crews, and support personnel provided by eighty electric utilities from across the United States, flowed in to the area to help the utilities hit by Sandy—by far the largest deployment of mutual assistance capabilities in US history.[7] Utilities contributed these assets from the West Coast, the Midwest, and other regions far beyond the storm's footprint. Now, drawing on the lessons learned from Sandy, utilities are expanding the mutual assistance system to bring to bear still greater restoration capabilities in future catastrophes.[8]

This system did not emerge by chance. For decades, hurricanes and other severe weather events have hammered utilities in the eastern and southern United States. Massive ice storms, wildfires, and other natural hazards have also inflicted wide-area power outages in other regions of the United States. In response, utilities gradually built up the mutual assistance system, developing increasingly effective governance and decision-making mechanisms to allocate restoration crews and other limited resources and prioritize assistance when multiple power providers requested help.[9] Restoration crews have become as expert at line stringing, replacing power poles, and performing other functions for partner utilities as they are for their own organizations. So that personnel stay sharp between events, utilities conduct frequent exercises that are modeled on the hurricanes and other hazards they typically face. They have also established mechanisms to reimburse each other for the cost of providing assistance and (together with state PUCs) have created special cost recovery mechanisms to help pay for restoration operations in severe storms.

Decades of experience also strengthened government support for power restoration after Sandy. When the superstorm hit, state National Guard personnel in New York, New Jersey, and other states were already prepared to perform well-established (and crucial) support functions at the request of their local utilities, including road clearance and debris removal to help utility repair crews reach damaged equipment. The Emergency Management Assistance Compact (EMAC) system enabled thirty-seven states outside the affected area to send thousands of additional Guard personnel to help to execute these missions.[10] The *National Response Framework* (NRF) also provided time-tested mechanisms to coordinate the provision of government assistance.[11] Moreover, as in the case of the power industry's mutual assistance system, federal and state agencies have launched a wide array of initiatives to draw on lessons learned from the superstorm and strengthen support for power restoration in future catastrophic blackouts.

The key underlying factors that made power restoration so effective after Sandy are absent in the cyber realm. Utilities and state National Guard organizations outside of the storm's track were able to send their own restoration assets to the affected area safe in the knowledge that their own states would

issuesandpolicy/electricreliability/mutualassistance/Documents/BeforeandAftertheStorm.pdf.

[7] FEMA, *Hurricane Sandy FEMA After-Action Report*, 4.

[8] Edison Electric Institute, *Before and after the Storm*, Appendix C.

[9] B. Jim Reagan, "Mutual Assistance: Changing a Paradigm?" (talk presented at California Utilities Emergency Association Annual Meeting, San Diego, CA, June 6, 2013), www.cueainc.com/documents/Mutual%20Assistance.pptx.

[10] "The EMAC Response to Hurricane Sandy," National Emergency Management Association, accessed January 13, 2016, http://www.nemaweb.org/index.php/54-em-advocate/emac-news-archive/566-the-emac-response-to-hurricane-sandy.

[11] US Department of Homeland Security, *National Response Framework*, 2nd ed. (Washington, DC: US Department of Homeland Security, May 2013), https://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.

not be hit. In contrast, cyber adversaries may be able to launch attacks nationwide. During Sandy, repair crews from outside the affected area were able to help the affected utilities because wire stringing and other missions are substantially similar from company to company. Industrial control systems (ICSs) and other potential cyber attack targets differ widely among utilities and often require detailed system-specific knowledge to repair.

Moreover, decades of experience with hurricanes and other natural hazards shaped the power restoration system for events such as Sandy. Cyber attacks have yet to take down regional US power systems or provide any comparable real-world experience to drive the design of a cyber-oriented system. Utilities face near-constant cyber penetration efforts, including attempts to break into their ICSs and other operational technology (OT) networks that help monitor and control the grid. But cyber weapons that destroy or disrupt grid components will present real-world power restoration challenges that have never been experienced in the United States and whose requirements differ markedly from those that the current restoration system has been optimized to meet.

Utilities and their partners will need to anticipate the restoration requirements that emerging cyber threats to the grid will create. In particular, they will need to develop a design basis to help size and structure the response system for post-attack power restoration, and they will need to adapt mutual assistance agreements, government support missions, and coordination mechanisms that the United States will require to respond to increasingly capable cyber adversaries.

Setting a Design Basis for the Restoration System

Admiral Michael Rogers, the combatant commander of US Cyber Command (USCYBERCOM), notes, "We have seen nation states spending a lot of time and a lot of effort to try to gain access to the [electric] power structure within the United States," as well as to other critical infrastructure. Admiral Rogers concludes that these nations are doing so "to generate options and capabilities for themselves should they decide that they want to potentially do something."[12]

However, ongoing efforts to map utility control networks and hide malware on them provide only a starting point to assess requirements for power restoration. The BlackEnergy campaign illustrates both the value and the limitations of using current cyber penetration activities to help size and structure the restoration system. In 2014, the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned utilities that this sophisticated malware "has compromised numerous . . . ICSs" and that "multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs)."[13]

ICS-CERT reported that it has not been able to verify whether the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. However, the alert noted that "typical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment."[14]

BlackEnergy highlights the effectiveness of current adversaries' efforts to establish a presence in utility ICSs and the difficulty of determining how far the malware has spread across key networks and control

[12] Damian Paletta, "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent," *Wall Street Journal*, September 8, 2015, http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541.

[13] "Alert (ICS-ALERT-14-281-01B): Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)," Industrial Control Systems Cyber Emergency Response Team, original release date December 10, 2014, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[14] Ibid.

mechanisms.[15] Indeed, simply detecting the presence of such sophisticated malware poses a major challenge: ICS-CERT notes that the BlackEnergy campaign has been under way against US infrastructure since 2011 or even earlier.[16] Havex and other difficult-to-detect advanced persistent threats (APTs) further illustrate the growing effectiveness of both malware payloads and the attacker's access strategies, including phishing e-mails, redirections to compromised websites, and trojanized update installers on ICS vendor websites (i.e., "watering-hole" attacks).[17]

However, while such network reconnaissance and APT campaigns can help "prepare the battlefield" for subsequent attacks on the grid, potential adversaries are unlikely to reveal the most effective weapons they have in their cyber arsenals until they use them. In a crisis, these adversaries could conceivably want to prove to US leaders that they hold the power grid at risk. More typically, however, adversaries can be expected to hold their most disruptive weapons in reserve until launching an attack, thereby reducing the risk that the United States can build and deploy defenses against them.

It will also be important to size and structure the proposed power restoration system to account for the growing severity of the threat. It will take years to establish such a system, develop the governance mechanisms it requires, and train and exercise OT teams so they can effectively function in the stressful operational circumstances that cyber warfare will create. Limited budgets, combined with the difficulty of implementing such changes, will make this an incremental process. Nevertheless, to build consensus on the design requirements that such a system should ultimately achieve, it is essential to anticipate the restoration challenge that utilities will confront in 2020 and beyond.

Accounting for Uncertainties in Future Restoration Requirements

Utilities and their partners will need to overcome three problems to reach consensus on this design basis. The first is the difficulty of knowing how adversaries' capabilities will grow. Director of National Intelligence James Clapper, Deputy Secretary of Defense Robert Work, and other senior national security officials emphasize that the grid and other US critical infrastructure targets face increasingly sophisticated and potentially disruptive cyber threats.[18] The number of potential adversaries with access to such advanced capabilities is also climbing. Secretary Work notes:

> To conduct a disruptive or destructive cyber operation against a military or industrial control system requires expertise, but a potential adversary need not spend millions of dollars to develop an offensive capability. A nation-state, non-state group, or individual actor can purchase destructive malware and other capabilities through the online marketplaces created by cyber criminals, or through other black markets. As cyber capabilities become more readily available over time, the Department of Defense

[15] Lucian Constantin, "Attack Campaign Infects Industrial Control Systems with BlackEnergy Malware," *PCWorld*, October 29, 2014, http://www.pcworld.com/article/2840612/attack-campaign-infects-industrial-control-systems-with-blackenergy-malware.html.

[16] "Alert (ICS-ALERT-14-281-01B)."

[17] "Advisory (ICSA-14-178-01): ICS-Focused Malware," Industrial Control Systems Cyber Emergency Response Team, original release date July 01, 2014, https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01; and *ICS-CERT Monitor*, May/June 2015 issue, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf.

[18] *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong. (September 29, 2015) (statement of James R. Clapper, Director of National Intelligence), http://www.armed-services.senate.gov/imo/media/doc/Clapper_09-29-15.pdf; and *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong. (September 29, 2015) (statement of Robert O. Work, Deputy Secretary of Defense), http://www.armed-services.senate.gov/imo/media/doc/Work_09-29-15.pdf.

> assesses that state and non-state actors will continue to seek and develop malicious cyber capabilities to use against U.S. interests.[19]

To account for the geographic scale and scope of the blackouts such actors will be able to inflict in 2020 and beyond, and to build consensus on how the power restoration system should be sized accordingly, the federal government must continue to strengthen its information sharing with cleared industry personnel on the nature of the emerging threat. It will also be critical to facilitate the flow of information on threat signatures and other data from industry to government agencies and build on the current sharing mechanisms established by the Cyber Information Sharing and Collaboration Program and other initiatives.[20] Industry-to-industry sharing of threat information (especially in the Electricity Information Sharing and Analysis Center, or E-ISAC) will be equally essential to building the design basis for restoration. Finally, because state PUCs play a critical role in determining whether distribution companies under their jurisdictions can recover costs for investing in restoration capabilities, it will also be crucial for government agencies to help PUCs assess threat-driven requirements for investment in response capabilities. Such outreach to PUCs can succeed only if larger numbers of appropriate personnel receive security clearances.

The second challenge for establishing a design basis for the power restoration system lies in the rapid technological change under way in the US power grid and the risk that this modernization is creating unanticipated vulnerabilities to cyber attack. The integration of new digital technologies into the grid, including smart inverters and other system components that facilitate the integration of renewable generation capacity and demand response operations, is creating new "attack surfaces" for adversaries to exploit. Until utilities experience cyber warfare, it will also be difficult to assess whether the features of the grid (such as system redundancies and capabilities to reroute power) that make it so resilient against traditional hazards will limit the cascading effects of a sophisticated attack on multiple grid components, or whether the complexity of the grid will magnify the effects from such a sophisticated attack.[21]

The third challenge lies in assessing the pace and effectiveness of utility efforts to mitigate these new vulnerabilities. Utilities and their partners are acutely aware of the cyber risks that grid modernization may create and are developing innovative ways to strengthen grid security and limit cascading power failures if attacks do occur. Key initiatives being advanced by the electricity sector include the following:

- Use of "ICS Cyber Kill Chains" and other assessment methodologies to help utility OT network defenders detect and disrupt adversaries earlier in the cycle of an attack, especially against APTs[22]
- Plans and capabilities to quickly reconfigure ICSs, reset safety settings, and restore other targeted

[19] *United States Cybersecurity Policy and Threats Hearing*, Work statement, 3.

[20] US Department of Homeland Security, *Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program* (Washington, DC: US Department of Homeland Security, 2014), https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.

[21] On the risks of complexity creating cascading infrastructure failures, see Charles Perrow, *Normal Accidents: Living with High Risk Technologies* (New York: Basic Books, 1984).

[22] Michael J. Assante and Robert M. Lee, *The Industrial Control System Cyber Kill Chain* (Bethesda, MD: SANS Institute, October 2015), https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297. This work builds on the Cyber Kill Chain™ developed by Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" (paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011), www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

equipment and controls to normal (by using secured gold copy and other means)[23]

- Installation of protective relays, produced by a variety of vendors, to reduce the risks associated with relying on a single provider (although this approach introduces additional system complexity and configuration challenges)
- Initiatives to complicate the already significant challenges that adversaries face in mapping operational control networks and systems and in maintaining the accuracy and currency of those maps as utilities modify their OT systems[24]
- New technical means to detect and remove APTs from the grid systems, including firmware, and eliminate the risk of follow-on infections to replacement equipment and autonomous reattack by APTs
- Measures to retain or rapidly restore the secure, reliable data and communications essential to control the grid and reintegrate unplanned power islands in a cyber attack, even if adversaries seek to degrade Voice over Internet Protocol (VoIP) and other communications links[25]
- Steps to prevent cyber attacks from causing misoperation and physical damage to nuclear power plants, natural gas-fueled generators, and other critical grid components, thereby averting lengthy equipment restoration requirements for power restoration[26]
- Creation of more effective defenses against potential adversaries who have demonstrated the ability to compromise the product supply chains of ICS vendors, and mitigation of the risk that when downloading legitimate software updates directly from the vendors' websites, utilities will also download malware designed to facilitate exploitation[27]
- Development and deployment of power maintenance or restoration fallback systems that are invulnerable to cyber attack, including electromechanical controls (which will also require survivable communications and the retention of trained staff to maintain and operate such fallback systems)
- Creation of "last-mile" technologies or other initiatives that can create more difficult-to-bridge gaps for cyber attackers to cross[28]
- Measures to mitigate the threat of insider cyber attacks conducted by utility employees and other personnel with cleared access to networks and

[23] Defense Science Board, *Task Force Report: Resilient Military Systems and the Advances Cyber Threat* (Washington, DC: Defense Science Board, January 2013), http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[24] Installing defenses against Shodan-enabled mapping provides a starting point for such progress. Phillip Allison, "Cloak and Secure Your Critical Infrastructure, ICS and SCADA Systems: Building Security into Your Industrial Internet" (paper presented at Pacific Northwest Section American Water Works Association Conference, Bellevue, WA, 2015), http://www.pnws-awwa.org/uploads/PDFs/conferences/2015/Technical%20Sessions/Thursday/4_Cloak%20and%20Secure%20Your%20Critical%20Infrastructure,%20ICS%20and%20SCADA%20Systems.pdf.

[25] North American Electric Reliability Corporation (NERC), Severe Impact Resilience Task Force, *Severe Impact Resilience: Considerations and Recommendations* (Washington, DC: North American Electric Reliability Corporation, 2012), 39–45, http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

[26] Jan-Ole Malchow et al., "PLC Guard: A Practical Defense against Attacks on Cyber-Physical Systems" in *Proceedings of the IEEE Conference on Communications and Network Security* (Piscataway, NJ: IEEE, 2015), 326–334.

[27] *United States Cybersecurity Policy and Threats Hearing*, Work statement.

[28] Michael Assante, Tim Roxey, and Andrew Bochman, *The Case for Simplicity in Energy Infrastructure: For Economic and National Security* (Washington, DC: Center for Strategic and International Studies, November 2015), http://csis.org/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf; and David C. Walsh, "Danzig: Analog Has Value in Countering Cyber Threats," *Defense Systems*, September 1, 2015, https://defensesystems.com/articles/2015/09/01/danzig-interview-cyber-defense.aspx.

equipment, potentially in coordination with other attack vectors[29]

- Initiatives to segment the grid if an attack occurs, preplan for islanded operations, and take other measures to prevent cascading multiregional failures of the electric system[30]
- Full implementation of the additional measures recommended by the National Institute of Standards and Technology (NIST) cybersecurity framework, the NIST updated ICS security guide, the DOE *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*, ICS-CERT reports, and other sources of guidance to drastically reduce the potential geographical scope and duration of cyber-induced blackouts

Proposed Design Basis

The North American Electric Reliability Corporation (NERC) *Cyber Attack Task Force: Final Report* (2012) provides a pioneering and technically well-informed analysis of power restoration challenges that cyber attacks would create.[31] The report sounds an important caution: while grid owners and operators "are challenged on a daily basis by new cybersecurity vulnerabilities and attempted intrusions, a successful coordinated cyber attack affecting the North American bulk power system has not yet occurred. Therefore, it is difficult to confidently determine the potential impact on the reliability of the bulk power system and what additional actions may need to be taken."[32]

Rather than make such a determination, the NERC report instead uses its analysis to propose an attack scenario that can help assess US restoration requirements. The scenario assumes that future attackers will be able to impair or disable the integrity of multiple control systems or take operating control of portions of the bulk power system such that generation or transmission systems are damaged or operated improperly. Specific attack consequences that will help drive restoration requirements include the following:

- "Transmission Operators report an unexplained and persistent breaker operation that occurs across a wide geographic area (i.e., within a state/province and neighboring state/province).
- Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.
- Loss of load and generation causes widespread bulk power system instability, and system collapse within state/province and neighboring state(s)/province(s). Portions of the bulk power system remain operational.

[29] The NERC report emphasizes that "insiders pose the greatest threat, especially if they are working with a Foreign State or other High Level Threat Actors, because of their detailed knowledge of system operations and security practices. In addition, they have legitimate physical and electronic access to key systems and the controls designed to protect them. Insider individuals can provide qualitative, technical or physical assistance to the team requirements of sophisticated adversaries or pose a unique unilateral threat detection challenge, if acting alone. Individuals with the highest level of access pose the greatest threat. Furthermore, an individual with access to grid infrastructure could unwittingly or inadvertently introduce malware into a system through portable media or by falling victim to social engineering e-mails or other forms of communication." NERC, *Cyber Attack Task Force: Final Report* (Washington, DC: North American Electric Reliability Corporation, 2012), 9, http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf.

[30] NERC, *Cyber Attack Task Force*, 20–23; and NERC, *Severe Impact Resilience*, 18–39. See also NERC, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (Washington, DC: North American Electric Reliability Corporation, 2010), http://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

[31] NERC, *Cyber Attack Task Force*. See NERC, *Severe Impact Resilience*, for additional details on the potential impacts of a cyber attack on the grid. See also NERC, *High-Impact, Low-Frequency Event*.

[32] NERC, *Cyber Attack Task Force*, 1.

- Blackouts in several regions disrupt electricity supply to several million people."[33]

This scenario provides a valuable point of departure to establish a design basis for the restoration system the United States should develop for 2020 and beyond. That system should be prepared to respond to attacks in multiple regions across the United States. In addition, the system should be built on the assumption that unless utilities and their partners can eliminate carefully hidden APTs from their networks, the malware will be able to reinfect replacement equipment and software and cause repeated disruptions of grid operations.

This design basis should also be refined to reflect the geopolitical circumstances in which cyber attacks are most likely to occur. Just as with nuclear weapons, the United States needs to hedge against the risk that an adversary would launch an all-out surprise cyber attack on the grid and other critical targets. However, it is much more likely that cyber attacks would occur in the context of an intensifying political crisis in the South China Sea or the Baltics or with a regional power elsewhere in the world. Deputy Secretary of Defense Robert Work notes "almost all our combat power" is now based in the United States itself. If a regional crisis emerged, and the United States launched preparations to deploy forces accordingly, "you now have to assume that you're going to be under intense cyber attack even before you move."[34]

Department of Defense (DOD) installations, networks, and private contractors needed to support these deployments could be prime targets for cyber attacks.[35] The adversary could also attack selected portions of the US grid to achieve specific political and military objectives aimed at encouraging US leaders to resolve the crisis on terms favorable to the attacker.[36] In particular, adversaries may target attacks on the grid to disrupt mission execution at key US military bases, especially those important for operations in the crisis region. Potential objectives for such targeted cyber attacks include the following:

- Degrading the ability of US defense installations to execute their critical missions by interrupting the flow of electricity to those facilities and to the water systems and other electricity-dependent infrastructure vital for defense operations
- Disabling or degrading financial systems, public health services, transportation, telecommunication nodes, and other targets that have proven to be of special concern to US elected leaders during Sandy and other blackouts
- Creating a politically tenuous situation for US leaders by demonstrating the ability to reattack the grid after initial restoration is achieved and to strike other selected power systems across the United States

A restoration system capable of restoring power in the face of these targeted attacks would be enormously helpful to US leaders during crisis management. Such a system could also serve as the foundation on which to build more extensive response capabilities sized to handle the multiregional outages envisioned by the NERC report. However, before any such buildout moves forward, it will be essential to continue to improve our technical understanding of the physical damage and other effects that cyber attacks are likely to have on the grid, including the degree to which

[33] Ibid., 2.

[34] Bradley Peniston, "Work: 'The Age of Everything Is the Era of Grand Strategy,'" *Defense One*, November 2, 2015, http://www.defenseone.com/management/2015/11/work-age-everything-era-grand-strategy/123335/.

[35] US Senate, *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors: Report of the Committee on Armed Services*, 113th Cong., 2d sess., 2015, http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

[36] For a broader analysis of the likelihood that adversaries will launch cyber attacks on the civilian sector to gain political leverage in a conflict, see P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 131.

adversaries can achieve cascading multiregional failures of the grid.

The analysis that follows discusses ways to build a system that can restore power after coordinated, selective attacks on US utilities during an escalating regional crisis—in other words, a targeted threat. As more data become available on adversaries' capabilities and intentions, and on the effectiveness of US efforts to reduce the vulnerability of the power grid, this preliminary design basis for the power restoration system should be revised accordingly.

Leveraging Current Mutual Assistance and Industry Restoration Systems for the Cyber Era

There are potentially significant advantages in leveraging the current mutual assistance system to meet cyber threats, rather than building a separate system for cyber threats alone. Existing sector-created systems for governance and cost reimbursement in mutual assistance operations offer particular value as a basis for progress against cyber threats. After many years of refinement and consensus building by utility chief executive officers (CEOs), power companies have developed effective decision-making mechanisms to mobilize and allocate restoration crews and other restoration assets. This governance system also enables utilities to prioritize the allocation of limited assets when multiple power providers request help. Rather than depart from this proven system, a better option would be to expand its all-hazards applicability and supplement the system with branch plans and decision-making guidelines tailored to meet cyber-specific challenges.

The analysis that follows examines four especially significant challenges and potential ways to meet them. The first problem is that cyber threats will corrode the underlying incentive structure that makes existing assistance mechanisms so effective. Second, even when utilities want to help each other, the technical challenges of restoring ICS operations (versus stringing wires after a hurricane) will limit their abilities to do so. Third, while utilities have well-understood principles and organizational practices to restore power against natural hazards, a new concept of operations (CONOPS) will be needed to guide post-cyber attack restoration operations. Fourth, who is going to pay for improvements in restoration capabilities?

Challenge 1: You Can Never Be Sure You Won't Be Hit—Repeatedly

The risk that the adversary might strike utilities nationwide would stress mutual assistance systems in ways that Sandy did not. During Sandy, governors in states beyond the storm track were able to deploy National Guard forces under EMAC, secure in the knowledge that Sandy would not hit their electric infrastructures. The same was true of utilities that provided mutual assistance under the Regional Mutual Assistance Group system (and the mutual aid programs managed by municipal and cooperative utilities) that worked so effectively during Sandy. In the assumed midrange threat, the risk that the adversary could attack utilities across the United States would create powerful incentives for governors and utility CEOs to err on the side of caution and retain restoration capabilities that their own citizens and customers might need.

The risk of reattacks would magnify these problems for mutual assistance. In a pioneering work on biological threats, Richard Danzig notes that the ability of adversaries to "reload" after an initial attack, conducting follow-on strikes using fresh supplies of the same biological agents, would put enormous stress on US response planning and preparedness against such hazards.[37] Similar challenges would emerge

[37] Richard Danzig, *Preparing for Catastrophic Bioterrorism: Toward a Long-Term Strategy for Limiting the Risk*, Defense & Technology Paper (Washington, DC: Center for Technology and National Security Policy, May 2008), http://ctnsp.dodlive.mil/files/2014/10/Preparing-for-Catastrophic-Bioterrorism.pdf.

from the ability of cyber APTs to launch reattacks on grid networks and infect replacement equipment and OT software that had been installed after the original strike. The NERC cyber report notes:

> During a cyber attack and the following aftermath, responders may be lulled into the false sense of security that there is only one wave of assault. As with a storm, once the storm passes, everyone pitches in to begin the restoration process with a clear and understood recovery plan. If the attack vector(s) and techniques/tools for the attack are not fully understood and mitigated, the attacker could launch subsequent attacks to disrupt recovery efforts or respond to mitigation efforts. These later attack waves may hold devastating impact potential if not understood and expected.[38]

Utilities will be especially reluctant to share their response capabilities with their counterparts in other regions if they will remain at risk of such devastating effects even after initial power restoration operations are complete.

These factors affect the amount of restoration capacity and support that the overall power restoration response system should be sized and structured to provide, and they help determine how scarce resources should be allocated. Utilities should also conduct exercises specially focused on the governance challenges that cyber attacks will create for the mutual assistance system. Real-world experience with hurricanes and other natural hazards has helped forge an industry consensus on how to allocate restoration resources. No such experience can help the industry prepare for the cyber attacks to come. The GridEx series and other exercises could be tailored to help CEOs drill down into the disincentives for sharing created by cyber attacks and build consensus on ways to overcome those challenges.

[38] NERC, *Cyber Attack Task Force*, 29.

Challenge 2: Capabilities for Mutual Assistance

A critical enabler for success during Sandy was that before the storm hit, utilities clearly understood the types of assistance they were likely to need and how that assistance should directly support their restoration operations. The same clarity will be essential for post-cyber attack restoration. Utility owners and operators are responsible for power restoration and have unique knowledge of their system architectures and restoration plans and challenges (including for black start operations). The risk that an adversary nation will cause a blackout in an act of war does not change that equation. On the contrary, in a cyber-induced outage, utility-specific knowledge for restoration will be *at least as vital* as in natural events such as Sandy. However, key factors that facilitate mutual assistance in events such as Sandy will be problematic in post-cyber attack power restoration.

Cross Utility Technical Expertise

Utilities have many decades of experience in executing the specific tasks required to restore service. Utility personnel have comprehensive knowledge of what it takes to erect replacement utility poles, string new power lines, repair damaged substations, restore ground-level services, and conduct all the other missions necessary after traditional hazards. Utility workers are trained and equipped to perform these tasks safely and effectively, even in the midst of the effects of a storm as severe as Sandy. When Consolidated Edison and other utilities struck by Sandy determined that their own restoration capabilities were inadequate after the storm, the support missions they requested through the Regional Mutual Assistance Group system were precisely those that other utilities were already staffed and equipped to perform. And viewed from a nationwide perspective, these familiar restoration tasks are being performed every day of the year, including by the public power utilities and electric

cooperative utilities (which have their own mutual assistance systems).[39]

Moreover, the equipment that mutual assistance crews needed to repair after Sandy was largely similar to the equipment that they repaired for their home utilities. Variation does occur across circuit breakers, substation components, and other grid assets, but many other assets are generally similar across utilities, enabling Sandy mutual assistance personnel to quickly and easily contribute to line restringing and other restoration tasks.

This commonality stands in stark contrast to the proprietary utility-specific OT applications, device configurations, and ICS networks that would need to be restored after a cyber attack. Every utility in the United States has its own ICS architecture, often with nonstandard protocols, legacy systems that may be many years old, and irregular or extinct proprietary technologies.[40] Attempts to reconfigure ICSs by personnel who lack detailed knowledge of those systems can easily "brick" the systems and greatly complicate restoration efforts.

While the heterogeneity of today's control systems would hamper recovery efforts, it also has benefits for wide-area grid security. The enormous diversity of ICS software and control system components among utilities greatly complicates the task of conducting a "single-stroke" attack to black out an entire interconnect or the US grid as a whole, although it would not preclude an adversary from conducting the more targeted, limited-scale attacks examined in this study.

It is possible that the ICS supplier landscape will experience further consolidation over the next few years. If so, shared reliance on a shrinking set of component suppliers may create more similarities across utility systems, facilitating cross-training and mutual support between companies that rely on the same brands of operating systems (although utility-specific network design features would likely persist, with utility-specific configurations and data). However, some of these desirable features could also be achieved through robust standards for interoperability and data storage. This would effectively reconcile the recovery advantages afforded by homogeneity with the security advantages arising from heterogeneity. Further study is needed to assess strategies for encouraging the availability and use of a diverse yet robust set of critical infrastructure components.

Still, for now, the basic challenge remains: highly trained personnel who know how to repair their own utilities after a cyber attack will have limited ability to repair others. As an initial step to facilitate cross utility support, utilities could voluntarily develop and adopt detailed competency requirements and skill standards for OT specialists in their sector. A foundation for establishing competency requirements has been under way, with industry-specific guidance provided by the DOE including the *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)* and skills-focused research into the need for secure power system professionals. Utilities could build on this foundation by developing a typology for the skills required to assist power restoration after a cyber attack, creating shared terminology on restoration tasks and operations.[41] Then, within the mutual assistance systems managed by investor-owned utilities, public power companies, and electric cooperatives, utilities could begin the process of setting the competency requirements for post-cyber attack restoration assistance.[42]

[39] Miles Keogh and Sharon Thomas, *Regional Mutual Assistance Groups: A Primer* (Washington, DC: National Association of Regulatory Utility Commissioners, November 2015), http://www.slideshare.net/SharonThomas27/naruc-rmag-paper-1122015.

[40] NERC, *Cyber Attack Task Force*, 28.

[41] L. R. O'Neil et al., *Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs—Summary Report* (Richland, WA: Pacific Northwest National Laboratory, July 2013), http://energy.gov/sites/prod/files/2013/12/f6/SPSP_Phase2_Summary_Final_Report.pdf.

[42] Another option for the Bulk Electric System (BES) would be inclusion of competency standards in the mandatory

The electricity sector could also explore opportunities to meet the challenges of cross utility training and support by starting with small-scale pilot mutual assistance initiatives. The nationwide mutual assistance system that exists today was not built in one step. It emerged over many decades, starting with agreements among a small number of utilities in individual states and regions and then gradually scaling up over time. Mutual assistance for cyber events might start in a similar fashion, with neighboring utilities establishing cross-training programs and joint exercises for mutual assistance and then gradually scaling up such collaboration into larger assistance agreements. In the cyber realm, however, geographic proximity could be less significant than the cross utility commonality of OT software and other network features. Mutual assistance initiatives might begin between utilities that share such network commonalities. Appropriately secure information-sharing mechanisms between utilities could help them identify potential partners for pilot programs far beyond their own states.

To develop such training and exercise programs, one practical approach could be to adopt a "crawl, walk, run" strategy to build mutual assistance capabilities in a sequenced fashion. Opportunities for support lie along a spectrum of difficulty in terms of the network-specific knowledge required for system restoration. Starting at the less difficult end of the spectrum and proceeding toward the more demanding, one utility might assist another by (1) assisting with the recovery of corporate IT systems; (2) scrutinizing network logs to identify anomalies and possible malware signatures; (3) supporting perimeter defenses against ongoing attacks; and (4) directly assisting OT component and system restoration. Assistance even on these less demanding tasks could be helpful because it frees up a utility's own cyber experts to concentrate on the more difficult tasks. Adopting a crawl, walk, run approach could also facilitate the gradual development of trust and cross network familiarity vital for providing assistance at the more difficult end of the spectrum.

The Electricity Subsector Coordinating Council (ESCC) and other coordinating bodies can help provide a broader framework for establishing and scaling up such assistance initiatives. The ESCC already is developing playbooks for incident planning and government–industry coordination.[43] As the playbook effort moves forward, the ESCC should help sponsor and oversee measures to overcome the technical challenges of utility-to-utility support, as well as help build the policies and coordination mechanisms that cyber mutual assistance will require.

Growing the Talent Pool

In the hurricane belt and other areas where severe storms frequently occur, or where earthquakes or other catastrophic events present significant risk factors, utilities build and maintain substantial capabilities for power restoration. Journeymen linemen and other contractor-provided assets supplement utility crews as needed. In terms of total potential capacity, these industry capabilities provide a vast pool of assets that can be drawn on by utilities in need, as exemplified by the massive deployment of repair personnel after Sandy.

The superstorm has also prompted industry to reassess the total amount of mutual assistance resources that might be required in future catastrophes. As noted above, investor-owned utilities are now structuring their mutual assistance system to prepare for national response events (NREs) that impact a large population

requirements for certified grid operators. The NERC Cyber Security Standards require awareness and training, but they fall short of establishing competency requirements and objectives for cyber defense roles instrumental in ensuring the security of reliability-critical OT and power restoration. However, voluntary adoption of such standards will likely provide a more immediate opportunity for progress.

[43] Critical Infrastructure Partnership Advisory Council, "Electricity Subsector Coordinating Council and Government Executives Meeting Agenda," June 15, 2015, https://www.dhs.gov/sites/default/files/publications/cipac-elec-scc-govt-exec-agenda-06-15-15-508.pdf.

or several regions across the United States and require resources from multiple regions to support power restoration. The NRE initiative has greatly improved the ability of industry to coordinate and allocate utility crews and other industry emergency restoration resources at the national level, including private contractors employed by utilities. The NRE initiative also explicitly recognizes that national events requiring such massive flows of mutual assistance could include acts of war.[44]

Public power utilities are also ramping up their mutual assistance agreements and capacity for providing aid. A number of these agreements are coordinated by state associations; in other cases, public utilities make arrangements directly with each other. Public utilities have also worked with the Federal Emergency Management Agency (FEMA), the National Rural Electric Cooperative Association (NRECA), and the American Public Power Association (APPA) to create an APPA/NRECA Mutual Aid Agreement, providing a much more comprehensive system for restoration assistance in region-wide or multiregional outages.[45] The APPA has also recently developed a national mutual aid network to support municipal utilities during disasters.

A much smaller pool of trained personnel can scrub malware and conduct other highly technical operations after a cyber attack. While utility personnel had comprehensive knowledge of the tasks required to restore power after Sandy, restoring ICSs that the adversary has covertly reconfigured to misoperate is a much less familiar mission. The same is true of scrubbing APTs from firmware or the broad range of other tasks that may be required against the 2020–2025 threat.

A growing number of utilities rely on private companies to provide skilled personnel for restoration operations. When hurricanes and other natural hazards occur, utilities often rely on journeymen construction linemen and other contractor personnel to augment their own staffs because having these assets on call is less costly than maintaining additional full-time crews on the utility's payroll. A similar approach might be taken to supplement utility personnel trained for post-cyber attack restoration, as long as contractors were familiarized in advance with the specific OT networks, software applications, and restoration protocols on which individual utilities will rely.

However, the same risk of multiple nationwide cyber attacks that complicates mutual assistance agreements could also create problems when relying on contractors. Individual companies may be called on to serve multiple clients at the same time (in both the public and the private sectors), requiring staffing levels far beyond those necessary for the typical levels of support. Contractor surge capabilities will be essential to meet such demands; otherwise, utilities will be left without the assistance they need.[46]

As an alternative to relying on contractors, many utilities are increasing their own staff capabilities for post-cyber attack power restoration. No publicly available report specifies the number of utility personnel who are trained to repair and restore OT systems. However, based on an initial survey conducted for this study, elements of the sector appear to vary widely in the size of the trained staffs they maintain. One large regional transmission organization (RTO) retains more than two hundred personnel to meet its estimate of its own post-cyber attack restoration requirements. In contrast, a major

[44] Edison Electric Institute, *Mutual Assistance Enhancements* (Washington, DC: Edison Electric Institute, October 2013), 2, http://www.eei.org/issuesandpolicy/RES/TAB%205.pdf.

[45] William Atkinson, "Mutual Aid Comes of Age," *Public Power* 70, no. 2 (March–April 2012), http://www.publicpower.org/Media/magazine/ArticleDetail.cfm?ItemNumber=34001.

[46] One possible means for providing such a surge capacity, currently under development in the electricity sector, is the creation of critical power restoration teams that would draw on engineering-based industry partners in the aerospace sector and beyond. Electric Infrastructure Security Council, http://www.eiscouncil.com/.

utility that distributes electricity over multiple states has fewer than fifty staff members to assist both information technology and OT restoration. Smaller utilities have little or no such organic capability and would need to rely on mutual assistance or private sector OT service providers (who could face widespread demands for support in attacks that create multiple recurring outages).

The shortage of available OT specialists for electric utilities is part of a broader nationwide shortfall across government and other critical infrastructure sectors. The dean of the National Security Agency's College of Cyber notes that "the demand is huge" for such experts. "Industry needs them. The government needs them. Academia needs them. And right now there's just not enough. Everyone is stealing from each other."[47]

High-quality training programs for OT security, such as those conducted by the DHS ICS-CERT, can help utilities grow their cyber-capable workforces. But the capacity of these training programs is limited. They would have to be substantially expanded to grow the pool of personnel needed for post-cyber attack power restoration.[48] Expansion would also be needed in the throughput of utility personnel in ICS defense and incident response training programs conducted by the SANS Institute and other providers.[49]

Expanded exercise systems will also be essential to expand the cyber workforce and build cross utility expertise. GridEx, Cyber Guard, and other existing exercises are extremely valuable, but they are not conducted with sufficient frequency or scale to serve the learner community that utilities require. A sustained exercise system using realistic scenarios, distributed interactive play, and shared standards for assessment and certification will be essential to supplement the exercises currently in place.

Such growth would come at considerable expense and would merit rigorous cost–benefit analysis before being undertaken. Moreover, even if such an effort proved to be cost beneficial, considerable time would be required to grow an appropriately sized workforce. Until utilities and their partners can expand the pool of available talent, the scarcity of cyber-capable specialists will exacerbate the previously noted problems for mutual assistance systems. In a cyber attack, unlike in an event like Sandy, utilities may be reluctant to send assistance crews for mutual assistance because the adversary could strike anywhere in the United States. The vastly smaller pool of trained personnel for post-cyber attack restoration, versus those available for stringing line or erecting poles after a storm, will tend to make utility CEOs even more likely to keep those assets close to home where they might be needed at any moment.

Increasing the trained staffs for cyber response in the electricity sector capabilities would ease the problems of mutual assistance for cyber attacks but would not fully resolve them. Even substantially augmented staffs would likely be unable to assist other utilities unless they are cross-trained to do so and gain sufficient familiarity with these other OT systems to be of value. Utilities could explore such cross-training opportunities as part of a broader analysis of alternatives that will assess US power restoration requirements, the array of options to meet them, and criteria for evaluating those options.

---

[47] Darren Samuelsohn, "Inside the NSA's Hunt for Hackers," *Politico*, December 9, 2015, http://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330.

[48] Brent Stacey, associate director of the Idaho National Laboratory, detailed the rationale for such an expansion. See *United States House of Representatives Science Subcommittee on Energy and Science Subcommittee on Research and Technology* (October 21, 2015) (statement of Brent Stacey, Associate Director, Idaho National Laboratory), http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf.

[49] ICS515: ICS Active Defense and Incident Response, course offered by SANS Institute, https://www.sans.org/course/industrial-control-system-active-defense-and-incident-response.

Replacing Damaged Equipment

The storm surge and weather effects during Sandy inflicted extensive physical damage on electricity substations and other critical grid components. As in Sandy, utilities can reroute power around damaged equipment to help speed power restoration. Such rerouting opportunities may also exist in response to cyber attacks (although it will be essential to prevent the spread of malware from one utility to the next). To further accelerate restoration time lines, utilities have also established programs to supplement their own stores of replacement equipment by drawing on cross utility programs to share grid components. In particular, initiatives such the Spare Transformer Equipment Program (STEP), SpareConnect, and the Grid Assurance initiative help enable utilities to support each other by providing spare high-voltage transformers and other components.[50] Although these programs emerged to mitigate the risk of physical damage caused by natural hazards or kinetic attacks, they could also serve as a model for creating equivalent initiatives to accelerate the replacement of equipment that is bricked or otherwise destroyed by malware.

The 2012 cyber attack on the Saudi Aramco oil company exemplifies the potential benefits of building such equipment-sharing mechanisms. That attack reportedly required the replacement of thousands of office PCs whose hard drives had been wiped.[51] If US power companies identify grid equipment that is at similar risk of large-scale damage, they might supplement their own cyber-protected spares by establishing programs to share replacements, thereby accelerating power restoration.

However, the Saudi Aramco attack did not strike the company's OT systems. Spare equipment replacement initiatives for the US grid would need to account for the risk that adversaries will disable programmable logic controllers and other OT equipment. Uncertainties also persist over the degree to which adversaries will be able to inflict widespread damage on generators or other difficult-to-replace grid components. Additional research will be essential to clarify these risks before equipment replacement programs can be sized and structured to mitigate them. Moreover, given the inherent difficulties of repairing and replacing generators, measures to protect them from attack (as opposed to building programs to restore these assets after they are damaged) are likely to offer a better way to strengthen grid resilience.

Challenge 3: Concepts of Operation to Accelerate Industry Power Restoration

When hurricanes and other familiar hazards strike the electric grid, affected utilities and those providing mutual assistance have well-understood and frequently exercised plans and operating principles to guide restoration efforts. The electricity sector is developing equivalent principles for post-cyber attack restoration. A critical step in that process will be to develop a consensus-based CONOPS to accelerate the restoration of electric service and help deny adversaries the political and military effects they seek to achieve by attacking the grid.

To be most useful to the power sector, such a CONOPS should concisely describe the structure for an industry-wide restoration system for cyber threats (as opposed to natural hazards). The CONOPS should also identify guiding principles for how the electric industry will use that system, and how utility partners in the public and private sectors should support restoration operations.[52]

[50] "Spare Transformers," Edison Electric Institute, http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

[51] Jim Finkle, "Exclusive: Insiders Suspected in Saudi Cyber Attack," *Reuters*, September 7, 2012, http://www.reuters.com/article/net-us-saudi-aramco-hack-idUSBRE8860CR20120907.

[52] For guidelines on developing CONOPS, see IEEE Computer Society, *IEEE Guide for Information Technology—System*

The analysis that follows identifies key issues and recommendations for the development of such a CONOPS by the two basic components of the US electric system: (1) electric distribution utilities and (2) Bulk Electric System (BES) entities, which include the owners and operators of electrical generation resources, high-voltage transmission lines, interconnections with neighboring systems, and associated equipment.[53] Although regulated differently, both components will confront shared challenges in post-cyber attack power restoration and will need to be integrated into holistic sector-wide resilience efforts.

Key Components of a Cyber Restoration Concept of Operations for Distribution Utilities

For blackouts caused by hurricanes or other natural hazards, the utilities struck by the event play a central role in assessing damage to their infrastructures and developing plans to guide and prioritize restoration efforts. Utilities typically have well-developed and frequently exercised emergency management procedures to conduct such operations. They are also incorporating advances in distribution automation, smart meters, and other smart grid technologies to remotely pinpoint outage locations and accelerate power restoration. Utilities use these systems to help generate work tickets to replace downed poles and repair other damaged infrastructure and to oversee restoration efforts by their own crews and those provided by other utilities under mutual assistance agreements, all in alignment with familiar emergency procedures for re-energizing the grid.

Different procedures and organizing principles will be required when responding to cyber threats. The first challenge that distribution utilities will face is detecting that an attack is under way and determining how adversaries are disrupting utility systems. During Sandy and other natural hazards, knowing that a destructive event is occurring is simple. Determining which poles are downed and need to be replaced is equally straightforward. Cyber attacks on ICSs pose different and much more difficult detection and damage assessment challenges, especially against APTs designed to hide on utility networks. Adversary-imposed changes in control system networks and operating instructions can be difficult to discover. Attack detection is further complicated because few ICSs maintain logs of changes to them, and legacy technology in OT networks (including outdated software and third-party applications) may provide multiple opportunities for adversary exploitation. The first indication that an attack is under way may be when HMIs begin to "gray out," equipment begins to misoperate, and power systems begin to fail. Opportunistic adversaries might even time their strikes to coincide with a hurricane, earthquake, or other severe natural event, thereby further complicating efforts to determine that a cyber attack is under way.

Power restoration against cyber attacks will require the ability to rapidly detect the malware or other attack mechanisms that are disrupting utility operations. Once detected, that malware must be analyzed so that countermeasures can be developed against it. Those countermeasures can then be deployed as utilities search for and eradicate that malware throughout their ICSs and reestablish the integrity of their networks.

Organizing Principles

Few if any utilities will have sufficient in-house technical expertise to reverse-engineer malware and develop effective network inspection and mitigation measures against APTs. Private contractors can assist

Definition—Concept of Operations (ConOps) Document, IEEE Standard 1362-1998 (Piscataway, NJ: IEEE, March 19, 1998).

[53] NERC, *Glossary of Terms Used in NERC Reliability Standards* (Washington, DC: North American Electric Reliability Corporation, September 29, 2015), 14–16, http://www.nerc.com/files/glossary_of_terms.pdf. Note that although distribution utilities and BES components are regulated differently, many of the largest US utilities own and physically operate both high-voltage transmission (BES) and distribution systems, creating significant overlap between these sector components.

utilities in such efforts. However, to provide more robust and broadly available sources of technical assistance, including from government sources, a highly coordinated system would be needed to rapidly analyze utility logs and data, catalog and analyze malware provided by utilities, and develop remediation measures. Such a support system would also need the ability to quickly deliver those measures back to utilities struck by the attack (and also warn and deliver prevention measures to block attacks on other utilities).

However, as already noted, individual utilities have the best understanding of their own network structures, applications, and other features and will have unmatched experience and expertise in managing their network operations. Their personnel—and those from utilities cross-trained to work on their networks—will need to play a crucial role in applying the remediation measures developed by supporting organizations. Accordingly, the power restoration system should be organized on the principle of tightly coordinated support and distributed utility-led execution. Subsequent portions of this paper examine how industry and government can partner to help provide utilities with such tightly coordinated support on malware signature identification, remediation measures, and other forms of technical assistance.

Principles for Emergency Operations and Power Restoration

CONOPS for post-cyber attack restoration will also require cyber-specific guiding principles and shared best practices for power restoration. APTs differ from natural hazards in that they can be designed to reattack utility networks if not completely eradicated and can also spread across utility components (and, potentially, from one utility to many others). Both of these threat characteristics will create challenges for restoration beyond those already discussed for mutual assistance.

Moreover, adversaries are intelligent and adaptive in ways that natural hazards are not. As adversaries modify their means of attacking in response to electricity sector and US government countermeasures, a centralized support/decentralized implementation system will not only need to be able to sustain operations during reattacks, but it will also need to keep pace with adversaries' adaptations.

Unlike hurricanes, cyber attacks can also seek to corrupt system integrity and manipulate data and control sensors on which utilities rely to provide reliable and resilient service. Major utilities typically use energy management systems (EMSs) that provide highly redundant hardware, software, and telecommunications components to help sustain their operations and support restoration as needed. These systems and the data they carry will be prime targets for attack. Malware that can propagate across networks, and use utility assets to disrupt other grid components linked to them, will pose additional problems for defending these systems and restoring them if an attack occurs.[54]

To meet the novel challenges posed by cyber threats, a number of utilities are developing a tiered approach to sustaining service during an attack and restoring service once disruptions occur. These measures include (1) hardening their primary control centers against attack; (2) building robust backup control centers; (3) securing their gold copies of OT system software and exercising to rapidly install it if needed; (4) developing "spare-tire" control mechanisms that will not provide the full functionality of regular systems but can sustain limited vital operations; and (5) maintaining fallback mechanical controls that would otherwise be at risk of degrading and becoming inoperable. Many of these same initiatives are also being adopted or developed by high-voltage transmission companies, RTOs, and other BES entities.

[54] NERC, *Severe Impact Resilience*, 35.

Utilities may want to accelerate and expand their sharing of potential best practices and restoration guidelines. The CONOPS for restoration should provide guidelines and operating principles on the following:

- How to operate a system that has lost its integrity and experienced a cyber incident that has demonstrated the ability to disrupt, misoperate, or physically damage equipment
- The communication and operating protocol that impacted utilities follow
- What neighboring and interconnected utilities should do with their data connections to the impacted utility
- How utility systems' components might be safely taken off-line to limit the spread and reduce the consequences of an attack (especially physical damage to grid equipment), thereby accelerating restoration

Developing an Integrated Restoration Strategy for the Bulk Electric System and Distribution Utilities

To disrupt distribution utilities' ability to sustain service to defense installations and other critical US assets during a crisis, cyber adversaries may attack those utilities directly, but they may also strike the BES that provides power to distribution systems. Adversaries can also attack the BES to cause wider-area outages. If cyber attacks can damage or disrupt the generation plants, high-voltage transmission systems, and interconnections with neighboring systems that make up the BES, adversaries may be able to affect multiple distribution systems and potentially cause cascading grid failures across broad regions of the United States. A CONOPS to accelerate post-cyber attack power restoration will need to encompass both BES and distribution utilities in an integrated way. Digital assets at nuclear power plants are subject to standards set by the Nuclear Regulatory Commission; these plants, too, should be part of a holistic approach to cyber resilience.

NERC standards require that utilities with BES assets maintain both primary and backup EMSs and meet a growing set of critical infrastructure protection (CIP) reliability standards in response to cyber threats.[55] RTOs and other components of the BES also have long-established principles to sustain service and guide restoration operations after natural hazards. When faced with an approaching storm such as Sandy, RTOs can go into conservative operations to help maintain the reliability of the BES. They can purchase additional power reserves, making more resources available to respond to unexpected events, staff up their backup control centers, and take additional measures before a storm hits. When damage to the grid begins to occur, they can route power around disabled substations and other complements and reconfigure their systems to limit the areas that lose electric service and help accelerate the restoration of power.[56]

[55] NERC, *Cyber Security Reliability Standards CIP V5 Transition Guidance: ERO Compliance and Enforcement Activities during the Transition to the CIP Version 5 Reliability Standards* (Washington, DC: North American Electric Reliability Corporation, August 12, 2014), http://www.nerc.com/pa/CI/Documents/V3-V5%20Transition%20Guidance%20FINAL.pdf. For broader principles and plan elements to guide BES guide restoration operations, see "Electric System Restoration Reference Document," in NERC, *NERC Operating Manual* (Washington, DC: North American Electric Reliability Corporation, August 2014), ESR-5–ESR-6, http://www.nerc.com/comm/OC/Pages/Operating-Manual.aspx.

[56] For examples of conservative operation triggers and response actions, see PJM, *Fundamentals of Transmission Operations: Conservative Operations* (Audubon, PA: PJM, October 3, 2013), http://www.pjm.com/~/media/training/new-pjm-cert-exams/foto-lesson9-conservative-operations.ashx; MISO, *MISO Operating Procedures* (Carmel, IN: MISO, 2015), https://www.misoenergy.org/Library/Repository/Communication%20Material/One-Pagers/One%20Pager%20-%20MISO%20Operating%20Procedures.pdf; and SERC Reliability Corporation, *Guideline: Conservative Operations Guidelines* (Charlotte, NC: SERC Reliability Corporation, May 20, 2015), http://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2.

Equivalent mitigation measures and principles to support power restoration may be essential when responding to cyber attacks. Some measures, such as standing up backup control centers, will be similar to those required for traditional hazards. Others may be cyber specific: for example, efforts to protect or reestablish the integrity of telemetry data on which RTOs rely. NERC's report on severe impact resilience (2012) proposes an array of options to help protect BES components from possible physical damage, preserve the integrity of BES data and systems, and limit the spread of malware across the US grid. Possible measures include the following:

- Disable supervisory control and data acquisition (SCADA) and communications networks from substations and generation facilities
- Disconnect relays from breakers
- Segment the power grid into preplanned islands (and effectively manage the unplanned islands the cyber attack creates)
- Isolate network connections to the Internet
- Safely shut down systems to deny an attacker the ability to cause further damage[57]

Although measures could be useful to blunt cyber attacks and downsize the power restoration requirements that BES entities would face, many of them could also seriously disrupt the ability of RTOs and other entities to sustain service or monitor and control grid operations. Realistic exercises will be vital to determine whether and how these options might best be used and how the consequences (and potential liability issues) associated with intentional service interruptions can be mitigated.

Energy Management Systems for Cyber Events

As noted above, NERC requires utilities with BES assets to maintain both primary and backup EMSs to manage those assets, including generators, high-voltage transmission lines, and interconnections with neighboring systems. EMSs include highly redundant hardware, software, and telecommunication components to maximize the availability and accuracy of data utilities needed to manage the grid. This redundancy makes EMSs extremely reliable after hurricanes and other familiar hazards. With cyber attacks, however, EMSs will be at special risk. To the extent that the redundant EMS components are of the same make and model as those used in the primary system, they may also fail during a cyber attack unless they are protected against infection or reinfection by persistent malware. Moreover, precisely because EMSs will be so vital for limiting the impact of cyber attacks on the grid and for accelerating power restoration, they may themselves be targeted for disruption.[58]

To mitigate the risk that adversaries will disable or corrupt both primary and backup EMSs and data, a growing number of utilities are developing independent, secured fallback systems to use in emergencies. These spare-tire management systems provide only those capabilities that are minimally necessary to operate key BES components. While grid operators performing the roles of balancing authority and reliability coordinator are trained to manually calculate critical data required to operate their portions of the BES, spare-tire systems can provide valuable support for such operations. In particular, such spare-tire systems can help utility personnel operate crucial assets to maintain load and generation balance by monitoring and controlling a core of generation units and tie lines for

[57] NERC, *Cyber Attack Task Force*, 63; and NERC, *Severe Impact Resilience*, 18–50. Note that many of the recommendations in the resilience study apply to noncyber hazards, including coordinated kinetic attack.

[58] For an analysis of potential EMS vulnerabilities and mitigation options, see NERC, *Industry Advisory: Preventable SCADA/EMS Events – II* (Washington, DC: North American Electric Reliability Corporation), http://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/Preventable_SCADA_EMS_Events_II.pdf.

a specific geographic area. A basic level of automatic generation control functionality from such a system can also help operators to maintain stability within their systems and the interconnections with their neighboring utilities.[59]

As with any EMS, these spare-tire systems require a mathematical model that represents the electrical and operational characteristics of the BES assets being monitored and/or controlled, a database for rendering operator displays, and reliable telecommunications connectivity between the core BES assets. Preplanning for the operation of these systems will also be vital to account for the varying designs and configurations of assets that make up the BES and the diverse telecommunications components that utilities use. DOE national laboratories or other research facilities could support such integrative efforts by developing additional software tools to support grid-wide emergency operations and by providing a common training platform for the use of spare-tire systems.

Managing Conflicts between Mission Priorities

The CONOPS will also need to help utilities and their government partners resolve potential conflicts between efforts to attribute the cyber attack to a specific adversary and operations to restore power. To retaliate against an attack (and to be able to credibly deter attacks), the United States must have the ability to determine the source of the attack, even when an adversary uses remote botnets or takes other measures to complicate attribution.

Acquiring and preserving forensic data from the attack will often be essential for attribution. Ideally, system operators will be able to capture live system data (i.e., current network connections and open processes) before a machine suspected of being compromised is disconnected from the network. But exercising such restraint in a large-scale attack will be difficult and perhaps inappropriate.

Indeed, many of the recommended best practices to support forensics and attribution may directly conflict with the imperative to restore grid functionality as rapidly and effectively as possible. Utilities are cautioned against running antivirus software after an attack because an antivirus scan changes critical file dates, which impedes discovery and analysis of suspected malicious files and time lines. ICS-CERT also warns system operators against making any changes to the operating system or hardware, including updates and patches, because they will overwrite important information about the suspected malware.[60] Quickly reconciling these potential conflicts between forensics and power restoration will be essential to build US preparedness for post-cyber attack operations.

In December 2015, the Defense Advanced Research Projects Agency launched the Rapid Attack Detection, Isolation and Characterization (RADICS) initiative to advance the development of forensic tools that will require less delay or disruption of system restoration operations.[61] In the end, however, it may not be technically or operationally possible to fully deconflict these missions. Delayed restoration may be the price of effective attribution.

Funding Improved Utility Capabilities for Power Restoration and Mutual Assistance

Utilities' initiatives to increase cyber-qualified staffs and make other investments in cyber resilience will

[59] Data provided by a major electric utility that asked to remain anonymous.

[60] *ICS-CERT Monitor*, July/August 2011 issue, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2011.pdf.

[61] Defense Advanced Research Projects Agency, *Broad Agency Announcement: Rapid Attack Detection, Isolation and Characterization Systems (RADICS)*, DARPA-BAA-16-14 (Arlington, VA: Defense Advanced Research Projects Agency, December 11, 2015), 10–13, https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-BAA-16-14/listing.html. See especially Technical Area 3.

cost money. At a time when many utilities face flat revenues and confront other business challenges, clarifying how they will be able to recover their costs for such investments is a critical issue. These cost recovery issues may be even more challenging for power generation companies that rely on market revenues and do not have cost-of-service rates.

NERC's CIP reliability standards provide BES entities not only with requirements to meet but also with an objective basis for determining whether proposed investments in cyber resilience are necessary to meet those requirements and should therefore be eligible for cost recovery. BES entities can also request that their regulated transmission tariffs include the cost of resilience investments above those required for compliance with minimum standards.[62]

In contrast, state PUCs are responsible for ruling on proposed resilience investments made by the investor-owned utilities that distribute the vast majority of electricity in the United States. PUCs have a long record of allowing utilities to recover their costs for maintaining system reliability after typical storms and other natural hazards, including staffing and equipment for restoration operations. Sandy created a wave of new rate cases and tariff proposals by utilities to build their resilience against less frequent but especially destructive events. PUCs have deemed many, but far from all, of these investment proposals to meet their requirement that they be "prudent" and cost-effective.

Cyber attacks present a more difficult challenge for cost recovery. For flooding, hurricanes, and other natural hazards to the power grid, ample historical data exist to help predict the likelihood of an event (although rising sea levels and the increasing severity of storms is driving updates in many of these predictive models). Data on the likelihood of an event occurring at a given level of severity provide a basis to assess the potential benefits of investments against such events and whether those investments are prudent and worth their costs.

No historical data are available to predict the likelihood of a destructive cyber attack or other man-made threats to the power grid. Potential adversaries are continually probing and mapping the electricity sector in ways that can facilitate future attacks. However, the probability of a future attack occurring on a specific utility is not only unknown, but it is unknowable. Assessing the prudence of investments against such hazards is far more difficult. Indeed, PUCs are only beginning to build decision-making criteria that can allow them to assess the prudence and cost effectiveness of proposed investments in post-cyber attack restoration capabilities. Until clear, objective criteria exist, electricity distribution companies that want to strengthen these capabilities are at risk of having PUCs deny the funding needed to recover their costs.

The National Association of Regulatory Utility Commissioners has recognized the growing significance of cyber threats to the electric industry and has recommended a useful list of discussion points for engaging with utilities on cyber preparedness issues.[63] PUCs in states such as Connecticut and Pennsylvania are also developing strategies and recommendations to strengthen grid resilience against these threats.[64] However, these

[62] US Federal Energy Regulatory Commission, *Extraordinary Expenditures Necessary to Safeguard*, Docket No. PL01-6-00096 FERC ¶ 61,299 (2001) (statement of policy), http://www.iso-ne.com/committees/comm_wkgrps/trans_comm/tariff_comm/mtrls/2002/oct102002/A4_1466800.pdf.

[63] Miles Keogh and Christina Cody, *Cybersecurity for State Regulators, with Sample Questions for Regulators to Ask Utilities* (Washington, DC: National Association of Regulatory Utility Commissioners, February 2013), http://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf.

[64] Pennsylvania Public Utility Commission, *Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities* (Harrisburg, PA: Pennsylvania Public Utility Commission), http://www.puc.pa.gov/general/pdf/Cybersecurity_Best_Practices_Booklet.pdf; and Connecticut Public Utilities Regulatory Authority, *Cybersecurity and Connecticut's Public Utilities* (New Britain, CT: Connecticut Public Utilities Regulatory Authority,

strategies primarily focus on prevention and offer little or no guidance on measures to accelerate power restoration. They are only beginning to define criteria for cost recovery. The Connecticut strategy calls for technical meetings between regulators and utilities to establish performance standards for managing cyber threats.[65] Such discussions should occur between PUCs and utilities nationwide to help build consensus on prudence and cost-effectiveness criteria for investments in cyber resilience, including capabilities to accelerate power restoration.

Additional funding for utility investments might come from DOD and other federal departments responsible for US security. Given the risk that adversaries will target the grid to disrupt the execution of critical missions at defense installations, and the importance of accelerated power restoration to those installations, a strong rationale exists for military bases to partner with their neighboring utilities to improve grid resilience against cyber threats.[66] Exploratory partnership initiatives are already under way, most notably the DOE-supported Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) microgrid demonstration project conducted with the Hawaiian Electric Company for Camp Smith, Hawaii. The project seeks to demonstrate how utilities and DOD can partner to develop a secure microgrid architecture for military installations, including distributed and renewable power generation and energy storage. The project has also examined whether and how such developments might be used by nonmilitary facilities and critical infrastructure.[67]

Intense competition for funding within DOD will limit the department's ability to scale up these projects on a nationwide basis. Instead, the DOD could develop new business models for public–private partnerships with utilities, including ways to price resilient electric service so that utilities can recover the costs of providing for rapid power restoration and other prudent investments in cyber resilience. DOD's *Energy Resilience Business Case Analysis Study* (commissioned April 2015) provides an important initial step in this direction.[68] That study, and associated efforts to strengthen energy resilience for the military bases, could become the focus of expanded discussions between DOD and the electric industry.

Government Support for Utility Restoration Operations

Campaigns such as BlackEnergy have already demonstrated the value of existing mechanisms of government support to the electricity sector. The ability of DHS's ICS-CERT to meet industry requests for assistance (RFAs) and help utilities identify and counter malware implanted on their systems provides a model of effective federal support.[69] A growing number of state National Guard organizations and other state agencies are also pursuing initiatives to help grid owners and operators deal with ongoing cyber intrusions.

However, an attack with a national security impact like that of the targeted threat scenario described in this study would create an entirely different operating environment. Such an attack could also spur industry requests for government cyber assistance far beyond those that state and federal agencies are currently

April 14, 2014), http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf.

[65] Connecticut Public Utilities Regulatory Authority, *Cybersecurity and Connecticut's Public Utilities*, 25.

[66] On the broader national security rationale for DOD–utility partnerships, see Department of Defense, *Mission Assurance Strategy*, April 2012.

[67] "SPIDERS JCTD Smart Cyber-Secure Microgrids," US Department of Energy, http://energy.gov/eere/femp/spiders-jctd-smart-cyber-secure-microgrids.

[68] US Department of Defense, Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, *Energy Resilience Business Case Analysis Study* (Washington, DC: US Department of Defense, forthcoming).

[69] "Alert (ICS-ALERT-14-281-01B)."

prepared to meet—that is, if industry can first identify what kinds of support would actually be useful.

The Post-Sandy System for Government Support to Utilities

Sandy has driven major improvements in federal and state agency preparedness to support power restoration. This emerging support system can help provide a foundation for assistance after cyber attacks on the grid. Indeed, because key components of this system are still evolving, now is the ideal time to clarify how the system should be adapted and supplemented to help utilities meet emerging cyber threats.

DOE is playing a key role in shaping the post-Sandy system for government support in power restoration operations. DOE is the federal coordinator and primary agency for Emergency Support Function (ESF) #12, Energy. ESF #12 states that "restoration of normal operations at energy facilities is the responsibility of the facility owners." However, when industry requests federal support for power restoration, ESF #12 is "the primary Federal point of contact with the energy industry" for such requests. More broadly, under DOE leadership, ESF #12 is "intended to facilitate the restoration of damaged energy systems and components" for events requiring a coordinated federal response.[70] DOE is also the energy sector-specific agency, which gives it additional leadership responsibilities in responding to non-Stafford Act emergencies.

DOE's Overview of Response to Hurricane Sandy-Nor'easter and Recommendations for Improvement (February 2013) identified a number of areas in which the department's plans and organizational arrangements "fell far short of what was needed to respond, mitigate, and restore the damaged energy infrastructure."[71] Two shortfalls proved especially critical and are now the focus of DOE initiatives to strengthen the department's support for future restoration operations.

First, Sandy revealed that DOE lacked the organizational structure needed to provide adequate situational awareness of power outage locations and restoration time lines. DOE's structure also failed to specify where and how utility representatives would tie in to the department and provide industry priorities for support. Under the OE-30 Energy Response Organization structure, DOE is now reorganizing itself to overcome these shortfalls and help strengthen its ability to support emergency response operations.[72]

Second, during Sandy, DOE lacked adequate plans to guide its response operations. In partnership with FEMA, the department was very successful in improvising during the superstorm, developing the mechanisms and decision-making systems to coordinate government responses to industry RFAs. But it would have been far better to have had a plan already in place. DOE's *Energy Response Plan*, version 1.0, takes initial key steps to establish such a plan.[73]

Sandy is also spurring FEMA's progress on power restoration support. As with DOE, FEMA is exploring new structural arrangements to support power restoration and build on lessons learned from the

[70] US Department of Energy, *Emergency Support Function #12–Energy Annex* (Washington, DC: US Department of Energy, January 2008), 1–2, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/nrf-esf-12.pdf.

[71] US Department of Energy, *Overview*, 7.

[72] US Department of Energy, *OE-30 Energy Response Organization* (Washington, DC: US Department of Energy, August 2015). To help meet the special challenges of establishing situational awareness during a cyber attack, including assessing the risk that adversaries will spoof or corrupt telemetry data, the Defense Advanced Research Projects Agency RADICS initiative includes an effort to develop regional situational awareness technologies with reduced vulnerabilities to such risks. Defense Advanced Research Projects Agency, *Broad Agency Announcement: RADICS*, 7–8.

[73] US Department of Energy, *The DOE Energy Response Plan*, version 1.0 (Washington, DC: US Department of Energy, February 2015), 6–7.

creation of the Energy Restoration Task Force during Sandy.[74] FEMA and DOE are also collaborating to develop a new framework, the Power Outage Incident Annex (POIA), to coordinate federal assistance in outages even more severe than after Sandy. The POIA will describe the process and organizational constructs that the federal government will use to respond to and recover from loss of power resulting from natural or unnatural disasters. Among other tasks, the POIA is designed to identify key federal government capabilities and resources, prioritize core capabilities, and outline response and recovery resource requirements.[75]

Cyber threats should figure prominently in the man-made hazards that the POIA addresses. More broadly, to the maximum extent possible, the emerging post-Sandy system for federal restoration support should provide the foundation for assistance in cyber attacks. As with industry's mutual assistance system, adopting such an all-hazards approach will avoid the operational risks and inefficiencies associated with building stovepiped mechanisms for government assistance. Yet, as in industry, an all-hazards approach will also have to account for the types of assistance that utilities are likely to need and the unique operating environment that a cyber attack on the United States would create.

Information and Intelligence Sharing

Before Sandy hit, the National Oceanic and Atmospheric Administration (NOAA) provided critical warning of the storm's likely path. By providing timely and accurate forecasts to emergency managers and the private sector, NOAA helped utilities and their government partners mobilize and stage resources to accelerate power restoration. NOAA is strengthening its modeling capabilities to provide still greater predictive accuracy in the future.[76]

Information requirements for cyber attacks will be entirely different but equally vital. As with Sandy's storm track, the occurrence of an intense regional crisis may provide advanced warning that a cyber attack could occur, as opposed to a "cyber Pearl Harbor" strike launched as a total surprise. The ability of the federal government to share classified information on the emerging risks of an attack could provide valuable time for utilities to stand up their emergency management systems, accelerate their network protection measures, and prepare for mutual assistance operations.

Once an attack is under way, utilities across the United States will need the fastest and most accurate data possible on threat signatures and remediation measures. The E-ISAC, in collaboration with DOE and the ESCC, serves as the "primary communications channel for the Electricity Sector" and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.[77] In particular, the E-ISAC helps the sector establish "situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange."[78] The ESCC, in turn, serves as the principal liaison between the federal government and the electric

[74] FEMA, *Hurricane Sandy FEMA After-Action Report*.

[75] US Government Accountability Office, *Critical Infrastructure Protection: Preliminary Observations on DHS Efforts to Address Electromagnetic Threats to the Electric Grid*, Statement of Christopher P. Currie, Director, Homeland Security and Justice, Before the Committee on Homeland Security and Governmental Affairs, US Senate (Washington, DC: US Government Accountability Office, July 22, 2015), 8, http://www.gao.gov/assets/680/671971.pdf.

[76] Louis Uccellini, "Sandy—One Year Later," *Weather Ready Nation*, October 28, 2013, http://www.nws.noaa.gov/com/weatherreadynation/news/131028_sandy.html#.VqvIaLEo7Gg.

[77] Patricia Hoffman, Assistant Secretary of Energy, Letter to Gerry Cauley, March 14, 2013, http://www.nerc.com/news/Headlines%20DL/ES-ISAC%20Letter%2014MAR13.pdf; and "Electricity ISAC," North American Electric Reliability Corporation, http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

[78] "Electricity ISAC," North American Electric Reliability Corporation.

power sector on issues pertaining to "joint planning, preparedness, resilience, and recovery related to events of national significance that may affect the secure and resilient supply and delivery of electricity," including cyber attacks.[79]

DHS can also provide information to support restoration operations. The ICS-CERT provides an especially important resource. Managed and operated by the DHS Control Systems Security Program and operated in coordination with the US Computer Emergency Readiness Team, ICS-CERT provides focused operational capabilities for defense of control system environments against emerging cyber threats. Specific support missions include the following:

- Responding to and analyzing control systems-related incidents
- Analyzing vulnerabilities and malware
- Developing situational awareness in the form of actionable intelligence
- Coordinating the responsible disclosure of vulnerabilities/mitigations
- Sharing and coordinating vulnerability information and threat analysis through informational products and alerts

At the state and local levels, fusion centers can provide utilities with an additional source of threat information to facilitate protection and power restoration operations. As in the case of the Kansas Intelligence Fusion Center, the presence of the National Guard at these centers can provide for especially valuable reachback to federal sources of classified threat data to share with cleared industry personnel. The Federal Bureau of Investigation and DHS can also provide valuable data to utilities through fusion centers and other sharing mechanisms.

However, fusion centers vary widely in their capacity to support post-cyber attack power restoration. Not all of them have provided for adequate representation by utility personnel during such emergency operations. They also vary in the degree to which they are building on the successful model of the Kansas Intelligence Fusion Center and capitalizing on opportunities for National Guard reachback for classified information. DHS and the Information Sharing and Access Interagency Policy Committee should encourage fusion centers to treat support for power restoration as a priority within their broader responsibilities to strengthen cyber resilience.[80] DHS could also adjust the grant guidance it provides to fusion centers to recognize and support the vital role that centers can play in strengthening the cyber resilience of the grid and other critical infrastructure sectors.

However, unless the flow of data from these disparate organizations can be integrated and provided in an efficient way, utilities could face an unmanageable number of "touchpoints" to get the assistance they need. A tightly coordinated approach will also be vital to facilitate the flow of information in the reverse direction: that is, from utilities to support organizations, so that utilities can provide samples of malware and other aspects of the cyber attack that they discover on their networks.

Progress is under way in providing for such coordinated information flows. In particular, the Cybersecurity Risk Information Sharing Program is already helping twenty operating companies (representing 65 percent of US customers) and their government partners accelerate the sharing of unclassified and classified threat information from multiple sources and develop situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection

[79] US Department of Homeland Security, *Electricity Sub-Sector Coordinating Council Charter* (Washington, DC: US Department of Homeland Security, August 5, 2013), https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf.

[80] US Department of Homeland Security, *Coordinating Federal Support for Fusion Centers* (Washington, DC: US Department of Homeland Security, August 2012), http://www.dhs.gov/sites/default/files/publications/coordinating-federal-support-for-fusion-centers-flyer-compliant.pdf.

of their critical infrastructure.[81] Utilities should play a leading role in determining how these and other information-sharing mechanisms should be coordinated and centralized to most efficiently support them. Of course, a more centralized two-way information-sharing system would also create an especially high-value target for attack. Utilities and their partners (including national laboratories overseen by DOE) will also need to focus on securing that system against efforts to disable or corrupt the flow of data.

Beyond Intelligence Support: Leveraging Government Capabilities to Assist Power Restoration

DHS, DOD, and other federal departments and agencies are rapidly expanding their capabilities to protect and restore critical government networks after a cyber attack on the United States. There is a strong possibility that the president, using Sandy as a precedent, would also direct the federal government to use these capabilities to help utilities restore power if a cyber attack disrupted the grid, especially in areas of extraordinary economic and strategic importance. But the national security context for providing such support in a cyber-induced outage would be entirely different from that created by a hurricane.

As Sandy made landfall, the president told all of his cabinet officers—including Secretary of Defense Leon Panetta—that in addition to supporting FEMA for immediate life-saving operations, the top priority for DOD would be restoring power for lower Manhattan. DOD responded accordingly. Most notably, DOD reallocated C-5A cargo aircraft away from their previously assigned mission to resupply forces in Afghanistan, instead dedicating them to transport utility trucks from West Coast utilities to the New York/New Jersey region.

But the superstorm did not strike any critical military bases or other defense infrastructure. DOD's initial Sandy after-action review noted that the department "dodged a bullet with Sandy: no Defense Critical Assets were degraded." The review also emphasized that in future catastrophes, including those caused by "cyberattacks on critical infrastructure," the department needed to prioritize its ability to ensure the continued execution of its core missions.[82]

A targeted cyber attack, and the political/military crisis that engendered it, would create issues for mission assurance and the allocation of federal cyber response assets above and beyond those created by Sandy. For example, the president might direct DOD (and perhaps even DHS cyber response assets) to prioritize the restoration of mission-essential ICSs and other systems on military bases, especially those important for military operations in the crisis region. Yet, assisting utilities that distribute electricity to those installations would also be a top priority. The same is true of the BES generators, transmission lines, and RTOs that help provide power to those distribution companies. And governors—who are responsible for the public health and safety of their citizens—would surely want to help shape national decision making on power restoration priorities.

Department of Homeland Security Support

The ICS-CERT can provide vital data on threat signatures and mitigation recommendations to support power restoration. What the ICS-CERT does *not* do is put "fingers on the keyboard" of a utility's HMI systems or other OT components to eliminate malware and conduct other power restoration operations. There are good reasons why this is the case. As is true for cross utility mutual assistance,

[81] Patricia Hoffman, letter to Tom Fanning and Fred Gorbet, August 5, 2014, http://www.nerc.com/pa/CI/Resources/Documents/Department%20of%20Energy%20Letter%20-%20Cybersecurity%20Risk%20Information%20Sharing%20Program%20%28CRISP%29.pdf.

[82] US Department of Defense, *Talking Points for Deputy Secretary of Defense: Hurricane Sandy After Action Review* (Washington, DC: US Office of the Secretary of Defense, January 10, 2013), 1.

unless OT experts are thoroughly familiar with the systems they are trying to fix, they can accidentally brick those systems in ways that will greatly complicate and delay power restoration.

It might be possible for ICS-CERT teams to partner with specific utilities so that the teams could train on each utility's OT system and develop the deployment plans and operational protocols necessary to help utility personnel conduct malware scrubbing and other hands-on restoration efforts. Staffing and training the ICS-CERT to provide such services to multiple utilities (potentially at the same time in a cyber attack) would require a significant increase in resources. At present, the ICS-CERT is staffed at such a low level that it can only deploy a handful of small fly-away teams simultaneously.[83] Building up these staff assets could provide substantial benefits for power restoration, if utilities and the ICS-CERT can agree on specific high-value support roles that the teams would play beyond their usual responsibilities for forensics assistance and other missions.

Relying on the ICS-CERT to provide such support will also require the resolution of unresolved questions as to whether (and under what circumstances) DHS employees would have the legal authority to directly reconfigure a private utility's ICSs or conduct other operations and what liability exposure the US government might have if such operations fail or go awry. Resolution of these issues should be expedited.

The Department of Energy: Key Authorities and Opportunities to Support Power Restoration

DOE does not maintain fly-away teams equivalent to those maintained in the ICS-CERT program. However, in addition to the lead federal responsibilities that DOE has to support energy restoration under ESF #12, Congress recently granted the department new emergency authorities that could prove enormously significant in responding to cyber attacks on the grid.

On December 4, 2015, President Obama signed into law the Fixing America's Surface Transportation (FAST) Act, which legislates a number of energy security initiatives. One of the provisions, Critical Electric Infrastructure Security, provides that when directed by the president, the secretary of energy can "issue such orders for emergency measures as are necessary . . . to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure" (i.e., infrastructure serving US facilities "critical to the defense of the United States" and other facilities as designated by the secretary of energy).[84] The legislation does not specify which particular actions the secretary might take within this grant of authority. Rather, Congress required that within 180 days of enactment of the bill, the secretary establish rules of procedure that ensure that such authority can be exercised expeditiously.[85]

As the secretary meets this requirement, DOE might coordinate with the electric industry not only on the procedures for issuing emergency orders but also on the types of orders that might be most valuable in the prioritized sustainment and restoration of power in a cyber event. As noted in the discussion of CONOPS for power restoration, the power industry could face significant issues in terms of whether to segment the grid and intentionally create power islands in a large-scale outage. Traditional imperatives to quickly restore power might also conflict with requirements to take grid components off-line to limit the spread and reduce the consequences of an attack. As the electric subsector examines potential restoration CONOPS and federal leaders consider measures for prioritized sustainment and restoration for defense

[83] Information provided by DHS to the author, November 3, 2015.

[84] Fixing America's Surface Transportation (FAST) Act, H.R.22, 114th Cong. (2015–2016), Section 61003, "Critical Electric Infrastructure Security," 806–807, https://www.congress.gov/bill/114th-congress/house-bill/22/text#toc-HDB4083C95A7D42688DE939127F01DF82.

[85] FAST Act.

critical electric infrastructure, close collaboration between industry and government leaders on such FAST Act implementation-related issues will be vital.

Department of Defense Capabilities: Assistance from US Cyber Command?

When President Obama met with his cabinet after Sandy made landfall and he emphasized that support for power restoration was an overriding priority for federal departments, department leaders heard his message loud and clear. But many of those departments—including DOD—had never before considered restoration of the US grid a priority mission, and they scrambled with their interagency partners to do the best they could to identify appropriate support missions and assets.

In a severe blackout caused by a cyber attack, it is possible that the president will once again turn to the secretary of defense and direct that DOD support power restoration operations. That possibility will be especially strong if the attack jeopardizes the flow of electricity to critical national security installations, including those necessary for commanding, controlling, and resupplying forces in the regional confrontation that sparked the attack. DOD, its interagency partners, and the electric industry must prepare for this eventuality and ensure that DOD assistance for post-cyber attack power restoration directly supports industry needs.

Planning for such defense support is very much a work in progress. *The DoD Cyber Strategy* (2015) provides a foundation for assessing potential DOD roles in a cyber attack on the US power grid and other critical infrastructure sectors. The strategy notes that during a conflict, adversaries may seek a strategic advantage by targeting utility ICSs and other infrastructure components.[86] The strategy also states that "DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence," which may include "loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[87] A nationwide cyber attack on utilities targeted for maximum political, military, and economic consequences would almost certainly rise to that level.

The strategy notes that, if directed by the president or secretary of defense, the US military may conduct cyber operations to blunt an attack and prevent the destruction of property or loss of life.[88] Such operations could occur both at home and abroad (including the disruption of an adversary's "military-related critical infrastructure").[89] The document does not, however, specifically address whether and how DOD might help utilities scrub malware from their networks or conduct other power restoration operations. Instead, the strategy provides a road map to advance the consideration of possible support missions but leaves key issues still to be resolved.

One issue is how DOD would provide assistance as part of the federal team. During Sandy, when President Obama told the secretary of defense that power restoration would be a top DOD priority, he added a key condition: FEMA and DHS would remain the lead federal agencies in charge of coordinating federal disaster response operations. DOD would operate strictly in support of civil authorities, rather than exercising any leadership using its own Title 10 or other authorities for homeland defense. The Defense Support of Civil Authorities operations that followed during Sandy included both support for power restoration and assistance in dealing with the consequences of the outage for public health and safety.

---

[86] US Department of Defense, *The DoD Cyber Strategy* (Washington, DC: US Department of Defense, April 2015), 2, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[87] Ibid., 5.

[88] Ibid.

[89] Ibid., 14.

A similar approach could be adopted for defense support in a cyber attack. *The DoD Cyber Strategy* calls for the department to "develop a framework and exercise its Defense Support of Civil Authorities (DSCA) capabilities in support of DHS and other agencies and with state and local authorities to help defend the federal government and the private sector in an emergency if directed." To help meet that exercise requirement, the department's Cyber Guard exercise focuses on contingencies that may require emergency allocation of DOD forces to help protect critical infrastructure under the leadership of other federal agencies.[90] Cyber Guard exercises are now conducted annually and include electric utilities as participants.

Admiral Michael S. Rogers, Commander, USCYBERCOM, emphasizes the value of Cyber Guard for advancing a shared understanding of how defense support might be provided in a cyber attack:

> We inaugurated the CYBER GUARD exercise series to test the "whole of nation" response to a major cyber incident affecting the DoDIN [Department of Defense Information Network] and U.S. critical infrastructure. USCYBERCOM offices work with experts from the Joint Staff and the joint cyber headquarters elements, Cyber Mission Force teams, U.S. Northern Command, National Guard, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), state governments, allies, and the private sector. Our defenders battle in the exercise networks against a world class "opposing force" to make this nearly three-week event as realistic as possible. The idea is to train our forces to operate as they would in an actual cyber crisis—i.e., against live opposition and alongside the federal, state, allied, and industry partners who would also have authorities and equities in such an event. Over a thousand participants, including representatives from critical infrastructure partners and National Guard teams from 16 states, practice how to collectively protect the nation along with DoD networks. Participants from the Department of Defense practice lending appropriate support to civil authorities, and doing so on a complex exercise network that takes months to fine tune in advance of CYBER GUARD.[91]

However, major issues remain to be resolved in terms of identifying specific capabilities that DOD would be prepared to bring to bear in support of DHS for power restoration. USCYBERCOM is building a Cyber National Mission Force that could have substantial capabilities to meet utility RFAs, as coordinated and assigned by DHS and approved by the secretary of defense. In particular, because the Cyber Protection Team (one of three components of the overall Cyber National Mission Force) is responsible for defending DOD networks and ICSs, it is likely to have technical expertise and deployable assets that might be useful for post-cyber attack power restoration.[92]

But the Cyber Protection Team is responsible for securing and restoring DOD systems. Whether the force could be diverted from its DOD mission to support the private sector, especially at a time when DOD assets are at risk of attack, will present a continuing policy challenge. The extent to which DOD forces can operate on utility systems by leveraging the authorities of DHS or other federal departments and agencies also presents unresolved issues.

An additional problem lies in specifying the tasks that USCYBERCOM personnel would perform to

[90] Ibid., 22.

[91] *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong. (September 29, 2015) (statement of Admiral Michael S. Rogers, Commander, US Cyber Command), 4–5, http://www.armed-services.senate.gov/imo/media/doc/Rogers_09-29-15.pdf.

[92] Cheryl Pellerin, "Rogers: Cybercom Defending Networks, Nation," *DoD News, Defense Media Activity* (August 18, 2014), http://www.defense.gov/news/newsarticle.aspx?id=122949.

support power restoration. The same constraints that limit the ability of utilities to work on each other's OT systems, which differ significantly in terms of system designs, applications, and other technical features, will also apply to military forces. Providing the utility-specific training and exercising opportunities for full-time military personnel on Title 10 status will be especially difficult. Far more promising is the possibility of providing such training for state National Guard personnel.

National Guard

The pace of power restoration after Sandy was greatly accelerated by the support missions performed by state National Guard organizations and other government agencies. Key missions and implications for post-cyber attack restoration include the following:

- ***Logistics support for restoration crews:*** During Sandy, state National Guard and DOD installations served as staging sites and base camps for utility crews providing mutual aid. By providing housing, food, and vehicle refueling and meeting the other support needs for crews from as far away as Canada, Arizona, and California, this logistical assistance was a critical enabler for industry's mutual aid system and will remain critical after other natural disasters. In contrast, large-scale logistical support will be less necessary for the specialized remediation tasks required for post-cyber attack restoration.
- ***Engineering support:*** Debris and road clearance proved crucial after Sandy for giving utility crews access to damaged grid infrastructure. These efforts, along with emergency evaluation of physical damage to bridges and other structures, will be essential after future natural hazard events of similar or greater severity. However, cyber events will not require these traditional engineering support functions.
- ***Public safety/security:*** After Sandy, utility contractors, state and local law enforcement, National Guard personnel, and other partners provided for wire guarding (site safety), flagging (traffic control), and other safety/security-related support missions. Again, cyber events will not typically necessitate such restoration support, although long-duration power outages could jeopardize public health and safety and therefore require substantial Guard resources to meet those challenges.
- ***Situational awareness:*** Utilities have substantial experience in mapping their outage areas and are currently using smart metering and other grid modernization tools to more rapidly identify where repairs are needed. As the federal lead for ESF #12, Energy, DOE attempted to support these restoration efforts by providing broader situational awareness of the availability of fuel for response vehicles and choke points in the broader flow of energy resources, as well as other types of data. DOE's after-action review of Sandy found that significant improvements are needed to provide shared real-time situational awareness of damage to the grid and associated energy infrastructure, as well as in refining estimated times of restoration (ETRs) and coordinating communication of these times to communities and government leaders.[93] An equivalent system will be required for cyber attacks. However, such a system will also have to account for the risk that the adversary will corrupt situational awareness data and the networks over which data travel.

DOE, the National Guard, and their industry partners are making significant improvements in situational awareness tools and technologies. These initiatives could provide a basis to help utilities better understand the scope and failure nodes in a cyber event if attackers disrupt their usual sources of data for making such assessments. National Guard efforts

[93] US Department of Energy, *Overview*, 7-1.

to develop advanced geospatially based displays for critical infrastructure assessments (tailored to be shared with industry) may be especially useful.

Most important, many National Guard organizations are building on their long-established support relationships with utilities in their states and are developing the sorts of utility-specific training and operational plans that could enable Guard personnel to directly support post-cyber attack restoration operations. California provides a case in point. In August 2015, Governor Jerry Brown issued an executive order to establish a Cyber Incident Response Team to partner with the private sector to support cyber threat detection, reporting, and response operations.[94] National Guard organizations in Washington State, Maryland, South Carolina, Michigan, and many other states are aggressively moving forward with their utility partners to advance similar restoration initiatives.[95]

Of course, plans for Guard assistance will be useless unless the Guard and its partners can train and exercise the pool of personnel needed to help utilities restore power after a cyber attack. The Cyber Guard exercise provides some training but only occurs once a year. The Army National Guard's annual response exercise, Cyber Shield, provides additional training and hands-on response simulations that have included students from the Guard and Title 10 Reserve personnel sitting alongside students employed by power utilities. Most notably, Cyber Shield has begun using a virtual cyber city that facilitates realistic training on power grid defense and restoration.[96] The continued development and expansion of training simulation tools will be essential to achieve the throughput needed by the National Guard, Reserves, and the utilities they will support. Development of detailed student assessment tools to measure the effectiveness of such training (and to support skill certification initiatives) will also be essential.

However, beyond providing foundational OT defense and restoration skills, preparing personnel to help restore the utility-specific ICSs will remain a challenge. Dozens of states have part-time National Guard personnel who also work for cyber-related firms. Guard leaders in Washington State, Maryland, and a growing number of other states are partnering with their local utilities to explore how these cyber-skilled personnel might provide a surge force to support power restoration operations. Another promising option proposed by an officer in the Maryland National Guard is that National Guard personnel would maintain their primary (full-time) civilian employment with electric utilities and other critical infrastructure entities while also maintaining part-time membership in the National Guard where they would receive specialized, classified training.[97]

If utilities were to hire such National Guard personnel to help operate their OT systems (or if existing utility employees were to join the National Guard), the familiarity of these personnel with proprietary software and other features of utility systems would enhance their ability to effectively restore power and put "hands on the keyboard." However, the National Guard Bureau and its partners in DOD need to continue to clarify the extent to which National Guard forces can conduct such hands-on activities in either Title 32 or Title 10 status and where additional authorities may be needed through legislative action. The ability of these National Guard forces to help defend utility networks while under state active duty,

[94] Exec. Order No. B-34-15, 3 C.F.R. (2015).

[95] See, for example, State of Michigan Executive Office, *Michigan Cyber Disruption Response Strategy* (Lansing, MI: State of Michigan Executive Office, September 16, 2013), https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.

[96] Jessica Cates, "Cyber Shield Concluded in Admiration," *Atterbury Muscatatuck*, March 27, 2015, http://www.atterburymuscatatuck.in.ng.mil/NewsMedia/LatestNews/Tabld/582/artmid/4756/articleid/25/Cyber-Shield-Concluded-in-Admiration.aspx.

[97] Victor R. Macias, "Game Changing Pivot" (master's thesis, University of Maryland Baltimore County, 2015), 14–17.

consistent with the laws and constitutions of their respective states and under the command of their governors, will need state-specific analysis as well.

Utilities seeking to rely on support from state National Guard personnel may also be in for a harsh surprise when an attack occurs: those personnel may be assigned to other duties. In periods of heightened risk of cyber attack, governors may place their National Guard forces on state active duty to help restore state IT networks and other non-utility assets. State National Guard forces may also be federalized (that is, put into Title 10 status) to serve national priorities. Indeed, significant elements of the National Mission Team workforce for USCYBERCOM may ultimately be composed of National Guard force personnel.[98] Before an attack occurs, it will be essential to deconflict these potentially competing demands on the National Guard and clarify in advance which personnel will be available to support power restoration.

Allocating Government Assistance: Coordinating Mechanisms and Criteria for Prioritization

Even during Sandy, when mutual assistance assets were plentiful and tens of thousands of National Guard and other state and federal agency personnel were available to support restoration operations, significant problems emerged in the allocation of resources to meet utility RFAs. Industry and its government partners have aggressive, far-reaching efforts under way to fill those gaps for natural hazards. The following analysis draws cyber-related lessons learned from shortfalls during Sandy and describes the ongoing improvements to address them.

[98] Sydney J. Freedberg, "National Guard Fights for Cyber Role in 2015 Budget," *Breaking Defense*, February 5, 2014, http://breakingdefense.com/2014/02/national-guard-fights-for-cyber-role-in-2015-budget/.

The Request for Assistance Process: Lessons from Sandy

Sandy and the Broader Disaster Response System

The process for allocating government support capabilities had the benefit of being based on a rock-solid foundation: that of the NRF. The NRF provides well-established guidelines for traditional disaster-response operations, including the following:

- Fundamental, doctrinal principles to guide, structure, and integrate response efforts across all levels of government and for government to coordinate with nongovernmental organizations and private sector partners.[99] In particular, the NRF is aligned closely with the National Incident Management System (NIMS), which provides the incident management system on which the framework relies and specifies the command-and-control arrangements for disaster responders.[100]
- Specific emergency support functions and (together with the *National Preparedness Goal*) core capabilities required for each function, including transportation, communications, and energy[101]
- Clear descriptions of the roles and responsibilities of federal departments and agencies, including the lead federal organization for each specific aspect of disaster response[102]
- Explicit recognition of the leading role that governors play in requesting federal assistance and the basic process by which FEMA will provide

[99] US Department of Homeland Security, *National Response Framework*.

[100] Ibid., 3–4, 30–33.

[101] Ibid., 31–36; and Department of Homeland Security, *National Preparedness Goal*, 1st ed. (Washington, DC: US Department of Homeland Security, September 2011), http://www.fema.gov/pdf/prepared/npg.pdf.

[102] US Department of Homeland Security, *National Response Framework*, 31–38.

mission assignments to federal agencies through the RFA system

The NRF has a strong grounding in US statutes that further minimize the risk that agencies will misunderstand their roles, responsibilities, and sources of funding in assisting power restoration and other disaster response operations. In particular, the Stafford Act provides "triggers" and thresholds for federal support activities and reimbursement mechanisms for disaster-response operations; in addition, it authorizes the federal government to conduct specific disaster preparedness and response activities, including the traditional restoration support missions conducted by National Guard in state active duty (and funded as authorized by the Stafford Act).[103]

The NRF also offers the advantage of being thoroughly familiar to and respected by agencies at all levels of government. Every federal department with significant roles in disaster response trains to operate within the guidelines of the NRF, NIMS, and associated plans and doctrine. The same is true of state emergency management agencies that help governors generate RFAs. Moreover, federal and state agencies—and with increasing frequency, utilities and other infrastructure owners and operators—collaborate on dozens of exercises and other capacity-building events every year to ensure they can effectively operate within the NRF. One additional factor helps facilitate these exercises and the broader familiarity with how support for utilities can go forward under the NRF: the framework is entirely unclassified.

Leveraging the *National Response Framework* for Power Restoration

Although the NRF is designed to encompass all hazards and provides a strong foundation for managing the consequences of cyber attacks (including those on public health and safety), the Obama administration has advanced an additional effort to coordinate government and private sector responses to cyber events.[104] DHS issued the interim *National Cyber Incident Response Plan* (NCIRP) in 2010 as an initial step to provide for such coordination. The interim plan lacks many of the advantages of the NRF and is poorly aligned with it. The analysis that follows identifies key problems in the interim NCIRP that should be remedied in a new cyber incident response framework and recommends how lessons learned from using the NRF during Sandy might be applied in response operations.

Shortfalls in the Interim *National Cyber Incident Response Plan*

The interim NCIRP establishes a "strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident," including critical infrastructure restoration operations.[105] The drafting of that document marked a vital first step toward meeting the challenges of responding to a cyber attack. Yet, recent exercises have identified significant shortfalls and ambiguities in the NCIRP strategic framework. The National Level Exercise (NLE) 2012,[106] which simulated a far-reaching cyber attack on SCADA networks and other critical

[103] Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 93-288, as amended, 42 USC. 5121 et seq.

[104] In addition to the NRF itself, the Bush administration issued a now-outdated 2004 annex, "Cyber Incident," to the framework. US Department of Homeland Security, "Cyber Incident Annex," in *National Response Framework*, http://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf.

[105] US Department of Homeland Security, *National Cyber Incident Response Plan*, interim version (Washington, DC: US Department of Homeland Security, September 2010), 1, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

[106] For more information, see "National Level Exercise 2012: Cyber Capabilities Tabletop Exercise," FEMA, https://www.fema.gov/media-library/assets/documents/26845.

infrastructure components, identified several key areas for improvement:

- Doctrinal and structural challenges, including time-consuming decision processes and an inability to generate viable, prioritized action plans. FEMA's report on the exercise found that "the multiple layers of coordination for cyber incidents confused participants and contributed to slow decision-making relative to the speed of the evolving cyber campaign."[107]
- Problems in accessing certain critical capabilities, including an inability to provide or procure the technical resources necessary to meet RFAs
- Ambiguities in the roles and responsibilities of various response agencies, including a lack of detail on the functions of response organizations, including those assigned to the National Cybersecurity and Communications Integration Center, the staff and senior levels of the Unified Coordination Group, the Domestic Resilience Group, the Cyber Response Group, law enforcement, and private sector owners and operators of critical infrastructure
- Uncertainties over the statutory authority for federal assistance, including how the Stafford Act might authorize federal support activities and reimbursement efforts after a cyber attack[108]

In developing a National Cyber Incident Response Framework (NCIRF) to replace the interim plan, DHS and its interagency partners will need to resolve each of these problems. However, government agencies alone will be unable to do so. Input from—and collaboration with—electric utilities and other critical infrastructure sector owners and operators will be essential to design a framework that can help them accelerate service restoration and quickly respond to industry priorities for assistance.

The NLE findings did not address an additional shortfall in the interim plan: the failure to assign governors an appropriate role in requesting federal assistance after a cyber attack and in helping to oversee response operations. Governors have primary responsibility in their states for public health and safety, both of which can be jeopardized by major power outages regardless of their cause. During Sandy, Governor Cuomo, Governor Christie, and other governors in the region were intensely focused on restoration operations for the grid and other critical infrastructure sectors. Consistent with the NRF, the governors took the lead in requesting and prioritizing federal assistance during the storm. The governors and their adjutant generals played a key role in allocating scarce National Guard resources to support utilities in restoring power. Of course, the involvement of governors in a multistate event adds a degree of political complexity to response operations, especially in the allocation of scarce federal resources and in shaping public messaging on restoration time lines and other sensitive issues.[109] That complexity is inherent in the constitutional structure of the United States and is just another coordination challenge in responding to major disasters.

Governors and federal department leaders are now exploring how to plan for such coordinated action in cyber attacks on the grid. The Council of Governors is driving that effort forward. Formally established by President Obama on January 11, 2010, the council enables governors to address issues involving the National Guard, homeland defense, and Defense Support to Civil Authorities with the leadership of

[107] FEMA, *National Level Exercise 2012: Quick Look Report* (Washington, DC: Department of Homeland Security, March 2013), 12, http://www.fema.gov/media-library-data/20130726-1911-25045-9856/national_level_exercise_2012_quick_look_report.pdf.

[108] Ibid.

[109] Susanne Craig, "Cuomo's Role in Hurricane Sandy Inquiry Foretold Fate of His Ethics Panel," *New York Times*, October 30, 2014, http://www.nytimes.com/2014/10/30/nyregion/cuomos-role-in-hurricane-sandy-inquiry-foretold-fate-of-his-ethics-panel.html?_r=0.

FEMA, DHS, DOD, and the White House.[110] The council and its federal participants have adopted the *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (2014), which provides a "framework for establishing a collaborative environment for States, territories, and the Federal government to expedite and enhance the nation's response to cyber incidents."[111]

The unity of effort initiative is specifically targeted to help resolve the issues of authorities and mission deconfliction that will otherwise impede effective post-cyber attack power restoration. To make the effort still more valuable, DOE and representatives of the electricity sector should also be brought into the response planning now under way.

Building a Cyber Response Framework: Lessons Learned from Employing the *National Response Framework* during Sandy

Although the NRF is a model of clarity, and federal departments and their sponsors had years of experience in functioning under it in events before Sandy, the scale of assistance operations required by the superstorm—and the specific RFAs that stemmed from utility power restoration operations—produced major lessons for developing and implementing a cyber response framework.

In its after-action report for Sandy, DOE noted that because of the size of Sandy and the uncertainty in where severe impacts would occur, utilities throughout the region retained crews in their own service territories as a necessary precaution. As the storm progressed northward, utilities had to assess, repair, and certify their own systems before releasing crews to areas where the storm continued to impact the electric infrastructure. Similar problems could emerge in a cyber attack on utility systems.[112]

DOE also found that during Sandy, the movement of crews and equipment within the region and within states was not adequately communicated and coordinated with state and local governments. In many cases, "states were not aware of the processes and protocols of the existing mutual aid framework which led to confusion at the local level as crews transited impacted areas."[113] Equivalent problems are likely to emerge in a targeted cyber attack and should be taken into account in designing and operating the NCIRF.

Finally, DOE emphasized the benefits of having dedicated senior leaders involved in shaping response operations. DOE found that the scale of Sandy's impact required direct CEO involvement in hurricane response, as well as direct and regular communication between CEOs and federal and state leaders. For example, the secretary of energy and governors participated in daily conference calls with CEOs of major utility companies to assess electricity restoration and conditions. These communications both aided the restoration process and provided situational awareness to the government, enabling increased coordination between the public and private sectors. Additionally, the high-level interactions led to the placement of a private sector staff at the FEMA National Response Coordination Center (NRCC). This facilitated greater access to services and resources to support restoration. Senior leaders in the field also provided senior management at DOE headquarters with high-level situational awareness.[114]

This finding has major implications for designing and operating a cyber response framework to support

[110] Exec. Order No. 13528 ("Establishing Council of Governors") (January 11, 2010), https://www.whitehouse.gov/the-press-office/president-obama-signs-executive-order-establishing-council-governors.

[111] Council of Governors, *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (Washington, DC: National Governors Association, July 2014), http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.

[112] US Department of Energy, *Overview*, 9.

[113] Ibid.

[114] Ibid., 6.

power restoration. Dedicated CEO-level participation by utilities will be essential to prioritize and shape government assistance operations. In the aftermath of Sandy, the ESCC has been formalizing procedures for CEO involvement in power restoration decisions; those efforts should be leveraged for cyber response. DHS, its federal partners, and the private sector should also assess the advantages of continuing to leverage FEMA's NRCC as an all-hazards venue for allocating and coordinating federal assistance operations, versus creating a separate cyber-only system.

Beyond Immediate Response Operations: Follow-on Phases of Power Restoration and "Grid Reconstitution"

When an adversary launches a coordinated cyber attack against multiple US utilities, power restoration operations will go forward in sequential phases. The NERC report *Severe Impact Resilience: Considerations and Recommendations* (2012) outlines a three-phased process that would occur in the aftermath of a catastrophic cyber attack on the grid.

The initial "mitigation" phase in a catastrophic outage would occur during the first days of the event and would include immediate power restoration operations. The second phase, a "new normal" period, would follow and last multiple weeks or even longer. Reattacks could occur during this new normal period and generation would remain inadequate to serve all consumer loads. The third phase would be marked by the electric system's return to normal service and reliability.[115]

Phases One and Two in a Targeted Attack

An equivalent three-phase sequence would occur in response to the less-catastrophic selectively targeted attack scenario examined in this study. However, the initial mitigation phase in a targeted attack would require restoration tasks and priorities beyond those cited in the NERC report. For example, if adversaries attempt to cut off power to critical US defense installations, and thereby disrupt their ability to conduct operations in an escalating regional crisis, prioritizing the restoration of power to those installations would be essential. Strengthening emergency power capabilities at such installations and partnering with the electric industry to improve their energy resilience could also provide a vital hedge against cyber attacks. These efforts could be extended to critical national security installations nationwide and supported by new industry–government partnership models and cost recovery mechanisms that can underwrite utility investments in cyber resilience.[116]

A targeted attack would also require specialized public messaging strategies and exceptionally close coordination by utility CEOs and government leaders in communicating with affected citizens. In weather-induced blackouts, the ETRs that utilities communicate to the public are often the focus of intense scrutiny by customers, elected officials, and the media. Establishing unity of messaging on ETRs between power companies and government leaders can help them manage public expectations and support disaster response planning and operations.

A cyber attack will present more challenging communications issues than natural hazards will, both in terms of the goals to be achieved and in the technical difficulties of providing accurate, consistent messages to the public. Adversaries are likely to launch targeted cyber attacks to achieve specific political and military effects. To advance their goals, they may seek to magnify the public's uncertainties

[115] Ibid., 14–16.

[116] Especially important in this regard, DOD is analyzing potential gaps in energy resilience in defense installations and investigating new business models that might facilitate expanded public-private partnerships to strengthen such resilience. US Department of Defense, *Energy Resilience Business Case Analysis Study*.

and concerns about the duration of cyber-induced outages and foment doubt regarding the ability of the US government to preserve the safety and security of its citizens.

US government and industry messaging will need to be designed and coordinated to counter such efforts. Communications with the public will need to account for the risk of reattacks on distribution systems that have been restored to service and the possibility that other regions may be attacked after initial restoration operations are under way. Government and industry leaders should also be prepared to explain potentially controversial restoration decisions (including the possibility of grid segmentation) that may be undertaken in restoration phases one and two. To the extent that restoration playbooks and CONOPs preplan for such options, those plans should include strategic messaging components that can be exercised along with other restoration activities.

Phase Three: Grid Reconstitution

According to the NERC report, the third phase of power restoration would be marked by the electric system's return to normal service and reliability. However, the post-cyber attack power grid will be significantly different from what it was before the initial attack. Utilities will have adopted effective protection and mitigation measures against the cyber weapons used by the adversary and will already be implementing lessons learned from the event to strengthen mutual assistance in the future.

The attack will also create both the impetus and the political opportunity for much more far-reaching changes. Just as occurred after 9/11, when al-Qaeda's attack spurred Congress and the Bush administration to adopt policies and organizational changes (including the creation of DHS) that they had previously refused to support, a cyber attack on the grid that successfully disrupts critical functions and services during a crisis will open the door to changes in the grid architecture and resilience characteristics that are now considered too politically difficult, technologically challenging, or expensive. In short: utilities and their partners will have a unique opportunity to reconstitute the grid and shift it toward a more inherently resilient structure.

Now is the time to plan for such an opportunity. In addition to accelerating the voluntary implementation of the NIST framework and other resilience recommendations developed in partnership with industry, government agencies and the private sector could also identify ambitious goals that anticipate (and ideally, get ahead of) future increases in the threat. Patricia Hoffman, the DOE's assistant secretary for the Office of Electricity Delivery and Energy Reliability (OE), has suggested a number of initiatives that might contribute to a grid reconstitution plan. One is to develop "out-of-band" technologies to monitor critical grid operations that cannot be attacked by cyber adversaries. Another is to adopt much more aggressive and far-reaching supply chain risk management policies and programs than are practical today.[117]

Given the risk that adversaries will seek to disrupt the utility communications systems on which power restoration will depend, utilities should also continue to explore initiatives to strengthen the resilience of their communications systems against cyber attack. Such measures might include the development of utility-owned and -maintained fiber optic communications. The development of last-mile technologies that can create more difficult-to-bridge gaps for cyber attackers to cross may be equally important for reconstitution strategies. Federal funding to support

[117] Pat Hoffman, "Plenary" (lecture, Resilience Week 2015 Conference, August 20, 2015, Philadelphia, PA). The RADICS initiative supports the development of a number of such initiatives, including "out-of-band" situational awareness technologies, secure emergency networks to provide communications during restoration operations, and automated threat analysis. Defense Advanced Research Projects Agency, *Broad Agency Announcement: RADICS*, 7–12.

such research and development efforts may need to be increased accordingly.[118]

It would be even better if these far-reaching improvements could be adopted before an adversary strikes. Improving the grid's resilience may even help reduce the likelihood of such an attack by increasing an adversary's uncertainty as to whether the benefits of attacking the grid would be worth the potential costs of US retaliation. However, until deterrence is certain to prevent cyber attacks on the US power grid, measures to accelerate power restoration if an attack occurs will be vital.

Conclusion

Sandy and other severe natural events have helped the electricity sector forge an impressive power restoration system for such hazards. Efforts to strengthen resilience against cyber attacks must go forward without the benefit of such real-world experience and will have to account for strikingly different restoration challenges. Nevertheless, rather than build a separate cyber-specific restoration system from scratch, utilities and their partners should pursue opportunities to adapt the existing system to meet cyber threats as well.

The first step will be to establish a design basis for post-cyber attack power restoration. Major uncertainties persist regarding the effects that cyber attacks can inflict on the grid, both because the future capabilities of adversaries are so difficult to determine and because power companies and their research partners are accelerating the development of new resilience measures. To help conduct an analysis of alternatives to determine which resilience investments are most cost effective and how they should be supported with new restoration training initiatives and exercises, it will be important to further refine our understanding of the physical damage, cascading outages, and other disruptive effects that potential adversaries will be able to create.

However, based on the targeted attack scenario described in this study, key challenges and opportunities to structure a post-cyber attack restoration system are already evident. Further exercises and collaborative planning efforts will be essential to help utilities overcome the disincentives for sharing restoration assets in cyber events. A crawl, walk, run approach to cross utility assistance may offer the most promise to build the talent pool for mutual aid and meet the technical challenges of restoring utility-specific ICSs.

Building a CONOPS to guide restoration operations will also be vital. Such a CONOPS will need to address the unique challenges of cyber threats, versus those of natural hazards, and will require supporting energy management and communications systems that can survive attacks targeted on them. Government partners can play a key role in helping industry develop and implement a cyber CONOPS. In particular, these partners may be able to provide tightly coordinated threat and remediation data to industry to support power restoration while utilities themselves lead the hands-on restoration of their own networks and grid components.

Further analysis will be required to determine whether and how DHS, the National Guard, and other potential sources of government support could provide such hands-on assistance if requested by utilities. Yet, any such assistance should be provided in ways that are consistent with the NRF and other proven, effective mechanisms for responding to RFAs. Future cyber response frameworks might be structured accordingly and used as part of the starting point to conduct an analysis of alternatives for potential government and private contractor sources of assistance to utilities.

Ultimately, however, mutual assistance between utilities will likely offer a crucial means for power

[118] Assante, Roxey, and Bochman, *The Case for Simplicity*, 6–7.

companies to supplement their own restoration capabilities. Creating the training, exercise, and governance system necessary for such assistance before a cyber attack occurs will be vital for saving lives and defending the United States if adversaries strike—and for making the grid a less tempting target in future crises.

Bibliography

All Hazards Consortium. *The Multi-State Fleet Response Initiative Working Group Workshop Report: Rapid Critical Infrastructure Restoration through Joint Integrated Planning for the Movement of Private Sector Resources in Response to Hurricane Sandy.* Frederick, MD: All Hazards Consortium, January 2013. http://www2.apwa.net//Documents/About/TechSvcs/Multi-stateFleetResponseWorkshopReport-02-21-13.pdf.

Allison, Phillip. "Cloak and Secure Your Critical Infrastructure, ICS and SCADA Systems: Building Security into Your Industrial Internet." Paper presented at Pacific Northwest Section American Water Works Association Conference, Bellevue, WA, 2015. http://www.pnws-awwa.org/uploads/PDFs/conferences/2015/Technical%20Sessions/Thursday/4_Cloak%20and%20Secure%20Your%20Critical%20Infrastructure,%20ICS%20and%20SCADA%20Systems.pdf.

Assante, Michael J., and Robert M. Lee. *The Industrial Control System Cyber Kill Chain.* Bethesda, MD: SANS Institute, October 2015. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Assante, Michael, Tim Roxey, and Andrew Bochman. *The Case for Simplicity in Energy Infrastructure: For Economic and National Security.* Washington, DC: Center for Strategic and International Studies, November 2015. http://csis.org/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf.

Atkinson, William. "Mutual Aid Comes of Age." *Public Power* 70, no. 2 (March–April 2012), http://www.publicpower.org/Media/magazine/ArticleDetail.cfm?ItemNumber=34001.

Bea, Keith, L. Cheryl Runyon, and Kae M. Warnock. *Emergency Management and Homeland Security Statutory Authorities in the States, District of Columbia, and Insular Areas: A Summary.* CRS RL32287. Washington, DC: Congressional Research Service, 2004.

Bipartisan Policy Center. *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat, A Report from the Co-Chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative.* Washington, DC: Bipartisan Policy Center, February 2014. http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf.

Cates, Jessica. "Cyber Shield Concluded in Admiration." *Atterbury Muscatatuck*, March 27, 2015. http://www.atterburymuscatatuck.in.ng.mil/NewsMedia/LatestNews/TabId/582/artmid/4756/articleid/25/Cyber-Shield-Concluded-in-Admiration.aspx.

Clapper, James R. *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee.* 114th Cong., September 29, 2015. http://www.armed-services.senate.gov/imo/media/doc/Clapper_09-29-15.pdf.

Connecticut Public Utilities Regulatory Authority. *Cybersecurity and Connecticut's Public Utilities.* New Britain, CT: Connecticut Public Utilities Regulatory Authority, April 14, 2014. http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf.

Constantin, Lucian. "Attack Campaign Infects Industrial Control Systems with BlackEnergy Malware." *PCWorld*, October 29, 2014. http://www.pcworld.com/article/2840612/attack-campaign-infects-industrial-control-systems-with-blackenergy-malware.html.

Council of Governors. *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity.* Washington, DC: National Governors Association, July 2014. http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.

Craig, Susanne. "Cuomo's Role in Hurricane Sandy Inquiry Foretold Fate of His Ethics Panel." *New York Times*, October 30, 2014. http://www.nytimes.com/2014/10/30/nyregion/cuomos-role-in-hurricane-sandy-inquiry-foretold-fate-of-his-ethics-panel.html?_r=0.

Critical Infrastructure Partnership Advisory Council. "Electricity Subsector Coordinating Council and Government Executives Meeting Agenda," June 15, 2015. https://www.dhs.gov/sites/default/files/publications/cipac-elec-scc-govt-exec-agenda-06-15-15-508.pdf.

Danzig, Richard J. *Preparing for Catastrophic Bioterrorism: Toward a Long-Term Strategy for Limiting the Risk.* Defense & Technology Paper. Washington, DC: Center for Technology and National Security Policy, May 2008. http://ctnsp.dodlive.mil/files/2014/10/Preparing-for-Catastrophic-Bioterrorism.pdf.

———. *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies.* Washington, DC: Center for a New American Security, July 2014. http://www.cnas.org/surviving-diet-poisoned-fruit#.VqvPFkajYgk.

Defense Advanced Research Projects Agency. *Broad Agency Announcement: Rapid Attack Detection, Isolation and Characterization Systems (RADICS).* DARPA-BAA-16-14. Arlington, VA: Defense Advanced Research Projects Agency, December 11, 2015. https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-BAA-16-14/listing.html.

Defense Science Board. *Task Force Report: Resilient Military Systems and the Advances Cyber Threat.* Washington, DC: Defense Science Board, January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

Donovan, Shaun. "Hurricane Sandy Rebuilding Strategy: Helping Communities Prepare for the Impacts of a Changing Climate." *The White House* (blog). August 19, 2013. https://www.whitehouse.gov/blog/2013/08/19/hurricane-sandy-rebuilding-strategy-helping-communities-prepare-impacts-changing-cli.

Edison Electric Institute. *Before and after the Storm: A Compilation of Recent Studies, Programs, and Policies Related to Storm Hardening and Resiliency, Update.* Washington, DC: Edison Electric Institute, March 2014.

———. *Mutual Assistance Enhancements.* Washington, DC: Edison Electric Institute, October 2013. http://www.eei.org/issuesandpolicy/RES/TAB%205.pdf.

———. "Spare Transformers." http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

Electric Infrastructure Security Council (2014). Electric Grid Protection (E-PRO) Handbook.

Emergency Management Assistance Compact website, http://www.emacweb.org/.

Executive Order No. 13528.

Executive Order No. B-34-15, 3 C.F.R. 2015.

Fenton, Robert. *Defense Support of Civil Authorities: A Vital Resource in the Nation's Homeland Security Missions: Written Testimony Before the House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications*, 114th Cong., June 10, 2015. http://www.dhs.gov/news/2015/06/10/written-testimony-fema-house-homeland-security-subcommittee-emergency-preparedness.

Finkle, Jim. "Exclusive: Insiders Suspected in Saudi Cyber Attack." *Reuters*, September 7, 2012. http://www.reuters.com/article/net-us-saudi-aramco-hack-idUSBRE8860CR20120907.

Fixing America's Surface Transportation (FAST) Act. H.R.22, 114th Cong. (2015–2016). https://www.congress.gov/bill/114th-congress/house-bill/22/text#toc-HDB4083C95A7D42688DE939127F01DF82.

Freedberg, Sydney J. "National Guard Fights for Cyber Role in 2015 Budget." *Breaking Defense*, February 5, 2014. http://breakingdefense.com/2014/02/national-guard-fights-for-cyber-role-in-2015-budget/.

Fugate, Craig. *Improving the Nation's Response to Catastrophic Disasters: How to Minimize Costs and Streamline our Emergency Management Programs: Hearing Before the United States House Transportation and Infrastructure Committee, Subcommittee on Economic Development, Public Buildings, and Emergency Management.* 112th Cong., March 30, 2011. http://www.fema.gov/pdf/about/programs/legislative/testimony/2011/3_30_2011_improving_the_nations_response_to_catastrophic_disasters.pdf.

Hakim, Danny, Patrick McGeehan, and Michael Moss. "Suffering on Long Island as Power Agency Shows Its Flaws." *New York Times*, November 13, 2012. http://www.nytimes.com/2012/11/14/nyregion/long-island-power-authoritys-flaws-hindered-recovery-efforts.html?_r=0.

Hoffman, Patricia. Letter to Gerry Cauley, March 14, 2013. http://www.nerc.com/news/Headlines%20DL/ES-ISAC%20Letter%2014MAR13.pdf.

———. Letter to Tom Fanning and Fred Gorbet, August 5, 2014. http://www.nerc.com/pa/CI/Resources/Documents/Department%20of%20Energy%20Letter%20-%20Cybersecurity%20Risk%20Information%20Sharing%20Program%20%28CRISP%29.pdf.

———. Plenary lecture, Resilience Week 2015 Conference, August 20, 2015, Philadelphia, PA.

Homeland Security Missions: Written Testimony Before the House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications. 114th Cong., June 10, 2015. http://www.dhs.gov/news/2015/06/10/written-testimony-fema-house-homeland-security-subcommittee-emergency-preparedness.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

ICS515: ICS Active Defense and Incident Response. Course offered by SANS Institute. https://www.sans.org/course/industrial-control-system-active-defense-and-incident-response.

IEEE Computer Society. *IEEE Guide for Information Technology—System Definition—Concept of Operations (ConOps) Document*. IEEE Standard 1362-1998. Piscataway, NJ: IEEE, March 19, 1998.

Industrial Control Systems Cyber Emergency Response Team. "Advisory: ICS-Focused Malware (ICSA-14-178-01)." Original release date July 1, 2014. https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01.

———. "Alert (ICS-ALERT-14-281-01B): Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)." Original release date December 10, 2014. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

———. *ICS-CERT Monitor*, July/August 2011 issue. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2011.pdf.

———. *ICS-CERT Monitor*, May/June 2015 issue. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf.

Keogh, Miles, and Christina Cody. *Cybersecurity for State Regulators, with Sample Questions for Regulators to Ask Utilities*. Washington, DC: National Association of Regulatory Utility Commissioners, February 2013. http://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf.

Keogh, Miles, and Sharon Thomas. *Regional Mutual Assistance Groups: A Primer*. Washington, DC: National Association of Regulatory Utility Commissioners, November 2015. http://www.slideshare.net/SharonThomas27/naruc-rmag-paper-1122015.

Macias, Victor R. "Game Changing Pivot." Master's thesis, University of Maryland Baltimore County, 2015.

Malchow, Jan-Ole, Daniel Marzin, Johannes Klick, Robert Kovacs, and Volker Roth. "PLC Guard: A Practical Defense against Attacks on Cyber-Physical Systems." In *Proceedings of the IEEE Conference on Communications and Network Security*, 326–334. Piscataway, NJ: IEEE, 2015.

Mansfield, Matthew, and William Linzey. *Hurricane Sandy Multi-State Outage & Restoration Report*. Baltimore: Maryland Public Service Commission, February 2013.

MISO. *MISO Operating Procedures*. Carmel, IN: MISO, 2015. https://www.misoenergy.org/Library/Repository/Communication%20Material/One-Pagers/One%20Pager%20-%20MISO%20Operating%20Procedures.pdf.

The Moreland Commission to Investigate Public Corruption. *Moreland Commission Report on Utility Storm Preparation and Response: Final Report*. New York: Moreland Commission, June 22, 2013. http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/MACfinalreportjune22.pdf.

National Emergency Management Association. "The EMAC Response to Hurricane Sandy." Accessed January 13, 2016. http:/www.nemaweb.org/index.php/54-em-advocate/emac-news-archive/566-the-emac-response-to-hurricane-sandy.

New York City. "Hurricane Sandy After Action Report and Recommendations to Mayor Michael R. Bloomberg." New York City, May 2013. http://www.nyc.gov/html/recovery/downloads/pdf/sandy_aar_5.2.13.pdf.

New York State Division of Military & Naval Affairs. "Hurricane Sandy After Action Review." Presentation to New York Military Forces. February 1, 2013.

North American Electric Reliability Corporation. *Cyber Attack Task Force: Final Report.* Washington, DC: North American Electric Reliability Corporation, 2012. http://www.nerc.com/%20docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf.

———. *Cyber Security Reliability Standards CIP V5 Transition Guidance: ERO Compliance and Enforcement Activities during the Transition to the CIP Version 5 Reliability Standards.* Washington, DC: North American Electric Reliability Corporation, August 12, 2014. http://www.nerc.com/pa/CI/Documents/V3-V5%20Transition%20Guidance%20FINAL.pdf.

———. "Electricity ISAC." http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

———. *Glossary of Terms Used in NERC Reliability Standards.* Washington, DC: North American Electric Reliability Corporation, September 29, 2015. http://www.nerc.com/files/glossary_of_terms.pdf.

———. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.* Washington, DC: North American Electric Reliability Corporation, 2010. http://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

———. *Industry Advisory: Preventable SCADA/EMS Events – II.* Washington, DC: North American Electric Reliability Corporation. http://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/Preventable_SCADA_EMS_Events_II.pdf.

———. *NERC Operating Manual.* Washington, DC: North American Electric Reliability Corporation, August 2014. http://www.nerc.com/comm/OC/Pages/Operating-Manual.aspx.

———. Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations.* Washington, DC: North American Electric Reliability Corporation, 2012. http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

National Governors Association. *Governor's Guide to Mass Evacuation 2014.* Washington, DC: National Governors Association, 2014. http://www.nga.org/files/live/sites/NGA/files/pdf/GovGuideMassEvacuation.pdf.

NYS2100 Commission. *Recommendations to Improve the Strength and Resilience of the Empire State's Infrastructure.* New York: Office of New York City Mayor, January 11, 2013. http://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/NYS2100.pdf.

O'Neil, L. R., T. J. Vanderhorst Jr., M. J. Assante, J. Januszewski III, D. H. Tobey, R. Leo, T. J. Conway, and K. Perman. *Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs—Summary Report.* Richland, WA: Pacific Northwest National Laboratory, July 2013. http://energy.gov/sites/prod/files/2013/12/f6/SPSP_Phase2_Summary_Final_Report.pdf.

Paletta, Damian. "NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent." *Wall Street Journal*, September 8, 2015. http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541.

Panetta, Leon. "Memorandum for Secretaries of the Military Departments: Actions to Improve Defense Support in Complex Catastrophes." Secretary of Defense Memorandum, US Department of Defense, July 20, 2012.

Pellerin, Cheryl. "Rogers: Cybercom Defending Networks, Nation," *DoD News, Defense Media Activity*, August 18, 2014. http://www.defense.gov/news/newsarticle.aspx?id=122949.

Peniston, Bradley. "Work: 'The Age of Everything Is the Era of Grand Strategy.'" *Defense One*, November 2, 2015. http://www.defenseone.com/management/2015/11/work-age-everything-era-grand-strategy/123335/.

Pennsylvania Public Utility Commission *Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities*. Harrisburg, PA: Pennsylvania Public Utility Commission. http://www.puc.pa.gov/general/pdf/Cybersecurity_Best_Practices_Booklet.pdf.

Perrow, Charles. *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books, 1984.

PJM. *Fundamentals of Transmission Operations: Conservative Operations*. Audubon, PA: PJM, October 3, 2013. http://www.pjm.com/~/media/training/new-pjm-cert-exams/foto-lesson9-conservative-operations.ashx.

Reagan, B. Jim. "Mutual Assistance: Changing a Paradigm?" Talk presented at California Utilities Emergency Association Annual Meeting, San Diego, CA, June 6, 2013. www.cueainc.com/documents/Mutual%20Assistance.pptx.

Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, 42 USC.

Rogers, Michael S. *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee*, 114th Cong., September 29, 2015. http://www.armed-services.senate.gov/imo/media/doc/Rogers_09-29-15.pdf.

Samuelsohn, Darren. "Inside the NSA's Hunt for Hackers." *Politico*, December 9, 2015. http://www.politico.com/agenda/story/2015/12/federal-government-cyber-security-technology-worker-recruiting-000330.

SERC Reliability Corporation. *Guideline: Conservative Operations Guidelines*. Charlotte, NC: SERC Reliability Corporation, May 20, 2015. http://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-%2805-20-15%29.pdf?sfvrsn=2.

Shields, Raymond. "Speech to NGAUS-2013." Speech delivered at 135th NGAUS General Conference & Exhibition, Honolulu, HI, September 23, 2013.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Stacey, Brent. *United States House of Representatives Science Subcommittee on Energy and Science Subcommittee on Research and Technology*, October 21, 2015. http://docs.house.gov/meetings/SY/SY20/20151021/104072/HHRG-114-SY20-Wstate-StaceyB-20151021.pdf.

State of Michigan Executive Office. *Michigan Cyber Disruption Response Strategy*. Lansing, MI: State of Michigan Executive Office, September 16, 2013. https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.

Stockton, Paul. "Wrap-Up: Defense Support in Hurricane Sandy." Memorandum to the US Secretary of Defense, November 27, 2012.

Uccellini, Louis. "Sandy—One Year Later." *Weather Ready Nation*, October 28, 2013. http://www.nws.noaa.gov/com/weatherreadynation/news/131028_sandy.html#.VqvIaLEo7Gg.

US Department of Defense. *Cyber Guard 14-1: After Action Report*. Washington, DC: US Department of Defense, September 2014.

———. *The DoD Cyber Strategy*. Washington, DC: US Department of Defense, April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

———. Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, Installation Energy. *Energy Resilience Business Case Analysis Study*. Washington, DC: US Department of Defense, forthcoming.

———. "History of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs: Superstorm Sandy Response Narrative," Draft, 2013.

———. *Hurricane Sandy After Action Review OASD(HD&ASA) Staff Top Ten List: What Worked Well and Needs Improvement*. Washington, DC: US Office of the Assistant Secretary of Defense, 2012.

———. *Mission Assurance Strategy*. Washington, DC: US Department of Defense, April 2012.

———. "Talking Points for Deputy Secretary of Defense: Hurricane Sandy After Action Review." Washington, DC: US Office of the Secretary of Defense, January 10, 2013.

———. *Strategy for Homeland Defense and Defense Support of Civil Authorities*. Washington, DC: US Department of Defense, February 2013. http://fas.org/man/eprint/homedefstrat.pdf.

US Department of Energy. *The DOE Energy Response Plan*. Version 1.0. Washington, DC: US Department of Energy, February 2015.

———. *Emergency Support Function #12 – Energy Annex*. Washington, DC: US Department of Energy, January 2008. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/nrf-esf-12.pdf.

———. Office of Electricity Delivery and Energy Reliability. *Overview of Response to Hurricane Sandy-Nor'easter and Recommendations for Improvement*. Washington, DC: US Department of Energy, February 26, 2013.

———. OE-30 Energy Response Organization. Washington, DC: US Department of Energy, August 2015.

———. "SPIDERS JCTD Smart Cyber-Secure Microgrids." http://energy.gov/eere/femp/spiders-jctd-smart-cyber-secure-microgrids.

US Department of Homeland Security. *Coordinating Federal Support for Fusion Centers*. Washington, DC: US Department of Homeland Security, August 2012. http://www.dhs.gov/sites/default/files/publications/coordinating-federal-support-for-fusion-centers-flyer-compliant.pdf.

———. *Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program*. Washington, DC: US Department of Homeland Security, 2014. https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.

———. *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: US Department of Homeland Security, August 5, 2013. https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf.

———. *National Cyber Incident Response Plan*. Interim version. Washington, DC: US Department of Homeland Security, September 2010. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

———. *National Preparedness Goal*. 1st ed. Washington, DC: US Department of Homeland Security, September 2011. http://www.fema.gov/pdf/prepared/npg.pdf.

———. *National Response Framework*. 2nd ed. Washington, DC: US Department of Homeland Security, May 2013. http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.

US Federal Emergency Management Agency. *Hurricane Sandy FEMA After-Action Report*. Washington, DC: US Federal Emergency Management Agency, July 1, 2013. http://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf.

———. "Hurricane Sandy: A Timeline." Washington, DC: US Federal Emergency Management Agency, April 24, 2013. http://www.fema.gov/media-library-data/20130726-1912-25045-8743/hurricane_sandy_timeline.pdf.

———. "National Level Exercise 2012: Cyber Capabilities Tabletop Exercise." https://www.fema.gov/media-library/assets/documents/26845.

———. *National Level Exercise 2012: Quick Look Report*. Washington, DC: Department of Homeland Security, March 2013. http://www.fema.gov/media-library-data/20130726-1911-25045-9856/national_level_exercise_2012_quick_look_report.pdf.

US Federal Energy Regulatory Commission. *Extraordinary Expenditures Necessary to Safeguard*. Docket No. PL01-6-00096 FERC ¶ 61,299. Statement of policy, 2001. http://www.iso-ne.com/committees/comm_wkgrps/trans_comm/tariff_comm/mtrls/2002/oct102002/A4_1466800.pdf.

US Government Accountability Office. *Civil Support: Actions Are Needed to Improve DOD's Planning for a Complex Catastrophe*. GAO-13-763. Washington, DC: US Government Accountability Office, September 2013. http://www.gao.gov/assets/660/658406.pdf.

———. *Critical Infrastructure Protection: Preliminary Observations on DHS Efforts to Address Electromagnetic Threats to the Electric Grid*. Statement of Christopher P. Currie, Director, Homeland Security and Justice, Before the Committee on Homeland Security and Governmental Affairs, US Senate. Washington, DC: US Government Accountability Office, July 22, 2015. http://www.gao.gov/assets/680/671971.pdf.

US Joint Chiefs of Staff. *Interorganizational Coordination During Joint Operations*. Joint Publication 3-08. Washington, DC: US Department of Defense, June 24, 2011.

US Secretary of Defense Memorandum. "Actions to Improve Defense Support in Complex Catastrophes." July 20, 2012.

US Senate. *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors: Report of the Committee on Armed Services.* 113th Cong., 2d sess., 2015. http://www.armed-services.senate.gov/imo/media/doc/SASC_Cyberreport_091714.pdf.

US Senate Armed Services Committee. *Advance Questions for Vice Admiral Michael S. Rogers, USN: Nominee for Commander, United States Cyber Command.* 113th Cong., March 11, 2014. http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

Walsh, David C. "Danzig: Analog Has Value in Countering Cyber Threats," *Defense Systems*, September 1, 2015. https://defensesystems.com/articles/2015/09/01/danzig-interview-cyber-defense.aspx.

Work, Robert O. *United States Cybersecurity Policy and Threats: Hearing Before the Senate Armed Services Committee.* 114th Cong., September 29, 2015. http://www.armed-services.senate.gov/imo/media/doc/Work_09-29-15.pdf.

Zimmerman, Rae. "Planning Restoration of Vital Infrastructure Services following Hurricane Sandy: Lessons Learned for Energy and Transportation." *Journal of Extreme Events* 1, no. 1 (August 2014): 1450004-1–1450004-38.

Abbreviations and Acronyms

APPA	American Public Power Association
APT	Advanced Persistent Threat
BES	Bulk Electric System
CEO	Chief Executive Officer
CIP	Critical Infrastructure Protection
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
EMAC	Emergency Management Assistance Compact
EMS	Energy Management System
ESCC	Electricity Subsector Coordinating Council
ESF	Emergency Support Function
ETR	Estimated Time of Restoration
FAST	Fixing America's Surface Transportation (Act)
FEMA	Federal Emergency Management Agency
HMI	Human-Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
NCIRF	National Cyber Incident Response Framework
NCIRP	National Cyber Incident Response Plan
NERC	North American Electric Reliability Corporation
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NLE	National Level Exercise
NOAA	National Oceanic and Atmospheric Administration
NRCC	National Response Coordination Center
NRE	National Response Event

NRECA	National Rural Electric Cooperative Association
NRF	*National Response Framework*
OT	Operational Technology
POIA	Power Outage Incident Annex
PUC	Public Utility Commission
RADICS	Rapid Attack Detection, Isolation and Characterization
RFA	Request for Assistance
RTO	Regional Transmission Organization
SCADA	Supervisory Control and Data Acquisition
USCYBERCOM	US Cyber Command

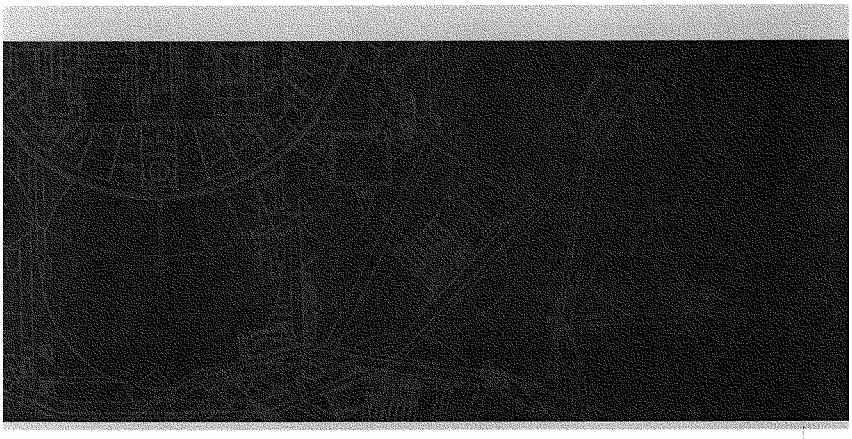
Acknowledgments

I thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Terry Boston (formerly with PJM); Gerry Cauley (NERC); Richard Danzig (Johns Hopkins University Applied Physics Laboratory); Daniel J. Elmore (Idaho National Laboratory); Tom Fanning (Southern Company); Dave Halla (NERC/E-ISAC); Debora Lavoy (Narrative Builders); Martin Libicki (US Naval Academy Cyber Operations Center); Colonel Timothy Lunderman (US Air Force); Steven T. Naumann (Exelon Corporation); Tim Roxey (E-ISAC Chief Operations Office); Matthew Schaffer (Johns Hopkins University Applied Physics Laboratory); Brent J. Stacey (Idaho National Laboratory); Mike Wallace (formerly with Constellation Energy); and Tad White (National Security Agency). I also thank the many additional reviewers who preferred to remain anonymous.

About the Author

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC, and a senior fellow of the Johns Hopkins University Applied Physics Laboratory. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support to FEMA and DHS during Superstorm Sandy, Hurricane Irene, and other disasters. Dr. Stockton also served as DOD's domestic crisis manager and was responsible for Defense Critical Infrastructure Protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors.

Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation and associate provost of the Naval Postgraduate School (NPS). Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the lead co-author of "Curbing the Market for Cyberweapons" (*Yale Law & Policy Review*, 2013) and numerous other studies.



JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

AIR WAR COLLEGE

AIR UNIVERSITY

AVOIDING THE NEXT FAILURE OF IMAGINATION:

HIGHLIGHTING OPPORTUNITIES FOR NATIONAL GUARD CYBER CIVIL SUPPORT TEAMS THROUGH AN ANALYSIS OF THE NATIONAL CYBER RESPONSE CAPACITY GAP USING 9/11 COMMISSION REPORT METHODOLOGIES

by

Gent Welsh, Colonel, WA ANG

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Robert Douglas, USAF

13 February 2014

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Colonel Gent Welsh is a United States Air Force Master Cyberspace Operations Officer in the Washington Air National Guard assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from Eastern Washington University with a Bachelor of Arts degree in English in 1995 and again in 2003 with a Master of Science in Communications.

Colonel Welsh began his career by enlisting in the United States Air Force in 1988 as a Security Policeman. He was commissioned in the Air National Guard in 1994, and has spent nearly all of his career in command assignments at the flight, detachment, squadron, and group level. His most recent assignment was as the Director, J-6, and Chief Information Officer for the Washington National Guard where he worked extensively on domestic cyberspace security matters.

Abstract

The threat of a catastrophic cyber attack occurring within the United States is a topic routinely discussed at the highest levels of our national government. However, despite the threat rhetoric, the reality is that the United States government is simply not doing enough to ensure the necessary response forces are created and available across the nation to directly assist in the domestic response and recovery from a crippling cyber attack.

This research paper outlines the current state of cyber response capability within the nation using a framework contained in the 9/11 Commission Report. Using the Commission's template outlining failures of imagination, capabilities, policy, and management, this paper breaks down these four failures from a catastrophic cyber attack response respective.

In looking at the failure of imagination, this paper explores the gap that exists between the talk of a "cyber 9/11" attack and our actual ability to respond and recover from such a devastating event. The failure of capabilities section outlines current Department of Defense and Department of Homeland Security capabilities and how those capabilities may not be adequate to support domestic state and local response requirements. The policy failure section describes the lack of adequate policy frameworks currently in place to deal with a cyber response. And last, the management failure section discusses the need to view cyber response from a "bottom up" versus "top down" perspective.

This paper concludes with a recommendation for how National Guard Cyber Civil Support Teams could be created, and a recommendation that Congress take steps to immediately address these capability gaps.

Introduction

After the event, of course, a signal is always crystal clear; we can now see what disaster it was signaling since the disaster has occurred. But before the event it is obscure and pregnant with conflicting meanings.

- The 9/11 Commission Report

Talk of a "Cyber 9/11" headlines contemporary media reports concerning our national vulnerability to a significant cyber attack. In early 2012, Senator Lieberman rose to the Senate floor to declare "Mr. President, I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber-attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens. Would-be enemies probe the weaknesses in our most critical national assets – waiting until the time is right to cripple our economy or attack a city's electric grid with the touch of a key. The system is blinking red. Yet, we fail to connect the dots – again."[1]

According to the *National Security Strategy* of May 2010, "Cybersecurity threats truly represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale."[2]

Despite the ominous warnings of cyber threats, the nation's, and specifically the Department of Defense's (DOD), collective ability to respond and mitigate the conditions resulting from a catastrophic cyber attack within the homeland is questionable. While the

current DOD Strategy for Homeland Defense and Defense Support to Civil Authorities (DSCA) mentions cyber 22 times,[3] a recent report from the Governmental Accountability Office (GAO) criticizes DOD's cyber response preparation. This report states "although DOD has prepared guidance regarding support for civilian agencies in a domestic cyber incident and has an agreement with the Department of Homeland Security (DHS) for preparing for and responding to such incidents, these documents do not clarify all key aspects of how DOD will support a response to a domestic cyber incident."[4] Additionally, the GAO finds "we recommend that DOD update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance and that such guidance should include a description of DOD's roles and responsibilities."[5]

Recent efforts by the DOD, specifically, U.S. Cyber Command, to create Cyber Mission Forces (CMF) and Cyber Protection Teams (CPT)[6] to fulfill these roles and responsibilities for responding to a domestic incident, however, are even too limited in focus. DOD's current answer to addressing the domestic cyber response concerns raised over the past year has been the creation of 39-person CPTs with the mission of "defense of the DOD Information Network (DODIN) and assistance outside the DOD when required and authorized."[7] However, the mission of these CPTs may not anticipate all the potential requirements relating to DOD and National Guard (NG) elements supporting domestic cyber responses at the state, local, and even private industry levels…the true "ground zero" where significant cyber issues will actually be managed. Left neglected are the multitude of cities, counties, states, and private sector critical infrastructure/key resources (CIKR) that will be clamoring for some type of governmental, most likely DOD and NG, assistance should they experience the devastating results of a cyber attack.

This paper examines the current domestic cyber response capacity gap from the framework of failures contained in Chapter 11 of the 9/11 Commission Report titled "*Foresight – And Hindsight.*" This report highlighted failures of imagination, policy, capabilities, and management[8] that lead up to the 9/11 attacks. This framework provides a useful lens for evaluating the current state of cyber response in the nation. This paper conducts an examination of these failures from a cyber response perspective and concludes with a recommendation for creating NG Cyber Civil Support Teams to immediately raise the level of cyber response capacity across the nation.

Imagination

While there is recognition at the national level concerning the possibility of a significant cyber attack occurring domestically in the future, the true failure of imagination lies within the unaddressed gap that exists between the rhetoric surrounding the nature of the cyber threat and our actual resource capacity to respond and recover from an attack. However, federal efforts thus far have principally emphasized efforts to prevent cyber attacks, rather than anticipate response considerations. Since 2000, federal government strategies have consistently emphasized the importance of information sharing, partnerships, analysis and warning capabilities, and coordinating efforts in cyberspace among relevant entities to minimize the impact of incidents.[9] While these information sharing and coordinating mechanisms are vitally important, they have done little to anticipate and develop actual response capacity that would be needed post-attack. In remarks before Congress in October 2013, Charley English, Director of the Georgia Emergency Management Agency, stated, "while the pre-event aspects of cybersecurity maintain a high level of importance, so too will the post-event considerations."[10]

In early 2013, both houses of Congress introduced legislation to address this capacity gap by specifically tasking the NG to develop "Cyber and Computer Network Incident Response Teams." Introduced as the "*Cyber Warriors Act of 2013*" in *Senate Bill 658* and *House Bill 1640*, these bills aim to address the cyber response capability gap by directing the DOD to "establish in each of the several States and the District of Columbia a separate team of members of the NG to perform duties relating to analysis and protection in support of programs to prepare for and respond to emergencies involving an attack or natural disaster impacting a computer, electronic, or cyber network."[11] In commenting on *Senate Bill 658* which she co-sponsored, Senator Patty Murray of Washington stated, "the *Cyber Warriors Act* is a good first step in capitalizing on the good work NG units are doing everyday across America. But there is certainly more work to be done. We must continue to provide cyber guards the tools and resources necessary to carry out their mission of safeguarding our economy, critical infrastructure, and citizens in this new era of security at home and abroad."[12]

Unfortunately, the introduction of the *Cyber Warriors Act* was not met with any enthusiasm within the DOD. According to minutes from a June 2013 meeting of the NG's Cyber General Officer Advisory Committee, "the Office of the Secretary of Defense (OSD) remains opposed to both bills or any other legislation directed towards the National Guard. OSD concerns stem from the notion that any legislation specific to the NG would take resources and focus away from the Resource Management Decision (RMD) directed CMF activation."[13]

Prospects in Congress for bill passage are equally as dim. Despite hearings on cyber response capacity,[14] the governmental transparency website, govtrack.us, gives the House bill a four percent chance of passage while giving the Senate bill a one percent chance,[15] contributing to the perpetuation of this failure of imagination. Outside of this proposed legislation, there is

little else going on nationally from an imagination perspective to address this gap between threat and response capacity on a broad scale.

Policy

While imagination is the starting point to consider when evaluating cyber response gaps, a brief examination of the current failure of policy provides a greater understanding into why cyber response processes have been difficult to establish.

The *DOD Strategy for Operating in Cyberspace* of July 2011 calls for "paradigm-shifting approaches such as the development of Reserve and NG cyber capabilities that can build greater capacity, expertise, and flexibility across DOD, federal, state, and private sector activities."[16] However, the policy failure in this strategy is the "paradigm shifting" approach has not been displayed yet with respect to building domestic cyber response capabilities within the NG, focused not exclusively on supporting DOD networks, but on supporting domestic state and local cyber response requirements.

DOD's exclusive focus on creating Title 10 (Armed Forces) capacity relative to the NG is clearly evident in a May 2013 letter from Deputy Defense Secretary, Ashton Carter, and Deputy Secretary of Homeland Security, Jane Holl Lute, to Governors Terry Branstad and Martin O'Malley, co-chairs of the Council of Governors. In this letter, DOD and DHS write, "In response to the Governors' interest in examining how the NG can serve as a cyberspace resource to the States as well as optimize NG contributions to DOD's cyber mission, DOD will spearhead efforts to share DOD's emerging cyberspace force structure and cyberspace workforce vision with the States. In a coordinated effort, U.S. Cyber Command, U.S. Northern Command, and the

National Guard Bureau (NGB) are working to build a Reserve component framework which integrates the NG into DOD's Title 10 cyberspace force structure."[17]

While approaches integrating NG forces into Title 10 structures may have merit from a DOD perspective, they do little to alleviate potential domestic "tugs of war" for these same forces when domestic cyber events occur in a state or territory. Left unaddressed are state and territory requirements to rely on these forces for an on-scene response at the actual incident site. Evidence shows current CMF proposals do not put domestic state and local response capacity as a first priority[18] calling into question DOD "paradigm-shifting" policy. This lack of formal response capability commitment may cause local cyber first responders and affected CIKR operators to question the commitment and availability of NG teams who may be subjected to mobilization or re-deployment elsewhere as part of a larger DOD response. The January 2014 report from the National Commission on the Structure of the Air Force also addressed DOD response requirements outside of Title 10 by stating, "without a better mechanism to capture the Governors' needs and other DSCA requirements, the Air Force and DOD risk building a force structure that does not adequately account for the DSCA mission."[19]

However, current DOD policy for DSCA appears to work against the notion of "paradigm-shifting flexibility" for the NG according to the recently published *DOD Instruction 3025.22, Use of the National Guard for DSCA*. This document states, "The use of the NG for DSCA will not be approved to perform DSCA operations or missions at the direct request to DOD of a State or local civil authority, or to perform activities that the Secretary of Defense determines to be a State's responsibility, including activities performed under a mutual aid and assistance agreement."[20]

In further examining the issue of policy failure from a "whole of government" perspective, *Presidential Policy Directive-21* (Critical Infrastructure Security and Resilience) signed in February of 2013 gives DHS the primary role to "coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure;"[21] however, DHS has yet to publish a final version of the *National Cyber Incident Response Plan* (NCIRP),[22] despite its existence in draft form for nearly three years.

In the draft NCIRP, DHS, in referring to State governors, writes, "Chief Executives should be prepared to request additional resources from the Federal Government, including under the Stafford Act, in the event of a cyber incident that exceeds their government's capabilities."[23] Yet, as will be explored in greater detail under the "management" section of this work, the very process for even requesting additional resources is completely absent, adding to this failure of policy.

Capabilities

While understanding current failures of imagination and policy is important for background, a deeper understanding is needed of the true dearth of response capability that is available now to respond to a domestic cyber attack.

In addressing the capabilities failure, Senator Patrick Leahy commented on the *Cyber Warriors Act* by stating that there exists "a shortfall of both capability and capacity at the federal, state, and local levels to prepare, respond, and mitigate the effects of cyber events."[24] The recently published *National Preparedness Report* by the Federal Emergency Management Agency (FEMA) in March of 2013 stated, "cyber efforts have matured over the past year, but work remains in this complex capability, including increasing state cyber capabilities."[25] Also

contained in the FEMA report were the results of the 2012 State Preparedness Report which stated, "78 percent of states and territories confirmed cybersecurity as a high-priority capability to have," but ranked cyber as the lowest rated actual capability possessed out of 31 assessed areas.[26]

Presidential Policy Directive-21, signed in March of 2013, assigned DHS the responsibility to "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure."[27] However, DHS lacks a comprehensive domestic cyber response capability as well, and would likely turn to DOD to provide response assistance according to a memorandum signed in 2010 between DOD and DHS.[28] In a catastrophic cyber attack, the federal response capacity found in DHS organizations such as the United States Computer Emergency Response Team (US-CERT) and the Industrial Control System Computer Emergency Response Team (ICS-CERT) would be considered, in military terms, a "high-demand, low-density" asset and would likely be saturated quickly with mission assignments and unavailable for a state or local response.

Since the US has not yet fallen victim to a crippling cyber attack, we can only look to ICS-CERT's current capacity to conduct assessments of CIKR across the country as an indicator of their limited capability. According to the DHS *ICS Year in Review, 2012*, between fiscal years 2010 and 2012, ICS-CERT provided on-site assessments of 31 energy companies,[29] amounting to roughly 10 visits a year across the nation. However, there are over 200 energy utility companies in the US.[30] Even if DHS had the resources to visit each one of the electrical utilities in the US in a preventative, pre-attack assessment mode, every energy utility could expect a DHS visit once every 20 years if DHS kept to its current schedule. More troubling in

this same report, DHS assessed elements of only 11 of the 18 overall total CIKR sectors in FY10, 14 of the 18 in FY11, and 15 of the 18 in FY.[31] Despite dedicating an entire publication[32] to securing the Dams CIKR sector, DHS has been able to only assess one dam in FY10 and none in FYs 11 and 12.[33] Yet according to Army Corps of Engineers figures, there are over 27,000 dams with potential cyber control systems risks operated by federal, state, local, and utilities across the country.[34]

Turning to current DOD cyber response capabilities, the *DOD Strategy for Cyberspace* outlines five key strategic initiatives including "Initiative #3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy."[35] However, this research has not found a single DOD cyber unit identified with the primary mission to partner with and assist officials and entities at the domestic (state and local) level to manage cyber attack consequences. The challenge of creating domestic cyber response capability should not be this difficult. For the DOD, creating domestic-only force structure in the NG is nothing new. Over the past 15 years, DOD, with help from Congress, has created domestic-only capabilities within the NG such as Weapons of Mass Destruction (WMD) - Civil Support Teams (CST); Chemical, Biological, Radiological, Nuclear and High Yield Explosive (CBRNE) enhanced response force packages (CERF-P); and Homeland Response Forces (HRF),[36] yet not a single dedicated domestic response capability in cyber exists today.

Lack of dedicated DOD domestic cyber capability notwithstanding, the NG is in a unique position to respond to cyber events across the US by leveraging existing emergency management relationships already well-established in each state and territory. For the past decade, the NG, through the Departments of the Army and Air Force, has been steadily investing in federally-

traced cyber missions. Currently, the Air National Guard has nine existing cyber units in numbered squadrons across the US,[37] while the Army National Guard has Computer Network Defense Teams in 53 of 54 states and territories.[38] However, this research has revealed none of these units have domestic cyber response in their federal mission description, leaving their ability to respond locally in a federal status with clear authorities given the DSCA constraints, debatable. The reality is, current NG cyber missions only have a clear trace to federal requirements, centered mostly on DODIN protection. The primacy of this federal mission focus leaves nothing clearly identified for the NG to support a domestic cyber response, contributing to a failure of capabilities, and a failure of DOD's "paradigm-shifting" approach.

Management

Finally, an examination of existing management shortfalls concerning our cyber response ability provides a basic framework for understanding that "all responses are local." Both a local capability as discussed above, and a well-understood management process are needed for an effective cyber response.

In further examining the concept that "all responses are local," the *National Response Framework* (NRF) is the key document outlining how disaster responses are managed, from the local incident site up to the federal level. According to the NRF, "most incidents begin and end locally and are managed at the local level."[39] The NRF further states, "scalable, flexible, and adaptable coordinating structures are essential in aligning the key roles and responsibilities to deliver the Response mission area's core capabilities. The flexibility of such structures helps ensure that communities across the country can organize response efforts to address a variety of risks based on their unique needs, capabilities, demographics, governing structures, and non-

traditional partners."[40] Additionally, "the NRF is not based on a one-size-fits-all organizational construct, but instead acknowledges the concept of tiered response, which emphasizes that response to incidents should be handled at the lowest jurisdictional level capable of handling the mission."[41] This building block approach to response management is an important concept to understand, because without an actual cyber response capability and management process residing at the local incident site level and building up, the NRF's envisioned methods of "tiered response" simply will not work.

The failure of management now follows that from a cyber response perspective, the aforementioned current policy and capabilities envision processes that are managed from the "top down" at both DOD and DHS, versus the "bottom up" structure outlined in the NRF. This approach concerns those looking at cyber response from a state and local perspective. According to Director English, "federal efforts must be structured in concert with states and locals rather than adopting a top-down approach."[42]

Although DHS and DOD processes appear "top-down" focused, the management processes necessary to even address cyber response issues really don't even exist currently. As evidence of these shortfalls, in a recent Congressional hearing titled "*Cyber Incident Response: Bridging the Gap Between Cyber Security and Emergency Management*," Director English stated, "79.1 percent of states interpret the consequences of a cyber-attack under statutes as 'All Hazards' versus 20.9 percent which list it as a specific hazard."[43] Despite cyber incidents now being looked at through an "all hazards" lens, there is no dedicated FEMA Emergency Support Function specifically for cyber to even allow for the procurement and allocation of any cyber response resources. The most current version of FEMA's *Typed Resource Definitions for Incident Management* in 2005 fails to list even a single resource type pre-identified for a cyber

response.[44] What this means is that if a cyber attack hit a municipal energy system today, there is no pre-defined management capability threading from the incident site all the way to the federal level to adjudicate the inevitable resource requests for cyber response and recovery capabilities.

Recommendation

The four failures of imagination, policy, capabilities, and management provide a useful framework for understanding the cyber response capacity gap that exists today. To address this gap, the National Guard, through its on-scene, local presence in every state and territory across the US, is in a unique position to cover-down on these deficits in a credible way ensuring the US develops the necessary resilience to respond and recover from a "cyber 9/11" event.

In testimony to the Senate Armed Services Committee in November of 2011, then NGB Director, General Craig McKinley, stated, "the domestic mission of the National Guard must be taken into account when making military contingency plans, when allocating scarce readiness resources, and when advising the president, the secretary of Defense, the National Security Council and the Homeland Security Council on strategies and contingency response options. Homeland defense and civil support must be at the core of our national strategy due to the changing threat environment, one that is asymmetrical and more dangerous within our homeland than at any time in our history."[45] Given this background setting, the single recommendation of this paper urges both DOD and Congress to take immediate action and establish NG cyber Civil Support Teams (CSTs) to address the cyber response capability gap outlined in preceding sections. The following sections outline a draft framework for addressing the mission, organization, and costs of a notional NG cyber CST force structure.

Mission

As a state response resource, cyber CSTs would be primarily a state domestic response asset, under the day-to-day control of the State Adjutant General. Cyber CSTs would actively build response relationships and partnerships with key CIKR sectors in their respective states and follow existing emergency management frameworks to respond to catastrophic cyber incidents. If an incident escalated, overwhelming state and local assets--including the cyber CST--the governor could request a Presidential declaration, placing the cyber CST in an ideal position to help facilitate any follow-on federal response.

Following the mission format from the existing WMD-CST model,[46] cyber CSTs would be primarily responsible for four main tasks: supporting civil authorities at a domestic cyber incident site through forensic and intrusion analysis; assessing current and projected consequences of the cyber event and resultant second and third order effects from an emergency management perspective; advising on response measures; and assisting with appropriate requests for additional support. Additionally, while in-garrison, cyber CSTs would be given additional missions to work with DHS and partner with CIKR sectors to assess threats and vulnerabilities at existing sites within that particular state or territory. The NG is already performing a mission similar to this through the DHS Vulnerability Assessment Team.[47] However, this team's mission is currently limited to assessing physical threats to critical infrastructure within a given state. The addition of a critical cyber assessment component provided by the cyber CST will strengthen this existing approach, assist DHS in increasing the capacity of CIKR sector cyber assessments, as well as build the trust, credibility, and partnerships with the day-to-day CIKR operators. All necessary processes to ensure a smooth transition from the protection/prevention

phase of the emergency management cycle to actual response and recovery should an event occur.

Organization

Absent from the congressional legislation creating NG cyber CSTs is a proposed organizational framework. Rather than replicating the CPT concept of 39 full-time personnel across all 54 states and territories, as a cyber CST concept, a smaller, less budget-intensive concept should be considered. In evaluating alternative viewpoints for team composition, we should first look to an organization that has extensive experience in managing cyber response issues: Microsoft Corporation. According to Russ McRee, Director of Threat Intelligence for Microsoft Corporation and Cybersecurity advisor for the Washington State Guard, "the premise of a NG cyber CST not only makes perfect sense, but it's the ideal construct for a specialized, rapidly deployable team to respond to significant state-specific cyber security events."[48]

Leveraging his Microsoft experience, Mr. McRee recommends, "a NG team consisting of 14 members who could deploy in four hours or less. At a high level this includes a unit commander, an executive officer or senior NCO, and twelve specialists divided into two squads. Team composition should consist of two-person teams who train and deploy together, including two teams of digital forensics and incident response specialists for attention to direct victim system analysis; two teams of intrusion analysts for activities specific to log and evidence analysis; and two teams of attack and penetration specialists to conduct hunt-like activities during events wherein they would seek out further evidence of compromise."[49] Mr. McRee's recommendations are sound, as this 14 member team represents the skill set balance (outlined in greater detail below) needed in a credible response force, without the possibility of smothering

the attack victim with uniformed military personnel, something the 39-person CPT concept must also consider.

Unlike the WMD-CSTs which consist of 22 full-time members and CPTs with 39 full-time members, the key force multiplier of a cyber CST response force would be found in its mix of full-time vs. part-time members. The cyber CST full and part-time composition mix reflects the need to constantly keep team member technical skills the most current they can be, as skill acquisition and retention simply can't be matched by having all the forces full-time. A recent memorandum titled, *National Guard Cyber Unique Capabilities,* from NGB J-6, only reinforces this point by stating, "many NG personnel possess highly valuable cyber skills acquired through their civilian employment and non-military training. These include, but are not limited to: network auditing, Supervisory Control and Data Acquisition (SCADA), hunting operations, information assurance, and other cyber/IT skills."[50] Hiring part-time members for cyber CSTs from the very corporations they work with on a daily basis is analogous to a "volunteer fire department" and only serves to strengthen the tremendous partnership opportunities between the NG and affected CIKR sectors.

Costs

Using the force mix recommended by Mr. McRee, the cyber CST composition results in four officers (two full time and two part time) and 10 enlisted (two full time and eight part time) members. According to cost planning figures obtained from the ANG for Fiscal Year 2014[51], combined salaries and benefits per team amount to $756,492 or $40,850,568 for 54 teams. Excluding salaries and benefits costs, and focusing on training, equipment, and temporary duty costs results in a per team cost of $154,000 per year or $8,316,000 for 54 teams.

A key hurdle to overcome for any NG response force is to also ensure the proper fiscal authorities exist to allow immediate response. To ensure NG CSTs have the fiscal authority to allow immediate response to cyber incidents, I recommend replicating the budget language existing WMD-CSTs use to fund their operational responses. Specifically, the Fiscal Year 2013 Budget Guidance Document for the Army National Guard includes funds for CSTs in category 121G00 that "funds all costs associated with training, exercises, common and peculiar equipment and equipment repair and sustainment, formulary costs, doctrinal development, training readiness oversight, modeling and simulation tools, general services and support services, operational deployments, and other associated costs for the WMD-CSTs."[52] Important in this language is that this fiscal guidance actually authorizes funds for operational deployments, thereby eliminating the cyber CST's need to request any additional authority prior to employment or deal with DSCA authorities issues.

Conclusion

When our national leaders talk about the possibility of a "cyber 9/11," it is important we first look back and see what lessons we may have learned from our experiences with the actual 9/11 attacks that can now be viewed through a cyber lens. We should look to these lessons and understand how they can apply now to both the cyber threat and our lack of response capacity. What these lessons show us is that we still have failures of imagination, capability, policy, and management; this time not in relation to terrorists using airplanes against buildings, but within our own nation's ability to respond and recover from a catastrophic cyber attack that politicians and senior national leaders concede is a near certainty.

From an imagination perspective, although we realize a catastrophic cyber attack is within the realm of possibility, as a nation, we have done little to create actual response forces that could make a difference where it matters at the domestic state and local level during an attack...the true "ground-zero" for cyber attacks. This is equivalent to saying firefighting is important, but never building a fire department. From a capabilities standpoint, both DOD and DHS acknowledge domestic cyber response is an important capacity; but to date, no dedicated response capability has been created to ensure those at ground-zero of a cyber attack--our state and local authorities--actually have a capability that can be used locally to support on-scene cyber response efforts. Additionally, while DOD continues to develop Title 10 cyber capabilities, none of these capabilities have the primary mission of assisting entities outside of DOD during an attack. From a policy standpoint, both DHS and DOD still struggle with developing clear policy for cyber response and understanding how limited federal capabilities could be made available to state governors. Although cyber response in many ways is just now being contemplated from an emergency management perspective, the speed of resource need and on-scene urgency that would be required in a catastrophic cyber response simply won't hold up to the bureaucracies in place now, such as requesting DSCA authority to even allow a NG federal response for a domestic cyber event. Additionally, from a management perspective, there are clear failures in anticipating cyber resource requirements at the federal level, and viewing cyber response processes from a "bottom-up" versus a "top-down" perspective.

From a NG perspective, these four failures represent yet another opportunity to develop true "paradigm-shifting" domestic Homeland Defense capabilities to protect our citizens from cyber threats in a manner similar to how the NG currently does for other threats such as hurricanes, earthquakes, floods, and WMD events. Worrying about raising a fire department

while the forest is burning is no way to plan. Similarly, exchanging business cards and developing a cyber response capability in the midst of a crippling cyber attack is no way to plan either. We can't simply rely on a pickup team the first time an event happens given the sophistication and scale of the well-documented cyber threats we face. The urgent need for dedicated NG cyber teams located in each state and territory that can quickly respond to a cyber attack, understand private industry concerns, has connections to federal level resources, and understand the interrelationships between the cyber event and the broader emergency management context has never been greater, and must be addressed now.

Notes

---

[1] Senator Joseph Lieberman, "*Introduction of Cybersecurity Act of 2012*" (floor speech, Washington, DC., 14 February 2012).

[2] The President of the United States, *National Security Strategy, May 2010* (Washington, DC: 2010), 27.

[3] Department of Defense, *Strategy for Homeland Defense and Defense Support to Civil Authorities, February 2013* (Washington, DC: 2013).

[4] United States Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Report no. GAO-13-187, February 2013 (Washington, DC: 2013), 34.

[5] Ibid.

[6] Cheryl Pellerin, "*Cybercom Builds Teams for Offense, Defense in Cyberspace,*" Defense.gov, 12 March 2013, http://www.defense.gov/news/newsarticle.aspx?id=119506

[7] United States Cyber Command J-34, *Cyber Protection Platoons*, 25 March 2013, 21.

[8] *The 9/11 Commission Report*, Washington, DC., 339.

[9] GAO-13-187, 49.

[10] Charley English, *Statement for the Record on behalf of the National Emergency Management Association* (Washington, DC., 30 October 2013), 5.

[11] United States Senate, *Cyber Warrior Act of 2013*, 113th Cong., 1st sess., 22 March 2013.

[12] Patrick Leahy, "*Leahy & Others Introduce Bill To Expand Cyber National Guard,*" 22 March 2013, http://www.leahy.senate.gov/press/leahy-and-others-introduce-bill-to-expand-cyber-national-guard

[13] Minutes of the National Guard Cyber General Officer Advisory Council, 13 June 2013, 3.

[14] United States House of Representatives, Subcommittee on Emergency Preparedness, Response, and Communications, "*Joint Subcommittee Hearing: Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management,*" (Washington, DC: 30 October 2013), http://homeland.house.gov/hearing/joint-subcommittee-hearing-cyber-incident-response-bridging-gap-between-cybersecurity-and

[15] Govtrack.us, "*S. 658: Cyber Warrior Act of 2013*" and "*H.R. 1640: Cyber Warrior Act of 2013,*" https://www.govtrack.us/congress/bills/113/s658 and https://www.govtrack.us/congress/bills/113/hr1640

[16] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: July 2011), 11.

[17] Departments of Defense and Homeland Security, Letter to Governors Terry Branstad and Martin O'Malley, 3 May 2013.

[18] United States Senate, *Senate Report 113-085: Department of Defense Appropriations Bill*, 113th Cong., 1st sess., 1 August 2013.

[19] National Commission on the Structure of the Air Force, *Report to the President and Congress of the United States*, (Washington, DC: 30 January 2013), 40.

[20] Department of Defense, *The Use of the National Guard for Defense Support of Civil Authorities*, Instruction 3025.22, 26 July 2013, 3.

[21] The White House, Office of the Press Secretary, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience: PPD-21* (Washington, DC: 12 February 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[22] Department of Homeland Security, *National Cyber Incident Response Plan: Version 1* (Washington, DC: September 2011).

[23] Ibid, H-1.

[24] Leahy, Patrick.

[25] Department of Homeland Security, *National Preparedness Report* (Washington, DC: 30 March 2013), 24.

[26] Ibid, 8.

[27] The White House, PPD-21.

[28] Department of Defense and the Department of Homeland Security, *Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity* (Washington, DC: 13 October 2010), 1

[29] Department of Homeland Security, *ICS-CERT Year in Review – Industrial Control Systems Computer Emergency Response Team* (Washington, DC: 2012), 14

[30] Bestenergynews.com, *Utility Companies list by State*, http://www.bestenergynews.com/solar/utility_co/utility_companies.php

[31] *ICS-CERT Year in Review*, 14.

[32] Department of Homeland Security, *Dams Sector: Roadmap to Secure Control Systems* (Washington, DC: 2010)

[33] *ICS-CERT Year in Review*, 14.

[34] United States Army Corps of Engineers, *National Inventory of Dams*, available at http://geo.usace.army.mil/pgis/f?p=397:5:0::NO

[35] *Department of Defense Strategy for Operating in Cyberspace*, 8.

[36]Army National Guard, *National Guard CERF-P Teams*, (Washington, DC: 20 December 2010).

[37] Air National Guard, *ANG Cyber Roadmap* (Washington, DC: May 2013).

[38] Minutes of the National Guard Cyber General Officer Advisory Council, 12 June 2013, slide 48.

[39] Department of Homeland Security, *National Response Framework, Second Edition* (Washington, DC: May 2013), 6.

[40] Ibid, 30.

[41] Ibid.

[42] English, Charley, 5.

[43] Ibid, 4.

[44] Federal Emergency Management Agency, *Typed Resource Definitions: Incident Management Resources* (Washington, DC: June 2005), http://www.fema.gov/pdf/emergency/nims/incident_mgmt.pdf

[45] Joint Chiefs of Staff, *Senate Armed Services Committee Testimony on Whether the Chief, National Guard Bureau Should be a Member of the Joint Chiefs of Staff* (Washington, DC: 10 November 2011), http://www.jcs.mil/speech.aspx?id=1658

[46] Washington National Guard, *10th Civil Support Team Capabilities Briefing* (Camp Murray, WA: Feb 2011), 3.

[47] Army National Guard, *Critical Infrastructure Protection Mission Assurance Assessments* (Washington, DC: March 2013), http://www.nationalguard.mil/media/factsheets/2013/CIP-MAA%20-%20March-2013.pdf

[48] Russ McRee (Director, Threat Engineering, Online Services Security & Compliance, Microsoft Corporation), in discussion with the author, 18 November 2013.

[49] Ibid.

[50] National Guard Bureau memorandum, National Guard Cyber Unique Capabilities, NG-J6, 11 April 2013.

[51] National Guard Bureau, *Air Force 2014 President's Budget Composite Rates* (Washington, DC: February 2013).

[52] Army National Guard, *Fiscal Year 2013 Budget Execution Guidance* (Washington, DC: 2013), 88.

Bibliography

Air National Guard, *ANG Cyber Roadmap*, May 2013.

Army National Guard, *Fiscal Year 2013 Budget Execution Guidance*, 2013.

Army National Guard, *Critical Infrastructure Protection Mission Assurance Assessments,* March 2013.

Army National Guard, *National Guard CERF-P Teams*, 20 December 2010.

Army, United States, Corps of Engineers, *National Inventory of Dams.* http://geo.usace.army.mil/pgis/f?p=397:5:0::NO

Bestenergynews.com, *Utility Companies list by State.* http://www.bestenergynews.com/solar/utility_co/utility_companies.php

Carter, Ashton, B. Deputy Secretary, Department of Defense and Lute, Jane Holl, Deputy Secretary, Department of Homeland Security to the Honorable Terry Branstad, Governor, State of Iowa and the Honorable Martin O'Malley, Governor, State of Maryland. Letter, 03 May 2013.

English, Charley, "*Statement for the Record on behalf of the National Emergency Management Association*", Washington, DC., 30 October 2013.

Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* July 2011.

Department of Defense, *Strategy for Homeland Defense and Defense Support to Civil Authorities,* February 2013.

Department of Defense, *The Use of the National Guard for Defense Support of Civil Authorities*, Instruction 3025.22, 26 July 2013.

Department of Defense and the Department of Homeland Security, *Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity,* 13 October 2010.

Department of Homeland Security, *Dams Sector: Roadmap to Secure Control Systems*, 2010.

Department of Homeland Security, *ICS-CERT Year in Review – Industrial Control Systems Computer Emergency Response Team,* 2012.

Department of Homeland Security, *National Cyber Incident Response Plan: Version 1*, September 2011.

Department of Homeland Security, *National Preparedness Report,* 30 March 2013.

Department of Homeland Security, *National Response Framework, Second Edition,* May 2013.

Federal Emergency Management Agency, *Emergency Support Functions Annexes: Introduction,* January 2008.

Federal Emergency Management Agency, *National Incident Management System (NIMS) Overview,* 2011.

Federal Emergency Management Agency, *Typed Resource Definitions: Incident Management Resources*, June 2005.

Govtrack.us, "*S. 658: Cyber Warrior Act of 2013*" and "*H.R. 1640: Cyber Warrior Act of 2013*". https://www.govtrack.us/congress/bills/113/s658 and https://www.govtrack.us/congress/bills/113/hr1640

Joint Chiefs of Staff, *Senate Armed Services Committee Testimony on Whether the Chief, National Guard Bureau Should be a Member of the Joint Chiefs of Staff*, 10 November 2011.

Leahy, Patrick, "*Leahy & Others Introduce Bill To Expand Cyber National Guard*," 22 March 2013

Lieberman, Joseph, "*Introduction of Cybersecurity Act of 2012*", Washington, D.C., 14 February 2012.

Minutes. National Guard Cyber General Officer Advisory Council, 12 June 2013.

National Commission on the Structure of the Air Force, *Report to the President and Congress of the United States*, 30 January 2013.

National Guard Bureau, *Air Force 2014 President's Budget Composite Rates*, February 2013.

National Guard Bureau memorandum, National Guard Cyber Unique Capabilities, NG-J6, 11 April 2013.

Pellerin, Cheryl, "Cybercom Builds Teams for Offense, Defense in Cyberspace," Defense.gov, 12 March 2013. http://www.defense.gov/news/newsarticle.aspx?id=119506

President. *National Security Strategy*, May 2010.

US Cyber Command. Cyber Protection Platoons, J-34. 25 March 2013.

US Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Report no. GAO-13-187, February 2013.

US House, Subcommittee on Emergency Preparedness, Response, and Communications, "*Joint Subcommittee Hearing: Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management*," (Washington, DC: 30 October 2013).

US Senate, *Cyber Warrior Act of 2013*, 113th Cong., 1st sess., 22 March 2013.

US Senate, *Senate Report 113-085: Department of Defense Appropriations Bill*, 113th Cong., 1st sess., 1 August 2013.

Washington National Guard, 10th Civil Support Team Capabilities Briefing, Feb 2011.

White House, Office of the Press Secretary, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience: PPD-21*, 12 February 2013.

BUSINESS CASE ANALYSIS FOR A WASHINGTON AIR NATIONAL GUARD CYBER-TO-PHYSICAL SYSTEMS CENTER OF EXCELLENCE

EXECUTIVE SUMMARY

As cyber threats to United States infrastructure and resources become more prevalent, a growing premium is placed on recognizing military-civilian dependencies and enhancing the security and resilience of interconnected critical infrastructure. For the last 11 years, the 262d Network Warfare Squadron (NWS) of the Washington Air National Guard has been on the leading edge of assessing and securing Cyber-To-Physical Systems (CPS) and Industrial Control Systems (ICS). Recognizing 262 NWS' leadership in this area, Air Force Space Command (AFSPC) tasked the 262 NWS to develop the Defensive Counter Cyberspace capabilities necessary to defend and secure ICS and CPS systems across the Air Force enterprise. This was in accord with the July 2016 "Annual Prioritized AFSPC Air Reserve Component (ARC) Initiatives" priority identified by the Commander, Air Force Space Command, General John E. Hyten. In response to this tasking the 262d has built and is delivering capabilities, component recommendations and operator training for integration into the US Air Force Cyberspace Vulnerability Assessment/Hunt (CVA/H) Weapon System. Further, the Governor of Washington appointed the 262d to partner with the Washington Army National Guard and Washington State Guard to perform an Industrial Control System defense assessment for State Public Utility organizations. This extensive background and experience makes the Washington Air National Guard the ideal DoD candidate to stand up a CPS Center of Excellence to enhance the cyber resiliency of our military critical infrastructure by training cyber forces within DoD as well as outside agencies. This business case analysis explores this Center of Excellence concept by explaining its purpose, discussing potential course offerings, and outlining required resources.

BACKGROUND

"It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof." PPD21 Feb 12, 2013

President Obama formulated PPD21 in 2013 in an effort to define and highlight our nation's dependency on critical infrastructure and the cyber-to-physical systems that this infrastructure relies upon. Since that time incidents such as the Ukraine power grid attacks in 2015 and 2016 have shown how these types of attacks have grown in sophistication and have become a viable instrument of national power for governments worldwide. Former Secretary of Defense Leon Panetta was prescient in his October 2012 warning of the potential for "a cyber-Pearl Harbor" when he noted that the United States was, "increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government". While this 'cyber Pearl Harbor' has not yet occurred on US soil, potential and vulnerability make such an attack extremely likely in the future.

Due to the interconnected nature of critical infrastructure, the military is similarly vulnerable to potential cyber-attacks. In their February 2016 letter to former Secretary of Defense Ash Carter, Admirals Gortney and Harris, Commanders of U.S. Northern and Pacific Commands respectively, voiced their concerns by requesting "assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed - cybersecurity of DOD critical infrastructure Industrial Control Systems." Specifically, these admirals pointed out "a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure."

In spite of this emphasis, our country continues to struggle to get the right people with the right skills on the front-lines to counter this threat. Today, the US Air Force (USAF) has only one Air National Guard (ANG) unit tasked specifically to counter cyber threats to Industrial Control and Cyber-to-Physical Systems. Air Force Space Command envisions all USAF Cyber Protection Teams eventually having the capability to evaluate Air Force Industrial Control Systems using the capabilities of the CVA/Hunt Weapon System coupled with training content developed by the 262 NWS. In terms of civilian cybersecurity preparedness, the 2016 DHS National Cyber Security Resilience review found that most state and local governments are below the recommended threshold prescribed by the NIST Cybersecurity Framework. More must be done to identify, train and employ expanded military and civilian cyber capabilities.

CPS CENTER OF EXCELLENCE

The Washington Air National Guard's 262 NWS is based at Joint Base Lewis-McChord, WA. It is comprised of 101 Citizen Airmen, 30 of which dedicated to three CPS Defense Teams.

Since 2001, the 262 NWS has been the go-to cyberspace operations organization for several high profile vulnerability and mission assurance assessments for major combat weapons systems to include a presidentially directed Cyber-to-Physical study of the Minuteman III Weapon System and the B-52H avionics data bus system. Additionally, the 262 NWS has led studies to validate ICS safeguards for Federal, State and other government agencies around the world to include the first ICS assessment on the CAOC at Al Udeid AB. Locally, under the authority of the Governor of Washington State, the 262d performed an ICS assessment on the water and power utilities of Snohomish Public Utility District (SnoPUD). Currently the 262d is tasked to evaluate life sustaining ICS systems at McMurdo Station, Antarctica and critical ICS systems for the Pentagon. Collectively, these missions have fostered a level of CPS defense expertise that is unique within DoD. It is this depth of experience as well as the civilian talent of its traditional Airmen that will form the core of the new Center of Excellence.

Finally, as part of its mission to develop a CPS defensive capability for the US Air Force, the 262d staff has designed and written a basic CPS security course and Concept of Employment for performing CPS security missions using the newly enhanced CVA/H Weapon system. While designed to serve as a CPS Specialized Mission Qualification (SMQ) within the Cyberspace Protection Teams (CPT) capabilities, these efforts by the 262d provide an outstanding foundation for expanded course offerings and present an opportunity to leverage existing efforts to get the Center of Excellence concept operating in minimal time.

PARTNERSHIPS

While benefiting from close proximity to numerous technology-centric companies that employ many of our Drill Status Guardsmen, such as Microsoft, Amazon and Boeing, the Washington Air National Guard has also benefitted from the foresight and vision of its state leadership. In January of 2016, Washington's Governor Jay Inslee announced, "an innovative partnership with the U.S. Department of Homeland Security to strengthen the protection of critical infrastructure and government services," to enable, "new ways for state government to defend against increasingly sophisticated and targeted cyber threats." While covering many aspects of his "community cyber" approach, a key enabler for this new policy was the outreach and partnerships that the Washington National Guard had already established with key governmental entities within the State.

One of the earliest of these relationships was a partnership with Idaho National Labs, one of our nation's foremost authorities on running and securing critical infrastructure supporting utility delivery systems. This partnership was one of the first of its kind between a National Guard (DoD) entity and a National Lab (DoE) entity in the area of cyber security. The result of this partnership was advanced training for Washington Air National Guard members to secure ICS and, later, developed into a methodology to assess Air Force specific systems.

While the skill sets of the WA ANG matured, so did its partnerships. Over time, these partnerships extended to a number of DoD and non-DoD entities:

- Air Force Civil Engineering Center (AFCEC): Key partner in exploring partnership opportunities between the US Air Force Civil Engineering and critical infrastructure security entities
- Pacific Northwest National Labs (PNNL): Supplied hardware and systems expertise for ICS modifications to the CVA/Hunt weapons system
- United States Cyber Command (USCC): Worked to establish/test alternative structures for a CPS defensive team; resulted directly in the ten person CPS UTC model
- Snohomish County Public Utility District (SnoPUD): Partnered to perform one of the first cyber security assessments of a State-run utility company

As Governor Inslee stated, cyber security is a community endeavor. The breadth of the relationships that the WA ANG has developed over time demonstrates its strength and leadership position within the critical infrastructure

community and highlights the diversity of skillsets and perspectives that it can bring to a future CPS Center of Excellence.

RESOURCES

As a part of the proposed Center of Excellence, the schoolhouse will consist of a squadron of 50 personnel (32 Full-time and 18 Drill Status) comprised of administrative staff and two cadre flights focused on a variety of CPS/ICS topics at varied levels. The facility will support both unclassified and classified training and consist of three classrooms, each designed for a maximum of 30 students and outfitted to deliver expert level instruction in hands-on laboratory environments.

SCHOOLHOUSE CAPABILITIES

The schoolhouse will offer three different courses that can be expanded over time, offering a total of 17 classes annually. The first course would be a USAF CPS course specific to CVA/H; second, a non-service specific CPS course tailored to government, industry and academic partners; and third,, an advanced CPS course. The first course would be our two week CPS/ICS SMQ course designed specifically for US Air Force CVA/H Weapon System operators giving them an understanding of how to provide Defensive Cyberspace Operations using the CVA/H Weapon System. Students successfully completing the CPS/ICS SMQ course would be awarded the US Air Force CPS/ICS Specialized Mission Qualification (SMQ) on the CVA/H Weapon System and would be eligible to take the advanced course. The second course is a "Joint CPS" course designed for non-CVA/H Weapon System services and external industry/academic organizations providing an understanding of processes, concepts and procedures of non-platform specific Defensive Cyberspace Operations and making them eligible for the advanced course. Finally, the advanced CPS course is designed to provide advanced techniques and procedures for operators specifically focused on Industrial Control Systems advanced topics and deeper dive discovery capabilities. The schoolhouse facility will be able to support 30 students per course resulting in a maximum throughput of 370 highly trained operators per year.
Once resources are received, the schoolhouse will be capable of offering the CPS/ICS SMQ course within approximately six months. This will provide initial throughput of 100 students in its first full year of operation. This startup period will allow the Schoolhouse to establish itself while hiring key members to continue developing a more robust curriculum for the Joint CPS and advanced courses. The schoolhouse will phase in the Joint CPS course and the advanced course at the beginning and end of the second year respectively.

The Washington Air National Guard is nationally recognized as having the preponderance of forces, capabilities, and specialized skills to establish a Cyber to Physical Systems Center of Excellence schoolhouse. We stand ready to answer the national call to strengthen the security and resilience of the nation's critical infrastructure against cyber threats.

The CHAIRMAN. Thank you, Colonel Welsh. I appreciate you summing things up from the state's perspective because I think it is critically important that we appreciate how that all comes down to the states and the responsibilities there.

There is an awful lot to talk about this morning in the spaces that you all have discussed in your comments.

Let me start with the information sharing protections, and I will refer back to the opening comments that I made with the FAST Act that we passed last Congress.

We codified DOE as a sector-specific agency for energy. We provided the Secretary with some authority to direct utility action in emergency situations. We also included provisions to protect some of the sensitive information from disclosure.

I will start with you, Mr. Highley. As the ESCC Co-Chair, how important are these provisions that we included in the FAST Act in its effort to help facilitate the timely sharing of the cyber threat information? And the CRISP program was mentioned, the Cybersecurity Risk Information Sharing Program. What we set up, is it helping at all? Is it too early?

Mr. HIGHLEY. Yes.

The CHAIRMAN. If you can speak to what we have put into law and what we are seeing as of this point?

Mr. HIGHLEY. We're very grateful for the FAST Act authority, and we're supportive of the naming of DOE, reinforcing DOE, as the sector-specific agency for electric energy and the electric sector.

That's where we want to see that. That's where the subject matter experts are, and that's where we have begun to develop a trust relationship between the CEOs that are part of the ESCC and our government counterparts.

And I think trust is the key to information sharing. We need to be able to get that information over the wall from government to industry and then back over from industry to government. That's why it was so crucial for us to see this transition go so well from one Administration to the next and see the support of Secretary Perry.

We support the direct action from DOE, in the event of an emergency. The FOIA protections are essential because this is critical infrastructure we're talking about that's at the front lines of international warfare. We can't just have that, you know, here's the most important target, be disclosed. So, we're supportive of that.

The CHAIRMAN. What about within the Quadrennial Energy Review and the recommendations there, the recommendation that FERC be granted the direct authority to promulgate the reliability standards?

I am assuming you do not support that recommendation from the QER? I would also ask you to speak to what it actually means for the stakeholder process that has been established through Congress.

Mr. HIGHLEY. So——

The CHAIRMAN. Mr. Cauley, I will ask you to comment on that as well.

Mr. HIGHLEY. We're supportive of the NERC process, because NERC has the subject matter experts that go through and vet a proposed, a proposal, from FERC before it gets to industry. It's a

very complex machine we're talking about modifying, and we think we need to rely on those experts at NERC which has both industry and government input to make sure that things are done properly.

And when you talk about making a change to the electric system, FERC has the authority now to order NERC to make a rulemaking and they can give them the timeline. So, it can happen very quickly and it has. I know Gerry will comment on that. But we're supportive of keeping that authority at NERC.

The CHAIRMAN. At NERC.

Mr. Cauley, on the stakeholder process?

Mr. CAULEY. Yes, thank you.

It's probably, I did read through most of the QER report and the one thing that I would struggle with the most is that additional authority at FERC to do standards.

When there's a crisis and something needs to be done quickly, standards are not the solution. Basically, we need to get directives and marching orders out, but not through a standard process.

To be able to have the industry expertise at the table and our process to get the best solutions for standards is very effective. We can produce a standard quickly. We were told to do the physical security standard in 90 days and we did it in 87 days. We could do a standard quicker than that. It's just really, in an emergency, it's not where you head to do emergency standards.

Thank you.

The CHAIRMAN. Thank you.

Senator Heinrich.

Senator HEINRICH. Thank you, Madam Chair.

Congressman McCurdy and also Colonel Welsh. I thought maybe you could start, Congressman, to speak just a moment about how this bottleneck in security clearances actually directly impacts your ability to manage risk and the timelines? Then, Colonel Welsh, you mentioned that you might have some thoughts on how we can speed this up? If the two of you can speak to that, together, I think that would be very helpful for all of us.

Congressman McCurdy?

Mr. MCCURDY. Sure, Senator. And everyone around here knows it is just Dave.

So, the affected policy starts at the top and one of the improvements, I think, over the last few years in the couple decades I've been dealing with this, is having the C Suite, the CEOs, the Senior Executives in corporations, focused on this issue of cybersecurity. It is not just a CIO issue. There weren't even CIOs when we started this process. So it's critical that you have senior executive level engagement.

Information sharing, in such groups, like the SEC, our groups, our safety committee within AGA and by the way, every investor-owned utility in the natural gas sector is a member of AGA. They've signed a commitment to security which is a call to action.

They are into developing the expertise within their companies and working with government and cross sector to improve our overall security. By the way, many of them, over half now, are both electric and gas combination companies.

What we find is critical is that when we have CEOs being able to sit across the table with each other and with government on a

regular basis, but then also in emergencies or in threat situations, to be able to receive information. Now we don't need to know sources and methods, the old terms we used to use. What we do need to know, though, is whether it's actionable, indirect or directly relevant for our particular environment and situation.

So it is a bit frustrating when we can't and I know a number of the CEOs on the electric side because they've been working a little bit longer through a formal process, had clearances. I've had—I was in the gang of eight, so I've had all kinds of different clearances. I currently have a DoD clearance. But if it's at a Secret level, that really doesn't help when we're talking Ukraine or some of those other issues that are timely when they came up. It's more of a backlog. I'm not in control of that. We do the reviews.

I applied. The Department is actually trying with officials, executives, to move the process. But it's, the clearance process, across government which is, kind of, fouled up there. I hate for it to be a personal example, but it's one that——

Senator HEINRICH. Actually, I think it helps for it to be a personal example.

Mr. MCCURDY. Yeah.

Senator HEINRICH. Because you are an unusual example.

Mr. MCCURDY. Yeah.

Senator HEINRICH. And if it is this tough for you, you can imagine how tough it is for lots of people in the utility industry broadly on both the electric and the gas side.

Mr. MCCURDY. Absolutely.

Senator HEINRICH. Colonel Welsh, do you want to talk about some of the advances——

Colonel WELSH. Yes, sir.

Senator HEINRICH. ——you have been able to make in Washington State?

Colonel WELSH. So, you can't have a partnership without access and sharing. Information sharing without any partners at the table is tough.

We view, from the National Guard's perspective and really in Washington State, I'll give you the Washington State case study.

Every state, every state governor has a Homeland Security Advisor. That Homeland Security Advisor has the authority in that position to sponsor folks in that state for clearances. So we have the luxury of our Homeland Security Advisor being our TAG and our Emergency Management Authority, so it, sort of, makes it easy. It's all in the same family.

But the fact that he is able to do that is a tremendous trust builder for our partners out there. Nothing makes more trust built, you can't build it without a, we'll put you in for a clearance. Here's the stuff to sign. Sorry, you'll probably get somebody asking your neighbors, you know, how you do, but it's tremendous for us. But it starts at that Homeland Security Advisor level. Again, we, sort of, wait for again, federal policy to, sort of, catch up with that.

I think on the DHS side what we would like to see is it's fairly easy to get a security clearance at the secret level. It's that TS level that takes a bit more of a nudge, and that's really the only thing that matters. You know, secret is great, as everybody knows, but it's at that TS level, you don't need to know the sources and meth-

ods, but there are some things going on out there that are of interest with our sectors.

Thank you.

Senator HEINRICH. Absolutely. Thank you for your input on that.

I yield back my remaining second.

The CHAIRMAN. Thank you, Senator Heinrich.

Senator Risch.

Senator RISCH. Well, Madam Chairman, first of all, thank you for holding this hearing.

I sit on the Intelligence Committee also and after all the testimony I hear there, I am convinced that the next major event in America is going to be a cyber event. Obviously, we are always vulnerable, not vulnerable, but at risk for some type of kinetic attack. But I am convinced that the next major one that affects large numbers of people is going to be cybersecurity.

So it is important that we do talk about this and continue to work at it because from everything we are told, we are running fast but need to run faster to catch up to where we need to be.

Mr. Bochman, thank you for coming from Idaho to testify today. Members of this Committee grow weary of me over the years explaining to them how important the INL is and being the lead lab for nuclear energy. And now, of course, we are developing our expertise on cybersecurity and becoming a lead, if not the lead.

Could you tell my fellow members here the unique capabilities that our lab has as far as moving in to that position?

Mr. BOCHMAN. Sure, thanks, Senator.

Thanks, Senator Risch, sure, you bet.

Idaho National Lab, without making too much of it, is a national——

Senator RISCH. No, go ahead and make too much.

[Laughter.]

Mr. BOCHMAN. It's a softball.

It is the nation's nuclear energy lab where nuclear energy has been developed with, I think, 52 test reactors with a small modular reactor on the way.

Senator RISCH. And the first one, of course.

Mr. BOCHMAN. I think we, I think people there figured out it was probably a better idea to monitor and control those somewhat dangerous processes from a comfortable distance, and therefore they were highly incented to create control systems that would allow them to do that. Hence, early control systems theory and practical engineering knowledge developed ahead of the curve there in Idaho.

When cybersecurity started to become on people's minds, certainly it landed in the IT universe first, but very quickly, I know folks realized that the same basic types of systems that help run banks and retail stores, et cetera, are also at the heart. They're either both at the heart of control systems operations, industrial control systems and they're also next door neighbors to them, as utilities, all our businesses and have IT organizations and with convergence.

We used to talk about convergence of information technology and operational technology as something that was coming that we needed to prepare for. The most recent SANS Industrial Control Sys-

tems Conference in Florida, two weeks ago, we all admitted, this group of subject matter experts, that it's happened, that these, now these two parts are inextricably fused and it's one of the ways adversaries can get in.

So Idaho is a great testing ground with that experience and also with its facilities. It has a test grid that has both transmission and a variety of distribution voltage assets, substations, transformers, control centers and linemen. It's integrated into the larger regional grid in a way that makes it, I'll say it this way, while we use models a lot and have to use models for a grid that's becoming ever more complex and get a handle on the types of risks that are there.

Every once in a while, maybe more than every once in a while, it behooves us to validate the models with real world testing. And it's been several times now, in my short time there, where we've run real world tests that have shown that the models we rely on so much and trust, weren't quite right and need to be tweaked and tuned. Once you do that, then you can have confidence in them again.

Senator RISCH. Could you talk just briefly about the test bed that we have there for doing that?

Mr. BOCHMAN. Yeah, well this is the—there's both the grid assets I described. There's also communications test bed assets. So you can have both.

Everyone knows a full electric indoor natural gas operation requires copious communications assets. Those are also subject to cyberattack and just as disruptive if you aim at them as if you aim at the actual industrial control systems that they support.

It's also the home of a program where, in the past, industrial control system suppliers sent equipment and the security subject matter experts did an exhaustive security assessments of it both at the hardware/software and firmware level in conjunction with the suppliers to give them feedback on how they might harden and build more secure systems in the future.

In my testimony, there's a call now from the Section Nine utilities to, in some form, bring about a modernized version that fits the purposes of the Industrial Internet of Things (IIoT) and world in which we live in. And so, I'll stop there.

Senator RISCH. Okay. Thank you, Mr. Bochman.

Thank you, Madam Chair.

The CHAIRMAN. Senator Manchin.

Senator MANCHIN. Thank you, Madam Chairman.

I will be quick.

[Laughter.]

Thank you, Madam Chairman, I appreciate it very much.

Thank all of you for coming.

My concern is reliability, and I think this first question will go to Mr. Cauley. Today our reliability organizations, electric utilities, are tasked with maintaining our electric grid in an increasingly challenging environment. As you all know, a perfect storm of factors has put baseload units at risk and states are more frequently using outer markets solutions to rescue units and to ensure their citizens and businesses have reliable, affordable electricity.

In the meantime, aging infrastructure, extreme weather events, the threat of cyberattacks, rapidly changing fuel mix and over reg-

ulations are increasingly testing our nation's electric grid. Several times throughout the month of January in 2014, the upper Midwest and mid-Atlantic experienced temperatures below zero. The Eastern portion of the PJM grid flirted with rolling blackouts.

On January 7th, a winter record was set with 141,132 megawatts of electricity being used. PJM is the nation's largest grid operator, basically overseeing 180,000 megawatts, and that's cutting it pretty close.

Interestingly, following the winter of 2014, AEP reported that nearly 90 percent of its coal plants scheduled for retirement ran during the Polar Vortex. If not for that, there would have been rolling blackouts. Coal helped keep the lights on, as we know.

Last week PJM released a report that said it could keep the lights on with the generation portfolio that is 86 percent dependent on natural gas. Current installed capacity, this is their actual figures, it is 33 percent of coal, 33 percent natural gas, 18 percent nuclear and 6 percent renewable. But more of that coal is going to be retired.

So my question would be this. I understand that your organization's reliability assessment from last year did not even flag PJM as having major near-term reliability issues, but I have to ask, is PJM correct? It seems highly risky for them to depend 86 percent on one fuel in an environment when all we talk about is fuel diversity.

Mr. CAULEY. Thank you, Senator, for that question.

As a reliability engineer for 37 years, I think one of my most important factors is a diversity of our fleet and a diversity of our fuel mix. And it is a concern. We've done a number of studies over recent years on the changing resource mix and its impacts on reliability. One of those——

Senator MANCHIN. Do you think PJM is correct?

Mr. CAULEY. I think currently, PJM——

Senator MANCHIN. 86 percent?

Mr. CAULEY. ——does have a very robust supply, capacity supply, in the near-term years.

The one concern I would have with PJM is the dependence on gas. And the concern there is, not so much the adequate amount of gas, but the dependence on gas infrastructure and supply during times of extreme weather when you'd be competing.

Senator MANCHIN. You would be concerned about the reliability, putting all your eggs in one basket?

Mr. CAULEY. Yes, exactly.

Senator MANCHIN. What do regulators need to do to help move natural gas into a position where it can serve as a baseload?

I know that the pipeline, I know the things, the pressures can freeze up. I have known all of that.

We are very blessed in West Virginia. We have a little bit of everything, coal, gas, wind, solar. We try to do it all, but throwing all your eggs in one basket.

Here is my problem. I have not spoken to one CEO of a major utility that believes that they have the right mix in their energy portfolio. Not one. They think they have been forced because of what we have done here, forcing them in a direction that reliability is not demand. FERC is not even looking at reliability as their re-

sponsibility. What happens when the system collapses and goes down? Who gets blamed?

Mr. CAULEY. Me.

[Laughter.]

Senator MANCHIN. Oh, okay.

Mr. CAULEY. Well, I will be one of the folks. But it is creating some difficulty, and that's why we're working hard to make sure we get that information out.

You know, one of the challenges is newer, inverter-based generators like renewable solar and wind don't have the rotating mass and the stability of larger units. So that creates a reliability challenge. We do see stability margins starting to shrink, so what we're trying to do is make sure everyone has the information needed to make the best decisions going forward.

Senator MANCHIN. I am sorry, sir, my time is running short.

This one is for Mr. Highley. In the U.S., approximately six percent of electricity is lost when it is transported from a generation facility across transmission distribution lines to consumers. Our transmission and distribution lines waste enough energy each year to power more than two million homes for one month. Each year they lose that much power.

The Department of Energy in the past did a significant amount of work on superconductive materials in an effort to reduce transmission line losses. This research has apparently not led to any significant breakthroughs. If we are going to become more energy efficient, we need to improve these transmission distribution of electricity.

Mr. Highley, what is the industry doing to improve the efficiency of electricity transmission and distribution lines? And do you expect any developments in the near term that will lead to dramatic line loss reductions?

I am to understand that there are so many new products on the market we have not used yet.

Mr. HIGHLEY. As a CEO of a member-owned system, I work for my members and I am absolutely incented to save every dollar I can for them. And if I could save them money by using those technologies for transmission distribution, we would be doing it. We don't see it as cost-effective today to deploy that.

Senator MANCHIN. To deploy the new technology?

Mr. HIGHLEY. Correct. If it was—in the areas where it's cost-effective——

Senator MANCHIN. So you are saying the six percent loss is more——

Mr. HIGHLEY. Is——

Senator MANCHIN. ——cost-effective than buying the new equipment?

Mr. HIGHLEY. Correct, correct in terms of life cycle costs.

Senator MANCHIN. So basically our whole——

Mr. HIGHLEY. I have to face the people who pay the bill every month. That's my Board of Directors.

Senator MANCHIN. I understand that. So I would say that basically all of——

Mr. HIGHLEY. They're my——

Senator MANCHIN. ——those senators who have been really on energy efficiencies that we have been trying to do here is all for naught when it comes down to cost?

Mr. HIGHLEY. It's just an economic choice.

Senator MANCHIN. I understand.

Mr. HIGHLEY. Yes, sir.

Senator MANCHIN. I understand.

Thank you.

The CHAIRMAN. Thank you, Senator Manchin.

Senator Cassidy.

Senator CASSIDY. I want to congratulate you all. I have never seen a collection of testimony with more acronyms, outside of maybe, Department of Defense. It was quite remarkable. And as a rule, they did not overlap. It wasn't as if I learned it here and then I would see it there, so good job, guys.

Ms. Hoffman, let's start off with that which we have not yet discussed, the electromagnetic pulse (EMP) resilience. Now that is not related to cyberattacks, that is just the sun decides to send off something one day.

I was not clear from your testimony, and you may have said it and I just did not follow, to the degree that we are now positioned to robustly endure such an electromagnetic pulse from either a military or the sun. I think I understand it could be either, right? How are we positioned to withstand that?

Ms. HOFFMAN. So thank you, Senator, for the question.

Electromagnetic pulses and GMD disturbances are basically electromagnetic disturbances that will affect not only the electric sector but multiple sectors in the United States.

Within the utility sector, we have taken an aggressive posture of looking and investigating further the electromagnetic issues. The Department has partnered with the Electric Power Research Institute and developed a strategy for looking at EMP.

Senator CASSIDY. I have limited time, so how, if either EMP was discharged in the atmosphere or the sun sent off such an issue, if you will, how well are we now positioned to respond to it?

Ms. HOFFMAN. So, it would depend where it was set off in the atmosphere. It would have multiple effects on transformers and components on the system.

There is a need to do some additional hardening on the system to mitigate some of those effects. But a lot of the discussions are what is the strategy and what is the most cost-effective solution to implement?

Senator CASSIDY. I am not sure I am getting an answer to my question, but implied, is that we are not there yet.

Ms. HOFFMAN. We are still working toward what is the best solution for the sector.

Senator CASSIDY. And so, if we are still working toward what is the best solution it suggests to me we have not yet implemented anything.

Ms. HOFFMAN. No, the industry has implemented some solutions. There have been specific utilities that have looked at shielding, hardening of substations. So there has been progress with respect to some mitigation measures.

Senator CASSIDY. Okay, but still I am guessing vulnerability. Again, it is some. You are speaking in fractions. You are not speaking in significant fractions. We are 50 percent of the way there is not what I am hearing. I am hearing some have done something.

Ms. HOFFMAN. Some, yes, utilities.

Senator CASSIDY. Colonel Welsh, you speak of failure of imagination. Now, it is a little bit, you know, existential. How do you imagine the future?

I remember being in Israel and somebody came up, some young whiz kids came up, with some software that used an eye to imagine where in software would be a vulnerability and to anticipate what would be a response. Maybe that is how we imagine, but I was not sure how should we imagine?

I saw your testimony, we need to have a robust response and the guy from Johns Hopkins on my staff gave me something that he has written also using National Guard as part of that response. But I guess my question is how do we imagine where the next cyberattack would be from?

Colonel WELSH. Well, I think that the failure of imagination covers a wide spectrum, so my concern on the failure of imagination is we've now acknowledged that a cyberattack is possible, but huge gaps in capabilities, you know, at the federal level, at the state level.

Senator CASSIDY. As I read your testimony, again, I am skimming it, I apologize, because there is much you did not say, it was written, so I am skimming that what you wrote and spoke of a failure of imagination as it regards management.

But is there a way to anticipate from whence the attack comes because, again, something else I read said that the folks who are going to attack us will probably save their best stuff for, you know, they are not going to tip us off as to what their most effective attack would be.

Colonel WELSH. Correct.

I think there are certain countries out there that we know we can potentially expect some interest from now and in the future. But again, back to the failure of imagination. It is, you know, I think we have decided that we can be attacked, but there is not much more imagination that is happening in terms of response and recovery. That is really where my concern is right now.

Senator CASSIDY. Response and recovery.

Colonel WELSH. Correct.

Senator CASSIDY. Is there a way to anticipate what the attack itself would be, beyond the say, eye, that perhaps I was exposed to in Israel?

Colonel WELSH. Maybe I'm not completely clear on your question, Senator.

Senator CASSIDY. Gentlemen, you seem to be——

Mr. BOCHMAN. If you don't mind, Senator.

Yeah, there's definitely ways to anticipate, and I'd say that's happening every single day.

If we're talking about a game changing cyberattack on U.S. infrastructure, the one it sounds like you're teasing out, we're looking for, we're always looking for that. But things of a lower order of impact are happening every day and people are monitoring them.

They're identifying where traffic is coming from. They're monitoring signatures and behavioral abnormalities and jumping on them and protecting some things, blocking some things, not responding later on.

Senator CASSIDY. So you can look at a signature of an attack and therefore block something from that particular signature from thenceforth, sort of thing?

Mr. BOCHMAN. Yes, that's business as usual.

Senator CASSIDY. Gotcha.

Mr. BOCHMAN. That's happening now, fairly broadly. And I would imagine, I could say on behalf of the energy sector, that's happening broadly.

Senator CASSIDY. And quickly, because I am almost out of time.

Mr. BOCHMAN. Sure.

Senator CASSIDY. You mentioned this, kind of, paradigm shifting attack and that is what I was getting at.

Mr. BOCHMAN. Right.

Senator CASSIDY. How do we anticipate that?

Mr. BOCHMAN. Ah, to your point, if it's done well, we'll have a hard time anticipating it.

Senator CASSIDY. Okay.

I yield back. Thank you.

The CHAIRMAN. Thank you.

Senator Stabenow.

Senator STABENOW. Thank you very much, Madam Chair, and thank you to all of you for your testimony. As we talk about cyberattacks, of course, we are being attacked right now through our communication systems and so on, so this is a very important conversation, as we look at capabilities and what could happen, what is happening, what will happen.

Mr. Bochman, I think you talked a little bit about, or you have included in your testimony a little bit about, something that I heard from a cybersecurity expert at the University of Michigan who suggested to me that we need to move away from the checkbox compliance mentality when it comes to securing our energy infrastructure and move toward building cybersecurity into the very fabric of our energy systems. For example, firewalls and anti-virus software described to me as merely afterthoughts and add-ons, and what we need is to be building security into the system.

What is being done to transition toward an approach that fully integrates cybersecurity practices and technologies into the systems that are so critical to the economy and national security?

Mr. BOCHMAN. I appreciate the question, Senator Stabenow.

First of all, in defense of checkboxes and mandatory compliance regimes that have, I think, demonstratively improved the security of the grid in the United States, you've got to achieve a baseline level of hygiene first before you can start thinking about playing even more advanced forms of defense.

Hygiene is what you get when you, if you, adhere to the recommendations of say, the SANS top 25 security controls or the NERC CIPs or the C2M2 maturity model from DOE. We're trying to have people make sure that, it's kind of like the analogy for folks is, you know, you brush your teeth and you take vitamins and you eat well and get exercise so that you don't fall prey to all manner

of different infections and bugs that could slow you down or worse, right? You want to, at least, be there with a level of hygiene. So, I'm responding to the, I think, compliance or checkbox mentality thing.

In terms of building security in, yes, every security professional in their earliest days says, we need to make sure that we don't try to bolt security on after the facts, after something is deployed because that's both more expensive and less effective than it is to just get it right the first time when you design it, at the design stage, right? The challenge is so that's mom and apple pie for security folks.

The problem is with the energy sector, it's true in all sectors, but if you're more IT you're used to replacing products on a fairly regular basis. You know, your laptop is giving you trouble after a year, or two, or three. It's time for a new one anyway, even faster sometimes for cell phones and other technologies.

With assets that are deployed in industrial applications like the grid, like natural gas, the way we buy those systems and budget for them expects that they will be operational for 10, 20 or 30 years or at least that's the way it's been up until now. And so, once that thing has been designed, purchased, deployed and now you're on maintenance cycle, you live with that thing. And so, bolt on, bolting on security, adding it after the fact, is your only choice.

I think, though, to conclude, a strong push this is something that, I think, all of us here and Senators as well, the Committee could do, is it's almost like the oath, vow to do no more harm. If we could start to have more rigorous, I won't say enforcement, but encouragement, incentivization, is the right word, to help people get it right the first time on the next generation of products before those are rolled out. I think that would be a demonstrable sign of progress.

Senator STABENOW. Thank you.

Ms. Hoffman, thank you for being here. Distributed energy systems are notable for their efficiency and their flexibility. However, in terms of cybersecurity, what are the benefits and risks to having a distributed energy network and what does an increasingly decentralized network mean for the government and industry's role in combating cyber threats?

Ms. HOFFMAN. So, thank you, Senator.

Distributed energy resources are both, provide a value and a risk, as you have mentioned.

From the value side of it, it brings generation closer to the load or closer to where demand is so it can provide consumers with a greater sense of resilience and reliability by being closer to where the customers are demanding that energy. It also provides a great diversity and resources from solar, from distributed solar, to natural gas generation and onsite generation. So it does provide that diversity.

On the security side of things, though, it's still another generation asset that has communications and controls, and one needs to look at building security into supply chain or generation assets as part of the system. So, it's very important that even if you're a solar manufacturer or you're a distributed energy manufacturer, that if you have a control system and you have a computer or any

sort of computer-aided control, you really need to embed cybersecurity into those devices.

Senator STABENOW. Thank you very much.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Stabenow.

Senator Wyden.

Senator WYDEN. Thank you, Madam Chair.

It has been an excellent panel. What is striking is how pervasive this challenge is. I am on the Intelligence Committee. We have cyber threats there. I am on the Finance Committee, and we are concerned about our data with respect to our taxes. And then, of course, we are concerned about the energy grid. So I want to, sort of, try to touch on several pieces of the puzzle this morning. I think I am going to start with you, Mr. Cauley.

First, I am particularly interested in this concept of red teaming because we saw this report coming from Houston where essentially a team of hackers, for a couple hundred bucks, got into a Houston oil refinery. Basically, they broke through an electric lock. They installed a small credit card-sized device to penetrate the company's control systems.

I think the government ought to be involved in red teaming. What do you think of that concept?

Mr. CAULEY. Well, I think one of the things that the NERC standards does is require the electric companies to do vulnerability testing which includes red team penetration tests and things like that to the critical systems. And I think part of our risk approach on our standards is that they're not prescriptive but tell people what they need to do.

Senator WYDEN. I guess I would like to hear if you think more should be done on this.

Mr. CAULEY. I think more should be done, could be done, and I think partnering with government to support that would be useful.

Senator WYDEN. Good.

Let's hold the record open on that point because I would like to hear, given the fact that you think more needs to be done, what additional work you think would make sense. Okay? Could you get that to us, say, within, say, 10 days?

Mr. CAULEY. Yes, yes, sir.

Senator WYDEN. Very good.

One other question for you and one point just with respect to the group. I have been trying to assess our witnesses' position on strong encryption, because I think strong encryption is vitally important to the security and well-being of the American people and certainly the energy grid. There are people around here who would be very interested in weakening strong encryption. I have made it clear that I will filibuster any bill that weakens strong encryption because it will leave Americans less safe.

If any of you have views you would like to advance to the contrary, I would like to see that in writing as well. In other words, if you do not agree with the notion of how important strong encryption is, I would like to have anybody share their views as to why we should not be for that.

The last point I want to make, Mr. Cauley, goes again, back to you, and it really involves the Internet of Things.

Last year, James Clapper, who was then the Director of National Intelligence, talked about how the Internet of Things was going to play a bigger and bigger role as it relates to surveillance and monitoring and location trackers. I would be interested in wrapping up this round of questions, we understand the important role that the North American Electric Reliability Corporation has, in energy lingo that is NERC. I would be interested in your wrapping up, if you could explain a potential role for NERC as we try to address the Internet of Things and ensuring that we prove, as is my guiding philosophy, that security and privacy are not mutually exclusive, that smart policies can give us both. What kinds of things could this NERC outfit, the North American Electric Reliability Corporation, help us with as we try to come up with a smart policy given the challenge with the Internet of Things?

Mr. CAULEY. Well, the distribution system, the Internet of Things we see, largely at the customer distribution level, are not really within NERC or FERC's purview at the federal level.

Senator WYDEN. But they could give advice.

Mr. CAULEY. They do create a significant risk to the bulk power system and the denial of service attack, that we saw last October, could inflict harm on the bulk power system. So we are very concerned about making sure that distributed systems and customer systems are not easily hacked and captured and become a weapon in and of themselves. Heavy encryption and protection of those systems and making sure that we work with vendors to make sure that they're not easily hacked is our focus.

Senator WYDEN. If you could give us additional suggestions with respect to NERC and if there are other organizations that could do that work, I would be very interested in it because I have not yet seen a government or an entity like NERC get this right yet and it is obvious because it is an incredibly challenging area.

Could you get us any thoughts you have, say, since I was looking at it for the next 10 days, on how they and other bodies could help us tackle the Internet of Things in this manner that would show that a smart policy means that security and liberty are not mutually exclusive, that you can have both. Is that agreeable?

Mr. CAULEY. Yes, sir, we'll do that.

Senator WYDEN. Great, thank you.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Wyden.

Senator Hoeven.

Senator HOEVEN. Thank you, Madam Chairman.

Essentially, the question I have is how to secure against the interconnectedness of things? I would like each of you to respond to that for just a minute. I mean, everything is interconnected now, right? So if something goes wrong in one place that has a potential cascading effect throughout the system.

How do you create circuit breakers or safeguards to prevent that because on the one hand you have to be fully integrated, and we are constantly trying to integrate more and more and get rid of silos? On the other hand, if something happens in one sector of our energy infrastructure, then potentially that is going to impact everybody else with a potential cascading effect. How do you handle

that issue, the interconnectedness of things, I guess, unless you have a better way to term it?

Ms. HOFFMAN. I will start and then——

Senator HOEVEN. Sure, that would be great.

Ms. HOFFMAN. So first of all, I think you need to test both devices and networks. So you must start testing these networks to make sure you identify vulnerabilities. As you're looking at components that are connected, you must understand where their vulnerabilities are in the components.

But also, build a system where cybersecurity is built in so that you know what normal operations of the system is and what abnormal operations or abnormal communications are so you can block them and prevent them from causing damage.

Senator HOEVEN. Can you create circuit breakers that both integrate systems and isolate them, when necessary?

Ms. HOFFMAN. So on the circuit breakers, that's a specific technology that has the specific function so you should be able to look at that.

Mr. CAULEY. So a lot of work has been done to compartmentalize within the power system. As I mentioned in my oral remarks, the grid operates over private networks, microwave and fiber systems that are owned and managed by the company. So there is a lot of isolation and departmentalization to protect those systems.

We require, within our standards, that critical assets, we understand the architecture and design of that system so we understand all the connection points and vulnerabilities from that.

The more you get further down into the system, into distribution and distributed resources and those kinds of things, then we're talking about more amass devices and instruments and communications and it's much more difficult because the sharing is the value is everybody is contributing. It is a dilemma to try to operate a very interconnected grid and a compartmentalized and protected grid at the same time.

Senator HOEVEN. As you develop your cybersecurity, as you integrate, are you building those types of circuit breakers or isolation systems to separate yourself from the problem? Is that a standard part of cybersecurity?

Mr. CAULEY. Separation and compartmentalization is standard. There are some of the more most critical assets in control centers and so on now where people are using one way data diodes and things like that, that would control the flow so no harmful information can come in. So that's, sort of, early stages of some of that more advanced work.

Mr. HIGHLEY. Just on the policy level, cross-sector coordination is critical. Oil and gas, telecommunications, electricity, finance, water, all depend on one another, and so what we're doing at the ASCC is bringing those sectors together in cross-sector dialogue, bringing our ISACs, that give us information about cyber threats and sharing those cyber threats amongst the different entities so that we're all working toward the same goal.

Senator HOEVEN. Dave?

Mr. MCCURDY. Senator, that's a great question.

In the natural gas sector, we're doing two things.

One, we are delivering electrons. So we have automated controls. We have Industrial Control systems in those. But we also are moving molecules. So it's a bit more of a mechanical and physical process. In both are safety and security, cybersecurity, concerns. And so, we have the automatic control systems that are separate from a safety standpoint we need to have backup for that and a second tier. In there we have shutoff valves. Again, because of pressurization and compressibility, it's a little slower process so we're able to have some physical control over it as well. And those are separate.

In addition to the other basic hygiene where you try to separate your enterprise system from your operations system. And even though you have human beings crossing between and probably the most significant risk, we haven't talked about it, but people are still the most important risk and we test that on a regular basis.

But there's a—you need that layer of—going beyond a layered defense but layered resiliency. And I think that's the culture we're trying to instill in our center.

Senator HOEVEN. The other question would be how do you know if you are safe? Maybe you alluded to it, but you just do that through testing? I mean, you run various scenarios and do the tests?

Mr. MCCURDY. Yes.

Senator HOEVEN. To try to assess whether you are safe, whether you have these safeguards and whether they work?

Mr. MCCURDY. Yes, sir. We do.

And to one of the other questions, I think to Ron Wyden's question about red teaming. We participate in GridEx. We have another one coming up in a few months, and natural gas, I think for the first time, will actually be participating in that as direct. So as we look at the interdependence of the bulk power system and we're a portion of that, maybe one-third now. Natural gas is being used more.

But you also have to recognize we deliver one-fourth of the country's energy directly to more than 74 million customer sites, not individuals. So, we've got multiple tiers here, and that's why it's important that we coordinate with DOE but also TSA and transportation, because we're a transportation system.

There's multiple layers here, and that's why it's important to have a hearing like this so we can, kind of, get a better understanding. It's not just as simply, just one overlay.

Senator HOEVEN. Are you seeing attacks on a regular basis, be it cyber or other types of attacks on the system?

Mr. MCCURDY. Absolutely, yes. We have detection capabilities, and even my small association has that capability. We've seen it. We're targets. If you have energy in your title or name, you've been attacked for a long time. You've been surveilled. You've been mapped. You've been all these. And it's no longer, you know, what we used to see as individuals, it's nation-state, it's other.

Senator HOEVEN. Yes.

Mr. MCCURDY. Ramping of those threats. You have to assume that you've been penetrated, and then what do you do from there? So, it's a whole different conversation than it was just a few years ago.

I know the Senate and Congress is much more acutely aware today than it was a few years as well.

The CHAIRMAN. Thank you, Senator Hoeven.

Senator King.

Senator KING. Thank you, Madam Chair.

Mr. Bochman, your paper on the Ukraine attack in December 2015 was, in large measure, the inspiration for S. 79, the bill that Senator Risch and I have put in. Could you give some background on what the concept is and what we are trying to do in that bill and the concept of places in the grid where we can protect ourselves by, perhaps, having analog technology?

Mr. BOCHMAN. Sure, thanks for the question, Senator King.

And it is, sort of, a follow on, in a sense from Senator Hoeven's. The paper the Senator is referring to is the National Security Case for Simplicity in Energy Infrastructure. And so, all those questions, all the other points about cascades and interdependencies of the systems in different sectors, all that are enthusiastically embracing adding more technology into systems that used to just be electromechanical and were protected, in large part, through isolation. Each would have a trained engineer, who knew the way that thing worked all the way down to their bones, like an engineer in a substation, for example.

For, as I alluded to in my testimony, many very good business reasons, usually having to do with efficiency and cost savings, but also the ability to see what's going on better. We've connected everything. Convergence has happened. Now we are adding communications and sensor and communications technologies into the most mundane parts of our different interconnected systems. So, they're all talking with each other.

I was going to say to Senator Hoeven, our ability to influence the wide deployment of Internet of Things and Industrial Internet of Things is very minimal. So one of the best things that we can try to do to focus our thinking is prioritization. And this gets to some of the issues in the case for the simplicity paper you're referencing.

What are the systems that absolutely must be protected from a national security point of view? Because of the energy and other processes they support, it would be unacceptable as an economy or as a nation to lose them.

Senator KING. What we are talking about is finding those places, not the entire grid, but finding places where simplicity, and perhaps even old technology, could be an isolating factor. That is what we are talking about here.

Mr. BOCHMAN. Yeah and it's, kind of, neat because very selectively adding these types of analog or out of band or putting a human, a trusted human, back in the loop, doing that in a moderate way in only the holiest of holy places, allows you to then proceed with the modernization which brings all the benefits of the grid that we need to have in the future. So it allows you to do that. At the same time, it might let utility executives, natural gas executives and folks on the hill, sleep a little bit more soundly.

Senator KING. Thank you.

Mr. Cauley, I think you touched on this and Dave McCurdy touched on it as well, I think. We are talking all about cybersecurity and cyberattacks, but in our own national security agencies,

insider attacks have been the vulnerability. To what extent is the industry looking at its own people and how they are investigated and examined and how do we protect against a rogue employee who could do a lot of damage?

Mr. CAULEY. Insider threat is one of the top risks that we look at in both physical and cybersecurity side. And the more critical the job, the more critical the facility that the individual works at, the scale of, in terms of screening and review, doing background checks, goes up with that. So it's a well-known and a well-understood risk.

It's not always perfect. I mean, there was one employee who several, a couple years ago, was at NERC ISO, who went through the normal background checks and turned out that it was a suspicious person, a foreign national that we didn't know about because it wasn't in the database. But to the extent that that information is available in—through a background check, that's a common practice.

Senator KING. Mr. McCurdy, I take it you see this as a threat as well?

Mr. MCCURDY. Yes, Senator.

And beyond just the individual that may have nefarious motives, just lackadaisical security practices. We do social engineering testing of our own staff, and we actually got caught. This week we did one and creative IT staff and just clicking on the wrong link or not checking everything. We test that regularly and you have to.

It's easy just to assume that because it looks like an email from me or someone else, doesn't mean, yup, you know, then you go check those lines. So there's a whole level, multi-levels, of testing with people to raise their awareness of what the threat is.

Senator KING. Mr. Bochman, I am out of time, but——

Mr. BOCHMAN. Super short.

I just wanted to say that you asked about insider threat. You mentioned self-phishing, auto phishing, making sure people aren't clicking on those crazy things, and some of them are very realistic.

When those people, when the attackers successfully phish you and they gain your credentials they know your login and password. They are insider. They have every right to use the applications and access the data to whatever authorization level you were given as that employee. They can proceed at pace. They're not hacking. They're not going against any—they're not bumping into any other security system. That's why everyone is so energized on that topic and still trying to figure out ways to start to take care of it.

Senator KING. Thank you, Madam Chair, and thank you for convening this important hearing.

The CHAIRMAN. Thank you, Senator King.

Senator Hirono.

Senator HIRONO. Thank you, Madam Chair, and I thank the panel.

I have some questions for Ms. Hoffman. In your testimony, you explain that an ecosystem of resilience, working in partnership with local, state and industry stakeholders is the solution to staying ahead of ever-evolving cyber threats to our energy delivery systems.

Is this ecosystem of resilience happening in every state because you have to work with the state level? I mean, it has to be present in every state? Is it?

Ms. HOFFMAN. So, I think there is a—thank you for the question.

I think there is a different level of maturity in the different states in creating an ecosystem of resilience. You could take the example here with Washington State and the National Guard and their ability to partner with a local utility and to do some testing. You also have some other states that are very sophisticated in information sharing with the fusion centers. And so, there has been some advanced best practices.

I think the states really have the opportunity to take advantage of looking at their critical infrastructure and building that partnership through the supply chain into the electric industry and supporting cybersecurity.

Senator HIRONO. But this ecosystem is being created in every state at whatever the level of their systems are?

Ms. HOFFMAN. I think it's a work-in-progress and there is maturing at the state levels, including the information sharing with the Federal Government with the state utility commissions.

Senator HIRONO. Do you have a model or what would work?

Ms. HOFFMAN. I don't have a single model for what would work. I think there are components of what would be successful including information sharing, testing, partnerships.

Senator HIRONO. Do you assess what is going on in every state with regard to this ecosystem of resilience?

Ms. HOFFMAN. The Department of Energy does not assess, but we do do energy assurance plans. We have worked, at least in the past, with the state energy offices in looking at energy assurance planning.

Senator HIRONO. Have you done this in Hawaii?

Ms. HOFFMAN. The energy assurance plans? I believe so. I would have to go back and check for you.

[The information referred to follows:]

INSERT FOR THE RECORD

The Office of Electricity Delivery and Energy Reliability (OE) sponsored Hawaii, through the American Recovery and Reinvestment Act, to develop an Energy Assurance Plan. The Hawaii Department of Business, Economic Development and Tourism made a full udpate of the plan in March 2013 and has since done supplemental reviews and updates, including adding a new Fuel Shortage Emergency Response Measures Annex. Given the sensitivity of the critical infrastructure described in the plan, it is not available for public distribution, however DOE has a copy of the plan by agreement with the state.

Senator HIRONO. In addition to our own ecosystem, we also have a huge military presence in Hawaii. I am wondering whether your Department and the national labs have been called upon to provide technical expertise to the Department of Defense to help address potential cyber threats to our military installations?

Ms. HOFFMAN. So thank you for that question. That's a very important relationship between the Department of Energy and the Department of Defense.

I would answer this in a couple ways. We have an MOU with the Department of Defense, so we've been collaborating on a regular basis from an R&D perspective with the Department of Defense. In the FAST Act, there was a requirement in the FAST Act for DOE to work in partnership with DoD to look at electric sector critical assets in relationship to the Department of Defense. That was completed with the Department of Defense.

We have also had innovation through microgrids that we've done with the Department of Defense. I'm sure you might be familiar with the SPIDERS activities which included several military bases in the Hawaii area as well as Colorado and some other states. So that is a very important relationship.

Senator HIRONO. With regard to the FAST Act, are there any concerns of moving the DOE office, the lead agency for cybersecurity for the energy sector, and going to Homeland Security, for example? Is that a concern, leading——

Ms. HOFFMAN. So the FAST Act did codify the Department of Energy's role as the sector-specific agency, as well as we are the Emergency Support Function #12 and it has been mentioned many times in the hearing today as the primary point for security issues.

Senator HIRONO. So as far as you are concerned it should stay that way.

Last month the President submitted a budget to Congress that would cut $2 billion, or nearly 53 percent, from four major DOE programs, including the office that you lead, the Office of Electricity Delivery and Energy Reliability.

I am deeply troubled about the potential impact that this proposed funding cut would have to the cybersecurity for energy delivery systems R&D program. The CFDC's R&D program aligns federal and private sector priorities for important research that helps detect, prevent and mitigate the consequences of a cyber incident for current and future energy delivery systems.

What will be the specific impact to the R&D program if these cuts are enacted next fiscal year?

Ms. HOFFMAN. Senator, thank you for the question.

As in your interest in the program, as the blueprint was released by the President there is, will be, the Secretary has announced as part of that blueprint, released that the mission of the department will change. We will focus on earlier stage research.

The details of the budget aren't available at this time. We're working diligently to work through those details. I look forward to and would have probably more details, more information when the budget is released in May, in greater detail.

Senator HIRONO. That is being very diplomatically put, I would say.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Hirono.

Senator Franken.

Senator FRANKEN. Thank you, Madam Chair, for holding this Committee hearing. Boy, this is pretty hair-raising stuff.

Colonel Welsh, you brought up in your testimony that we are not well prepared for what comes after a successful cyberattack. You say we have done little to anticipate and develop actual response capacity that would be needed post attack.

The CHAIRMAN. That is interesting.

Senator FRANKEN. Can you elaborate on that? What does that look like? Would anyone else care to jump in too?

Colonel WELSH. You bet, Senator.

So my premise is basically that we've treated cyber different for a long time. Our view is cyber from an emergency response perspective can be looked at just like any other response that we undertake as a nation. So, through DHS and FEMA.

Using the existing natural response framework, things like the National Cyber Incident Response Plan, but one of the most troubling things is, you know, we fight a lot of wildfires out in the State of Washington, there are things called resource types. We know what to call, what to order, what to buy, when something happens. We don't have any of that in cyber.

If some cyber event happens tonight and it happens in the State of Washington, thankfully we've got a lot of cyber folks to help. But let's just say it happens in Idaho, and they don't have a whole lot. There's no way to get cyber resources. There's no cyber ninja force, for the most part, out there ready to call and organized in a way that can respond. That, sort of, goes back to the previous question before us on failure of imagination. We've not taken that next step from a response and recovery standpoint.

And also, the acknowledgement that a cyberattack is, sort of, a cyber is an IT, sort of, issue. But the second and third order consequences that are emergency management issues, that are already handled by our existing emergency management processes, have to be brought into the discussion as well. Thanks.

Senator FRANKEN. Anyone else want to jump in on that?

Mr. HIGHLEY. We all——

Senator FRANKEN. Does anyone not want to jump in on that?

[Laughter.]

Okay.

Mr. CAULEY. So, I would say first, Senator, that that's the purpose of our massive GridEx exercise we do. We basically break the system. We put people in the dark. We have massive disruptions in cyber and physical attacks.

Senator FRANKEN. So you do it at night?

Mr. CAULEY. We do it over a 2-day period.

Senator FRANKEN. Okay.

Mr. CAULEY. And it's simulated so no one actually gets hurt in the process. But with leadership from the White House and Energy and Defense and DHS, and the CEOs and leadership of the industry are on the table. We're working through the challenges.

Senator FRANKEN. Because the Colonel seems to be saying we are not prepared for this.

Mr. HIGHLEY. There is a cyber——

Mr. CAULEY. One of the things that came out of this was the need to create a Cyber Mutual Assistance Program, and I'd like Mr. Highley to talk about that work.

Mr. HIGHLEY. There is a cyber ninja force. It's in its early formation.

Senator FRANKEN. Cyber what force?

Mr. HIGHLEY. Well, somebody said there wasn't a cyber ninja force. There is a cyber ninja force. It's the Cyber Mutual Assistance Program that's parallel to the utilities in the electric sector.

Senator FRANKEN. Is ninja an acronym or just——

[Laughter.]

There are too many acronyms.

Mr. HIGHLEY. We have 93 member utility systems that are members of Cyber Mutual Assistance that will help each other in the event of a cyberattack and send their IT professionals to assist the others in restoration. That means that 80 percent of utility customers in the country are covered by that right now from the membership.

Senator FRANKEN. Because I think what the Colonel is saying that after this happens it is not just cyber.

Mr. HIGHLEY. True.

Senator FRANKEN. It is the effects of the cyber.

Mr. HIGHLEY. True.

Senator FRANKEN. And that we have got to be ready for that.

Colonel, you were talking about the number of personnel that you have, cyber personnel or people prepared for this in Washington. What I am wondering about, and you talk about this too, is the need to train people in this. The need to, you called it a, some kind of school, schoolhouse, cyber schoolhouse program. Are we training enough people to do this? And how can we do that? That is the question.

Mr. BOCHMAN. There's an incredible dearth of trained utility qualified or industrial control systems, security personnel in the country, probably in the world. But where we need, the demand signals that we're getting from all over the place, are for a thousand or many thousands of these people who can touch that specialized type of equipment. We probably have hundreds from some informal surveys we've done.

To your—go ahead.

Senator FRANKEN. I am sorry, but I am curious. What countries do this better than we do or which piece of it? In other words, I think, Russia attacks well.

[Laughter.]

I have this theory. You know, other? Who is good at attacking and who is good at defending and who has these people?

I remember after World War II we took some of the German scientists.

Mr. MCCURDY. Well, Senator.

Senator FRANKEN. I am not suggesting—I think we need to have home grown and——

Mr. MCCURDY. Yeah.

Senator FRANKEN. Yes.

Mr. MCCURDY. Senator Franken, there's a lot in that question, but first of all, no one can surpass the United States in its offen-

sive capabilities in the cyber arena whether it's national security agency or other confident, you know, classified areas. So, put that aside.

China, Russia, Israel, in certain respects there are criminal elements. There are subnational levels, Iran. So, you know, there's multiple levels of capabilities.

The question is what is the threat to us? And this is all risk assessment. If a nation-state decides they want to take down the grid, there are many ways to attack and it's not just cyber. It would be a combination of physical and cyber, if it got to that level because that's act of war.

Now, there are other ways that people are attacking our systems. They either want to demonstrate capability. They want to, you know, steal information. So again, we have to plan for those different types.

Recovery is a different question though, and I think you were, kind of, asking that other question. Recovery from the IT standpoint, the ICS, the control systems, that's where we need to work with the Federal Government and that's where the—we own 90 percent of the infrastructure out there so we have to have those backups.

If you're talking about large units that could be affected. That's one issue. It's another if it's computer systems. And on my front, it's mechanical systems. If we have to restart pilot lights around the country, you know, in the dead of winter, it's pretty challenging.

So there are multiple levels that we have to plan for. We do this with regard to storms. A lot of this activity you see, collaborative, is in fact the result of Superstorm Sandy where the Administration worked with utility sectors to respond to a natural disaster. So we've learned. Is it perfect? Never. Will it be perfect? You can't get there, but we're improving.

Senator FRANKEN. Okay. Thank you. I am way over.

The CHAIRMAN. Thank you.

Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you, Madam Chair.

I want to follow up on my colleague, Senator Franken. I am really interested in the Cyber Mutual Assistance Program. Can you elaborate? I am really interested in whether there is a set infrastructure to it and put on paper? And do you have involvement from the federal, state, local government, first responders, everybody that would be involved in an incident? And then, do you have regular table top exercises to address some sort of cyber threat that has an impact on a community's grid and the consequences of that?

Mr. BOCHMAN. If you don't mind I'd like to briefly go after, to answer your question, come back from Senator Franken's first question to Colonel Welsh of the National Guard and Cyber Mutual Assistance and how it is like and how it is unlike the mutual assistance that we often reference with storms and Sandy and such.

We're all used to, utility folks, are all used to rallying when a hurricane or a tornado happens. You count on those proximate to you who weren't affected, who weren't damaged and they roll trucks and linemen and equipment and help out. That's a well-worn and very effective process.

The thing in the cybersecurity world, and there's a subtlety here which I hope I can convey, they're all not interchangeable people. They all have, they're like specialties in the medical profession, all right? You can't take a brain surgeon and help someone set their leg and vice versa.

So the people that are capable of bringing cybersecurity good effects after an incident are those most familiar with the particular type of equipment that that utility uses, which means, and DoD Under Secretary Paul Stockton who was in charge of mission assurance at the time articulated this, that your best ally when you need that type of help and it may come from a National Guard source, we're all looking to the National Guard increasingly for this capability is not the person in the utility that's right next to you.

This could be a person in the utility on the complete other side of the country, but the control systems you use are the same make and model. And so, and not only that, since you knew that, you practiced and did exchanges beforehand and built a trust level with that person and a level of familiarity with that person. So that when you're in your time of great need, you knew who to call. You trusted them and they were familiar enough with your environment that you let them come. You trust them and they could potentially help you in that situation.

Senator CORTEZ MASTO. Okay, just so I understand, because what I am thinking about are, let me just put it in conceptual terms or rings. The interior ring is the cybersecurity specialists that responded at that level. The next would be community-wide, what is happening in that community and the responders that would be involved and the impact to that community and then whether it goes state and then federal.

So what you are talking and what I hear is that the Cyber Mutual Assistance Program is that first ring. That is all that is involved and that is sharing that information back and forth to those cybersecurity experts who are addressing a response at that time. Is that correct?

Mr. HIGHLEY. The Cyber Mutual Assistance Program is a written agreement that 93 member utilities have signed to share resources and then to trade who has what kind of system. Then it goes over to NERC and the exercise we do under GridEx where we get all the sectors together to practice the restoration, the rest of the circles. So working with state and local governments on restoration is what we also do with NERC, through GridEx.

Senator CORTEZ MASTO. Okay, that is helpful.

Is that done on a regular basis or are there things that we need to improve upon those circles and that response?

Mr. CAULEY. Well, we do the GridEx exercise every two years. The next one will be November. The intervening time between there's a lot of building capability and doing mini exercises to develop that, test that capability.

This coming exercise in mid-November will have a new emphasis on having state level participation and emergency response at the local and state level involved in the exercise. It's been there in the past. We just need to make it much more expansive this time around.

Senator CORTEZ MASTO. Thank you.

Let me follow up very quickly on something that the Chairman started talking about. I have been sitting in a number of these committee hearings addressing cybersecurity threats. And thank you very much, it is such an important topic.

One of the things I constantly hear is the need to be able to expedite and share classified information with private companies and utilities and with the federal level as well. I am curious, do any of you have suggestions that could improve CRISP's ability to distribute classified and unclassified information in a timely fashion while still protecting that classified content?

Mr. CAULEY. I'll—I'd like to answer the question more broadly even than it was asked.

I think what's happened is that in the last couple years our position has changed to the point where protecting our critical infrastructure, including the electricity system, is a national security matter. I think what we've got to do is figure out how do we get government and industry to work together like we have a shared problem in front of us and not that the assets belong to the power companies and our job over here, historically, has been to find sensitive information and classified information and protect it. I think it starts with, really, two things.

One is getting industry and the top levels of government together and develop a strategy and a plan going forward on how we're going to manage the critical nature of these assets to national security and how we're going to protect that. I think something like that was proposed in the NIAC report recently.

Then the second piece is how do we, if we believe in the plan and we're going to work the plan together, how do we become part of a shared community where we trust sharing the information because the old rules of protecting classified information, sensitive information. We have cases where we've actually created new information out of the CRISP project, handed it over to the government and then the government says now that's classified. But we just gave it to you, so we're having a hard time sharing it because you just classified it. We need to figure out a new set of ground rules around a partnership between industry and government on fighting the war together.

Senator CORTEZ MASTO. Thank you. I appreciate the opportunity to speak today.

The CHAIRMAN. Thank you.

Senator Duckworth.

Senator DUCKWORTH. Thank you, Chairman Murkowski, Ranking Member Cantwell, for convening this very important hearing and about how we can secure our energy infrastructure against cyber threats.

When I was on the House Armed Services Committee, I saw, first-hand, the vulnerability across departmental efforts on this. For example, I was touring a contractor for a major Army maneuvent command and they had the capability. They were very proud to show me that they had installed low wattage light bulbs for the street lights at this military post. They were showing me in Illinois how they could dim the lights and save energy at the post.

But I was in a room where they were controlling the grid for this major military command in Texas, and I said, who has access to this computer? Who has a security clearance? They had one person with a security clearance who was an engineer over there. I said, oh. The room is just left unlocked but look at what we can do, how nifty this is. We're saving all this energy. And there was no thought to the cyber.

And yet, this post is the headquarters of a major military command, and it was connected to the civilian grid of the community immediately off post. So anybody could have gotten access to that room, to that computer, and affected not just the military installation but also the civilian community on the outside. That's why, I think, we need to be much more sophisticated in how we talk about these issues.

In my own home state, Argonne National Laboratory has a team of scientists and researchers with deep expertise in cybersecurity and critical infrastructure. They have been working on developing advanced power grid, cybersecurity solutions for DOE cybersecurity for the energy delivery systems program, including cloud-based grid applications, wide-area protection and control and distributed energy resource management systems.

Ms. Hoffman and Mr. Bochman, can each of you quickly address the value of this cutting-edge research that is being conducted at Argonne at this time?

Ms. HOFFMAN. So thank you to the Senator for the question.

The laboratories provide a wealth of research and solutions for these energy delivery systems, and Argonne National Laboratory is on the cutting-edge of a couple of topics.

You've mentioned clouds. Cloud-based computing is now being evaluated and looked at to be implemented within the energy sector, especially around the smaller type utilities that want to look for cost-effective solutions. Getting ahead of implementing cloud-based solutions is absolutely critical that we build security in. That is one example that they are working on.

I was—admit I did not bring it up when Senator Stabenow brought up about the distributed energy resources, but looking at security around inverters, the work that Argonne is doing there is also a critical, important asset.

But the national laboratories, working together, through the Grid Modernization Lab Consortium, really provide an opportunity for us to add value across all the capabilities of the national labs.

Senator DUCKWORTH. Thank you.

Mr. BOCHMAN. Thanks, Pat. And Senator, thanks for the question.

Yes, we have many fine colleagues, really brilliant people at Argonne and appreciate the effort that they bring.

To go right at your question with two concrete examples. The oft-referenced CRISP program for threat intelligence and information sharing in the energy sector, Argonne plays a very important part of that, both in its current version and as we're working to improve it in some ways so it's better for the customers.

They also play an important role in a California/DOE-funded, supported, California energy systems for the 21st century project that involves machine-to-machine information threat sharing. So

whenever people say this needs to be faster and near real time or real time, that project that Argonne plays an important part on along with INL, PNNL and other labs. They play a big role.

Right to your first thing, I want to finish this. When you gave that very bleak example, I don't know how many years ago that was, but I assume it could still be——

Senator DUCKWORTH. Not too many.

Mr. BOCHMAN. We could find that still today, right?

I think the ultimate solution for problems that are as heinous as that is a cultural one, not a technology one. When we eventually start to see that security which we haven't spent much time worrying about up until recently, it is actually every bit as much a safety issue as a compliance issue or anything else and some lapse in security somewhere could cause physical damage or kill people in other places.

Once those two things are fused much more tightly than they are today in people's minds, I think you'll see better behavior across the board.

Senator DUCKWORTH. And, you know, people have just simply had not thought about the cyber part. They were just very proud of the fact that they were saving money for the DoD.

Mr. BOCHMAN. Right.

Senator DUCKWORTH. And how great it was to have this technology. When I brought up how vulnerable are you to cyberattack, it was something that the engineers, because they were worried about wattage and controlling the street lamps, it never occurred to them that they could be under cyberattack.

So I would think that you both would agree with me that Congress should prioritize funding for research like the one at Argonne in developing efforts in this area.

Mr. BOCHMAN. Sure thing.

Senator DUCKWORTH. Thank you.

I am out of time. Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Duckworth.

Senator Cantwell.

Senator CANTWELL. Thank you, Madam Chair, and thanks to all the witnesses and to our colleagues. I think this has been a very good hearing illuminating where we are and many of the challenges we face going forward.

Mr. McCurdy, I wanted to ask you, there is a 2014 Bloomberg report that states, "hackers had shut down," this was in Turkey, "had shut down alarms, cut off communications, super pressurized a crude oil pipeline which led to a physical explosion. The main weapon, Valve Station 30, was a keyboard."

We've given the Transportation Security Administration (TSA) the responsibility for mandatory reliability standards, and yet, here we are with TSA in this ever-changing and dynamic environment. What is the TSA budget for these activities and how many TSA employees are actually involved in the cybersecurity of the million miles of pipeline that we have in the United States?

Mr. MCCURDY. Well, it was, I guess, above my pay grade. I don't know what their budget is. I'd have to check. You probably do, I think.

It's a—and you're right. We have 2.5 million miles of natural gas pipelines which is only a little less than the 2.6 million miles of paved roads.

The TSA does regular audits. They do cooperate. We work closely. They are a subject matter expert in the Department of Transportation, as is PHMSA.

We talk about the culture of safety and security being together. That's where it really does come closest, and they are expert in that area.

We dual hat. The other, as they say, is energy and as to the extent that we are interdependent and support them, we do benefit from that relationship in and across sector sharing of technologies, standards.

We've done things as well. Downstream Natural Gas, we formed our own ISAC. Gerry runs the E-ISAC. We now have, we just announced that the Downstream Natural Gas ISAC has a seat in the E-ISAC. So, there is this sharing.

We get the alerts that they put out that are relevant to our sector so that we disseminate that to our, you know, critical owners and operators out there in the system. So there's a lot.

We use Idaho labs. We use the ICS CERT. We were involved in the NIST, development of the NIST standard. So the industry is very pro-active on this front, and we've had good collaboration with TSA.

Senator CANTWELL. I think you hit on it, which is the notion that you are on the private side and on the public side GAO has said that we still don't have the metrics needed to measure the relative cybersecurity of our pipeline system.

I think what we need to do is, as we continue to see, and I mentioned the situation in Turkey, as those kinds of threats prevail, we need to elevate this discussion like we are doing today. But to get the Transportation Security Administration, who I'm not sure everybody understands who they are and what role they play in this, to some elevated level so that we actually have metrics here that we are holding the industry accountable.

Now, I know, you may say something like that people would probably say, wait, wait, wait, no, we don't want any new regulation. But at the same time, I am for the collaborative effort. I am. I think that we have to have some measureables here that we need to put in place.

So we will be looking at that.

Mr. MCCURDY. Well again, you know, I think it would be an opportunity to bring them in and have that conversation as well.

But when you look at the cybersecurity standards and if you look at—which are minimal. What we do beyond that in the level of focus it has now within the companies themselves.

I'll give you an example, I have some CEOs in this week, a leadership program. A CEO told me this morning, they're now recruiting board members from software companies or from IT companies or security firms because that's an expertise they need to even continue to push.

So, on the private side, I can only speak to that. But I will tell you that it's a constantly evolving system and the threat evolves, with our actions evolving and we try to stay up with that.

Senator CANTWELL. You are willing to think about those things in a collaborative fashion.

Mr. MCCURDY. We have a culture of safety which means that we constantly adapt and improve. And as the Ranking Member knows, I've been involved in this for quite some time. I've watched this evolve. And anyone whose static is lost. It's a constant challenging game, and we have to be on top.

Senator CANTWELL. Well, I wanted, if I could, Madam Chair. I know we have a vote that has been called. I wanted to again thank Colonel Welsh for being here and for all that is happening in the State of Washington.

And to the point that Mr. McCurdy was just making, what you have hit on is 600, I think, cyber personnel within the National Guard. So, that's been a great bonus to the operation and infrastructure.

It sounds like cross pollination of cyber expertise in security as it relates to the infrastructure. We need to continue to do that.

I know that the Center for Strategic and International Studies has called it a human capital crisis, that there will be by 2020 an opening of 1.5 million cybersecurity positions. Do you have thoughts on how we should proceed on a cyber workforce?

[Laughter.]

Either from your own National Guard perspective. I know what we're doing at the University of Washington, which is really great work, particularly at University of Washington, Tacoma with three different levels of degrees in cybersecurity. But is there more that we need to do, even within our own ranks?

Colonel WELSH. You bet, Senator.

So, I think, in some ways, I mean, just the fact that we've got that number of cyber professionals in the state is its own economic engine, you know, if managed appropriately.

But you know, the National Guard does a great job of training folks. We get them into school. They're drug free. You know they're in great shape. Then they get security clearances, so I mean, that's a huge benefit to companies out there from, sort of, we can give back a little bit.

But you're right. There are more jobs than people out there. We've got some great training programs with University of Washington, great internship opportunities in the state. And that's the great thing about, as I talked before about, the Adjutant Generals Convening Authority. You can actually, kind of, get folks together and talk about things like educational diversity and things like that.

So we're doing good on workforce development. There's a lot more to do. But again, it's things like having jobs in the Guard. It's having jobs in the state that as we have good folks come out of schools we can actually place them and they can get to work.

Senator CANTWELL. And do you think that that kind of information and partnership, as you alluded to in your testimony, has put us, I don't mean ahead, but on the right track, as it relates to outlining this theme throughout the conversation, which has been how do we share information, how do we analyze and share this critical information?

Do you think the fact that we are knitting a culture in layers across the public and private sector is creating avenues for information sharing that didn't exist before?

Colonel WELSH. Yes. We don't copyright our processes at all in Washington State. So we are willing to share. Everything we do we'll be more than happy to talk about and discuss, but again, it's one approach that has worked.

I'm worried more about the states that aren't. And really, we, in some ways, have really have and have nots, if you look across the states. I think the Senator from Hawaii was, sort of, nibbling around that a little bit.

We're fortunate in the state. We're geographically blessed. But there are others that aren't and when you look, from an attacker's perspective, you just have to find the one that isn't and start there.

Senator CANTWELL. Did you want to say something, Mr. Bochman?

Mr. BOCHMAN. Yeah, thanks, Senator.

Yeah, sure, the Pacific Northwest National Lab in your state of Washington, the Idaho National Lab and Sandia down in New Mexico, are arguably the three most operational technology or industrial security-oriented and capable labs in the complex. There's others as well that assist. And recognizing that tremendous shortfall in that type of talent, not just a generic IT security talent, but industrial control system security specialists which requires years of experience and special education.

Those three labs have joined together to work with the regional universities, with other government agencies, with STEM programs, to begin to really kick this into a much higher gear than it seems to be doing on its own.

Senator CANTWELL. I would just note for everyone that the Chair and I have worked hard on this and we still have provisions of the energy bill that we would like to see passed that would double the R&D for this effort in DOE and help us look at a supply chain initiative and invest in the cyber workforce, given that there is such a high need. So, we hope that we will be able to keep pushing those ideas and getting our colleagues in the House to understand.

I think we had a great representation here today and lots of great questions, lots of good information brought out by our colleagues.

Thank you.

The CHAIRMAN. Thank you, Senator Cantwell.

I appreciate your comments there at the end, General Welsh, about the fact that in certain states, they are perhaps not as evenly endowed with the resources. Of course, Alaska and Hawaii sit off that grid. Sometimes the simplicity of our grid is something that gives us a little more comfort. But at the end of the day, we are truly one of those islanded states when it comes to access to resources as well.

Senator Cantwell mentioned the metrics and how we measure, and there has been a lot of discussion in these past four, now five, hearings that we have had when we have been talking about infrastructure and talking about regulation and permitting and all that that entails. But we recognize that when it comes to regulations there are mandatory and there are voluntary. There are tradeoffs

and benefits, I think, to each. But in recognizing that when we are talking about cybersecurity, our real challenge here is to be nimble, to be faster and smarter than the guys that are looking to bring us down.

What is the right mix between mandatory as opposed to voluntary regulation? I don't know if any of you have anything concrete, but it is something that we need to assess here as we are looking at legislating.

Mr. Cauley?

Mr. CAULEY. I think mandatory requirements has its place, and I think what we've done in the bulk power system is an appropriate fit where you have the most critical assets in the system. You want to make sure that everyone is meeting a threshold set of requirements that, you know, you could be harmed by the weakest link. So, I think, there's comfort across the industry having a common set of standards that are risk-based.

It also helps with the mandatory standards in terms of cost recovery and making sure that the resources and investments are there. So, I think, the power industry appreciates having mandatory standards for the bulk power system.

I think in other areas it may be more challenging. And I, you know, one area where I'm particularly concerned is a lot of the electronics and the distribution system. How do we get guidelines and best practices adopted in a consistent way across so many different jurisdictions?

I think mandatory standards there would be very difficult given the jurisdictional challenge, but getting stronger guidelines and practices in a consistent way across that area would be helpful.

The CHAIRMAN. Mr. McCurdy, on the gas side, do you think that the gas industry needs a set of mandatory standards? Should the mandatory NERC cyber standards need to apply to the gas industry?

Mr. MCCURDY. No.

The CHAIRMAN. Okay, that's easy.

[Laughter.]

Mr. MCCURDY. The—and part of that is the nature of the systems themselves. We've seen and we've all learned in the electric sector that because of its true interconnectedness and even though there are sub grids there, there can be massive cascading failures and those are critical infrastructures and they are a lifeline and they're absolutely essential for our economy and way of life and in public safety.

It's less of a challenge, less risk, I think, in the gas distribution network. There are potentials, but they are not because they're—it's mechanical, it's gas, it's pressurized and it's less likely to have a complete regional failure based on a particular attack. So I think we've evolved. We're growing into that.

The reason this is now part of this hearing, I think, and focus is the more that the electric sector is using natural gas as a base fuel, there is the concern what's the reliability in the access to that fuel?

That's both the cyber question, but that's also a physical question that you know extremely well and that's where pipeline permitting and infrastructure and capacity, those are all issues as well.

The Northeast in the Polar Vortex, that was raised earlier, was more risk because they had limited access to natural gas pipelines through firm capacity contracts than they are from a cascading failure because of some incident.

So those are both questions that we have to ask and that's something that FERC has to deal with and it's a regional issue, it's not federal.

The CHAIRMAN. Yes.

Mr. MCCURDY. It's not a federal fix. It's going to be a regional fix, but we all need to be working together and raise the awareness of that concern. That's the reason I put that one section in my testimony about the access.

The CHAIRMAN. We have got a vote that started at noon and it is a 15-minute vote, but we are on Senate time here. So I am going to ask Ms. Hoffman, you wanted to weigh in and I also wanted to ask you. With the FAST Act we have identified DOE as the head, if you will, in terms of granting authority to direct utility action. Do you think that is being recognized and respected by DHS? Are we on the same footing as DHS?

Ms. HOFFMAN. So the answer is yes, but I do believe that there is the interdependence issue that DHS has a strong capability of making sure that the interdependencies are recognized.

The one point that I wanted to make on the earlier conversation is how do we measure success? I think at the end of the day the way to measure success is to make sure that every industry and sector has the capabilities to do what needs to be done when a cyber event occurs. So whether it's a workforce capability, whether it's installing additional equipment, whether it's having continuous monitoring, that we have the capabilities built and that we can test against those capabilities and be evaluated that we're performing correctly with those capabilities. That was the comment I wanted to add.

The CHAIRMAN. Okay.

Mr. Bochman, you get the last word.

Mr. BOCHMAN. Fantastic. Thanks, Senator.

Your opening question about voluntary or mandatory types of security guidance, I think there's something, there's some things, there's three flavors, I think. There's guidance and best practices.

And just back from Estonia where the Baltic Sea and Black Sea countries are, who are all trying to figure out how to regulate their energy sectors for security. They are so thankful that the DOE had put down in writing some very helpful best practices, both for managing—both for measuring maturity of security practices and also for procurement guidelines. These are things that took a lot of effort and a lot of expertise to build and give some of our friends a big head start. And so that's one plug for them. They appreciated that. Those are guidelines.

Swing to the other extreme, are mandatory things. Thou must do, else you'll be penalized a significant amount of money and you won't like it reputational either. That's the NERC CIPs. Those have moved the utilities, many would argue, much farther, must faster than they otherwise might have, if they hadn't had to comply with those. With those, that's the stick, right?

I think I'll finish with the carrot. The carrot which I've seen from—that seems missing, I think in some and could be improved from work with public utility commissions and utilities themselves would be incentives, ways to motivate, financially and otherwise, motivate good security behaviors that aren't just the stick of the mandatory things, but certainly go far beyond the guidelines and the best practices you should do these things. I think if we could look at incentives to motivate the types of behavior we want, I think you might see things go a lot farther, a lot faster.

Mr. MCCURDY. And just on that point, if I could, because we are state regulated in the natural gas area. And the current Chairman of NARUC was just at our offices this morning.

We now have reimbursement. They are rate based. The ability to rate base the cost of cyber is a big deal. And if—because it's huge. You can, you know, throw money at this forever and never get to the level you want. But if you don't have it as recoverable in your rates, then it doesn't really work.

So, that's—they are moving in that direction. So that's where the partnership with the states is really very critical from the incentive standpoint.

The CHAIRMAN. Good.

We could clearly go on for a long time, but even by Senate standards, I am late.

[Laughter.]

I thank you all for your very, very important testimony. I think you saw the level of interest here. Know that we will continue to work in this important area.

Thank you.

We stand adjourned.

[Whereupon, at 12:22 p.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

Department of Energy
Washington, DC 20585

May 9, 2017

The Honorable Lisa Murkowski
Chairman
Committee on Energy and Natural Resources
United States Senate
Washington, DC 20510

Dear Madam Chairman:

On April 4, 2017, Patricia Hoffman, Acting Assistant Secretary, Office of Electricity Delivery and Energy Reliability, testified regarding the efforts to protect U.S. energy delivery systems from cybersecurity threats.

Enclosed are the answers to questions submitted by Senator Ron Wyden and you for the hearing record.

If you need any additional information or further assistance, please contact me or Lillian Owen, Office of Congressional and Intergovernmental Affairs at (202) 586-5450.

Sincerely,

Shari Davenport
Principal Deputy Assistant Secretary
Congressional and Intergovernmental Affairs

Enclosures

cc: The Honorable Maria Cantwell
Ranking Member

QUESTIONS FROM CHAIRMAN LISA MURKOWSKI

Q1. With regard to Geomagnetic Disturbances (GMD), you testified that "[c]urrent DOE efforts relate to obtaining better data on GMDs, developing an approach to monitoring the grid and its components for GMD effects, and testing the effectiveness of blocking devices." However, FERC ordered NERC to produce a standard on GMD which it did and the Commission has since finalized. Is a GMD mandatory standard appropriate at this time or was it premature of FERC to direct such a standard?

A1. Department of Energy (DOE) believes the standard is timely, and the nature of North American Electric Reliability Corporation standards allows for updates to be made when necessary. DOE has supported the standard and will continue to support any update to the standard by providing data gathered through monitors (such as variometers and geomagnetically induced current [GIC] monitors) and any potential testing on the effectiveness of mitigation and protection devices.

Q2. What kind of plans does DOE have in place should a 15-day emergency order be issued by the Secretary of Energy?

A2. We are finalizing our review of comments provided on the "Grid Security Emergency Orders: Procedures for Issuances." For the time being, we are prepared to use the procedures as currently laid out in the Federal Register.[1]

Q3. What has DOE done to implement its FAST Act authorities? What, if anything, remains to be finalized?

A3. DOE developed and adopted procedures related to emergency preparedness for energy supply disruptions and submitted a report to Congress in 2016 describing the effectiveness of these activities in response to Section 61001 of the Fixing America's Surface Transportation (FAST) Act of 2015.

DOE is prepared to issue emergency orders, when required, pursuant to Section 61002 of the FAST Act, which amended Section 202(c) of the Federal Power Act (16 U.S.C.

[1] https://www.federalregister.gov/documents/2016/12/07/2016-28974/grid-security-emergency-orders-procedures-for-issuance

824a(c)) regarding mitigation of 202(c) emergency order conflicts with environmental laws.

Section 61003 of the FAST Act amended Part II of the Federal Power Act (specifically 16 U.S.C. 824o-1) to provide the Secretary of Energy with the authority to issue emergency measures during a Presidentially declared grid security emergency and required DOE to establish related rules of procedure. The public comment period for the grid security emergency draft closed February 6, 2017, and final promulgation is underway. This new authority included the ability to share classified material during a grid security emergency when supporting an incident. DOE was also directed to designate defense-critical electric infrastructure, which was completed in October 2016 in coordination with the Departments of Defense and Homeland Security and the Federal Energy Regulatory Commission (FERC). The Secretary of Energy and FERC were authorized to designate critical electric infrastructure information (CEII). FERC's CEII rulemaking was finalized in December 2016 and DOE is currently assessing the need for a complementary procedural rulemaking.

This section also appointed DOE as the sector-specific agency for cybersecurity for the energy sector. This clarification, which is unique in the critical infrastructure sectors, supports coordination efforts to enhance preparedness, response, and restoration to cybersecurity issues.

In March 2017, DOE submitted to Congress a strategic transformer reserve technical analysis and examination of efforts currently underway by industry and Government in response to Section 61004 of the FAST Act.

DOE, in collaboration with the Department of State, submitted a report on recommended United States energy security valuation methods in January 2017 in response to Section 61005 of the FAST Act.

Section 32204 of the FAST Act directs the Secretary of Energy to draw down and sell crude oil from the Strategic Petroleum Reserve in the quantity appropriate to maximize the financial return to U.S. taxpayers in fiscal years (FY) 2016 and 2017 and to drawdown and sell 16 million barrels during FY 2023 and 25 million barrels during each of FY 2024 and 2025. No sales pursuant to Section 32204(a)(1)(A) occurred in FY 2016

or FY 2017, but sales are planned for FY 2023, FY 2024, and FY 2025. Pursuant to Section 32204(a)(2), proceeds from these sales must be deposited into the general fund of the Treasury.

Q4a. Obtaining the appropriate clearance for cyber security professionals seems to be a challenge for the private sector. What do you see as the biggest challenge to the issuance of clearances?

A4a. The ability to provide security clearances to the private sector is very important to ensure adequate information sharing between the Federal Government and industry. The biggest challenge in issuing clearances is the time it currently takes to process and issue a security clearance to individuals.

Q4b. What do you recommend to make this process more efficient?

A4b. The Office of Personnel Management (OPM), as the Suitability Executive Agent, and the Office of the Director of National Intelligence, as the Security Executive Agent, are responsible for suitability and security clearance reform activities that include policy, guidance, oversight, and compliance. DOE will work with its investigative service provider, OPM's National Background Investigations Bureau, to prioritize investigations supporting clearances for energy-sector critical infrastructure owners and operators, as needed.

QUESTIONS FROM SENATOR RON WYDEN

Q1. Ms. Hoffman, can you explain how the proposed Trump budget cuts to the DOE's Office of Electricity Delivery and Energy Reliability could affect the office's cybersecurity plans?

A1. The President's Budget Blueprint recognized the importance of cybersecurity for the grid, stating "The President's 2018 budget . . . [s]upports the Office of Electricity Delivery and Energy Reliability's capacity to carry out cybersecurity and grid resiliency activities that would help harden and evolve critical grid infrastructure that the American people and the economy rely upon." We will be able to discuss the 2018 budget in greater detail after the full budget is released this month.

Q2. Ms. Hoffman, I asked the witness panel to express their views on encryption. It is my belief that weakening encryption used on the electricity grid, and in other aspects of our energy infrastructure, would be outlandishly bad judgement--and I have made it clear that I will fight this every step of the way. Do you believe encryption plays an important role in protecting the electricity grid? Please explain your answer.

A2. Encryption plays an important role in ensuring the Nation's electric grid is adequately protected against cyber events. For example, encryption is needed to meet several North American Electric Reliability Corporation Critical Information Protection standards. Encryption is used to protect data at rest and for secure data transfer to reduce the risk of unauthorized interception of communications that could lead to misoperation and grid instability. Encryption is also used for enhanced protection during authentication of system users.

The role of encryption in the cybersecurity of the energy grid has been, and continues to be, advanced, e.g., Chapter 4 of the NIST-IR 7628, entitled "Cryptography and Key Management."[2] Ongoing research in the cybersecurity for energy delivery systems community continues to advance technologies that will further enhance the effective use of encryption throughout critical energy infrastructure. For example, Department of Energy (DOE) is supporting early stage research at Pacific Northwest National Laboratory where researchers are developing a new encryption key management architecture suited to the unique requirements of energy delivery control systems.

[2] http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

Another example is DOE-supported early stage research being conducted at the Los Alamos and Oak Ridge National Laboratories, where researchers are developing cybersecurity technology for critical energy infrastructure that uses the principles of quantum physics for the secure exchange of secret keys that can then be used in traditional cryptographic algorithms. This technology, Quantum Key Distribution, reveals, in real time, adversarial attempts to steal secret keys being exchanged between trusted parties because any attempted interception changes the key, at the moment of interception, in a measureable way.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

Questions from Chairman Lisa Murkowski

Question 1: NERC has mandatory authority over its standards, which means that sometimes it finds itself recommending a penalty assessment for approval by FERC.

a. Roughly speaking, about how many penalties has NERC assessed?

b. About how many fines has NERC assessed?

c. What percentage of those penalties and/or fines involve cyber issues?

d. Were any of the cyber violations notable?

From January 1, 2015, through March 31, 2017, NERC assessed Notices of Penalty (NOPs) for 956 violations. Of those 956 violations, 506 violations involved a financial penalty, 62 violations involved a zero-dollar penalty, and 388 violations carried no penalty because they involved federal entities.[1] Over 80% of noncompliance is self-reported by the registered entities. Mitigation is required for all noncompliance, whether or not there is a penalty. In addition to mitigation, some NOPs involve above and beyond activities, along with or instead of a penalty, that enhance reliability and security beyond what is required for compliance with the mandatory Reliability Standards.

For the 2015-2017 period, 68% of the 956 NOP violations (651) involved the Critical Infrastructure Protection (CIP) standards. NERC's caseload has predominantly involved CIP violations for the last several years. As registered entities gained more experience with the non-CIP Reliability Standards, rates of noncompliance with these standards has decreased.

In two NOPs involving CIP violations, NERC (through the Regional Entities to which NERC has delegated enforcement responsibility) assessed penalties in excess of $1 million. The CIP violations resulting in NOPs involve 65 registered entities, approximately 5% of all of the registered entities subject to CIP standards. Further, only one of those CIP violations had an actual impact, as a registered entity's failure to patch the software on its Energy Management System (EMS) caused the EMS to fail and the registered entity to lose visibility and monitoring capability of its system. During the loss of visibility, the registered entity maintained communication with neighboring entities, which helped to sustain reliable system operations.

[1] NERC does not have authority to assess financial penalties against federal entities, based on the decision of the U.S. Court of Appeals for the District of Columbia Circuit in *Southwestern Power Adm'n v. Federal Energy Regulatory Comm'n*,763 F.3d 27 (D.C. Cir. 2014)(*SWPA*).

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

All NOPs are available on the NERC compliance website.[2] In the case of CIP matters, specifics remain confidential due to security considerations.

Question 2: Obtaining the appropriate clearance for cyber security professionals seems to be a challenge for the private sector.

a. What do you see as the biggest challenge to the issuance of clearances?

b. What do you recommend to make this process more efficient?

Some challenges industry faces in obtaining security clearances are: unclear guidance on how the government prioritizes and reviews individuals for consideration; the length of time the clearance process takes to review and approve candidates; and the process to pass clearances for briefings.

NERC understands and appreciates the importance of appropriate vetting for security clearances. NERC has received and is provided clearances by federal agencies and appreciates this support. However, in many cases, the long and unclear process results in preventing security professionals from accessing critical information. Different agencies appear to have different requirements for allowing an individual to be processed for a clearance. In addition, there are many challenges when agencies are requested to accept clearances for briefings; the process varies by agency and, in many cases, is unclear. The lack of uniformity across departments in passing clearances has resulted in last-minute negotiations to have clearances passed, and in some cases, individuals having to miss briefings because their clearances were not processed and passed.

Some actions that might make the overall process to obtain clearances more efficient include: ensuring departments have a uniform process or set of requirements for prioritizing and vetting individuals, and communicating this process with industry; determining what causes the significant delays in processing clearances, and addressing those problems; and a uniform process for accepting clearances.

Finally, some departments and agencies are able to provide a one-day "read-on" for SECRET-level briefings, and should extend this practice. This option would enable critical infrastructure leaders to participate in classified briefings once or twice a year to hear information they need to know, rather than have industry members obtain clearances they do not use during the rest of the year. With respect to TOP SECRET (TS) clearances with Secure Compartmented Information (SCI) access, the government should consider providing appropriate industry members with Single Scope Background Investigations, which makes them eligible for SCI

[2] *See* http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

tickets; the government can then issue the tickets as needed, much like the one-day "read-on" concept for SECRET level clearances.

In addition to the challenge of obtaining clearances, classified information needs to be digested at an unclassified level so that industry can act on it. The lengthy "tear line" process to downgrade classified information to be shared at an unclassified level either results in fewer timely and actionable products, or requires more individuals from industry with clearances.

Question 3: How is collaboration through the E-ISAC helpful at improving security? Can you detail how the E-ISAC works with the other ISACs?

Information sharing and collaboration within the electricity sector and across sectors are critical to identifying emerging threats and enable the E-ISAC to provide members with early warnings.

Sharing information provides access to subject matter experts not available at a single organization. As member organizations share information with the E-ISAC, the E-ISAC, in turn, is better able to identify trends that allow members to proactively reduce cyber and physical risk. The E-ISAC provides wide-area situational awareness of cyber and physical security events occurring across the North American grid. Just as system operators rely on real-time tools to identify wide-area events occurring in a control area or across regions, members' cyber and physical security operators rely on information sharing and the identification of a broader coordinated attack through the real-time E-ISAC tools.

After receiving information, the E-ISAC reviews data and conducts various types of analysis, including malware and indicator extraction, campaign link, sector-scale scoping, and sector relevance assessments. This analysis allows the E-ISAC to create a unique dataset to help its members and improve security. Collaborating with the E-ISAC:

- Assists in understanding intent/campaign attribution of indicators: Identifying adversary campaign tactics, techniques, and procedures (TTP) allows the E-ISAC to share specific actions that members can take to mitigate the threat. Additionally, sharing allows the E-ISAC to do predictive analysis on future threat TTPs.
- Assists in reverse-engineering malware or better understanding an event: The E-ISAC has access to closed environment malware analysis systems that perform static and dynamic analysis on files submitted for malware analysis.
- Shares tactical information that can preemptively stop threats by providing mitigation actions: Through member sharing, the E-ISAC has developed actionable indicators and mitigation strategies to reduce members' cyber risk.
- Allows for identifying additional information within the industry or other critical sectors: The E-ISAC works with other ISACs to share indicators of compromise that appear across

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

sectors to include requests for information from cross-sector partners (cross-sector partners include representatives from organizations within other non-energy sectors that overlap with the electricity industry) to help identify threat campaign TTPs.

With respect to other ISACs, the E-ISAC works closely with the Downstream Natural Gas (DNG) ISAC, the Financial Services ISAC, the Communications ISAC, the Information Technology ISAC, and the Multi-State ISAC, to name a few.

In early April, the E-ISAC and the DNG-ISAC launched a more formalized partnership that takes advantage of the growing interdependency and collaboration between the natural gas and electricity industries. Under the partnership, staff from the DNG-ISAC have joined the E-ISAC in Washington, D.C., to improve coordination on potential security risks related to critical electricity and natural gas pipeline infrastructure. The partnership between the E-ISAC and the DNG-ISAC builds on the long-standing efforts of the gas and electricity industries to address supply interdependencies by developing a robust information exchange on shared security risks.

Through a variety of tools, the E-ISAC and DNG-ISAC monitor and analyze potential physical and cyber security threats to their respective industries and use their secure portals to alert and advise members on mitigating actual threats. The goals of the E-ISAC and the DNG-ISAC under the partnership include exchanging information on threats within their industries that have the potential to impact critical infrastructure in either or both industries. Currently, more than 45 percent of the gas utilities represented by the DNG-ISAC are also E-ISAC stakeholders. The partnership has three primary objectives to better serve both industries:

- Improve security collaboration on common threat information and incident response.
- Provide more joint analysis of security concerns and events.
- Advance shared processes for information sharing and situational awareness.

The E-ISAC works closely with other ISACs in one-on-one settings, as well as in formalized settings, such as through its membership with the National Council of ISACs (NCI). The NCI is comprised of 24 ISACs and provides a forum for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response. Sharing and coordination is accomplished through daily and weekly calls between ISAC operations centers, daily reports, requests-for-information, monthly meetings, exercises, and other activities as situations require. The NCI also organizes its own drills and exercises and participates in national exercises.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

Question 4: How closely does the electric industry coordinate with the military, including the National Guard, on the topic of cybersecurity? Are there opportunities to improve that coordination through improved information sharing?

The electricity industry participates with the Department of Defense (DoD) and the National Guard in training exercises such as CYBER GUARD and CYBER SHIELD to practice cyber incident response. Likewise, DoD and the National Guard participate in NERC's biennial GridEx exercise. The E-ISAC has a strong relationship with the National Guard Bureau and encourages utilities to build cyber incident response relationships directly with their local State National Guard Defensive Cyber Operations Elements. These relationships are crucial to mitigating the impacts from a major malicious cyber event and help ensure secure and reliable electricity in North America.

Question 5: At the hearing, you noted that there are energy security challenges posed by distributed energy and other behind-the-meter actions. Please explain.

As more and more power is produced behind the meter, maintaining visibility for operators and addressing the modeling challenges for planners are important. The technical and engineering challenges of integrating distributed energy resources (DERs) on the distribution system are well understood, but the reliability implications on the BPS are less understood. This extends to security as well. The addition of 10,000 smart meters in a neighborhood expands the potential attack surface for malicious actors that could impact the BPS. While NERC's registered entities include some distribution providers that are connected to the BPS, necessary sharing of information associated with the behind the meter DERs, including aggregated resources, will require fundamental changes to modeling, planning, and operations.

The E-ISAC is one way NERC is working to address security challenges behind the meter. Distribution system owners/operators — both within and outside of the NERC footprint — that are members of the E-ISAC are able to securely share information with the E-ISAC and other asset owners and operators to understand current threats and vulnerabilities. They are also able to receive information from a variety of sources that might otherwise be unavailable to them to help better secure their systems. Participation in the E-ISAC fosters a learning environment from which distribution system owners and operators benefit.

Shortly after the first reported Internet of Things compromises in 2016, NERC released a non-public Level 2 alert to industry members. The alert detailed known information about the attack and recommendations for our sector members to evaluate their exposure to these attacks. NERC's E-ISAC also developed a public IoT White Paper[3] which provided recommendations including:

[3] *See Internet of Things DDoS White Paper at* https://www.eisac.com/.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

Industry companies perform the following evaluations:

- Inventory internet-facing devices and examine them for vulnerabilities
- Evaluate business justification for devices that are Internet-facing
- Evaluate protections for utility-owned and managed systems that are exposed to the Internet

We also recommended that companies take the following actions:

- Avoid permitting direct, unprotected, public internet access to ICS devices, to include security cameras, digital video recorders, printers, servers or controllers
- Evaluate entity's Internet address space to discover what components are exposed to the Internet
- Perform risk assessment of exposed devices to determine potential risk

In addition, NERC CIP standards afford protections and safeguards to the "Industrial" Internet of Things where over the past decade we have observed a substantial increase in the number of intelligent devices deployed throughout the bulk power system that, if compromised, could have real impacts to reliability. NERC's CIP standards have evolved to better address new and dynamic threats. As discussed in my testimony and above, Reliability Standards are a necessary foundation to address the vulnerabilities to utilities posed by IoT devices, but they are not sufficient alone to protect against these evolving threats. Monitoring and communication with timely information exchange is essential.

Question 6: At the hearing, you noted that the industry has previously prepared unclassified information and presented that information to the federal government – only to have the federal government decided to classify that information, thus precluding its wide-spread use throughout the industry. Please expand upon this problem. Do you have any suggestions to address this situation?

Industry and the E-ISAC regularly present information to our federal government partners to understand what the government has seen or knows with respect to various threats. Some of the information, while unclassified, may link to other open source information and methods, which then—from the government's point of view—pushes information from an unclassified to a classified level.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

We believe we can have discussions at a classified level to keep sources and methods protected; however, we also need to work with our government partners to bring the conversations to an unclassified level so that those industry members who do not have clearances can have access to critical information, understand the security implications, and be given clear, actionable guidance on how to address the security issues.

Questions from Senator Ron Wyden

Question 1: Mr. Cauley, as we discussed during the hearing, I think we both agree that more mock penetration tests, such as the Houston "red teaming" event I described, are needed to better secure the grid. What additional measures could be implemented to promote further penetration testing, building on the vulnerability assessment requirements in existing NERC standards?

Penetration testing is a common practice employed by businesses to test physical and cyber security, including in the electricity sector. As you point out, NERC standards do require periodic vulnerability assessment. For instance, under CIP-010-2, operators of medium and high impact cyber systems must conduct a vulnerability assessment at least once every 15 months. The standard provides flexibility in how entities meet this requirement. "Red-teaming" is one approach used by industry to meet their compliance obligations. NERC evaluates the rigor of the vulnerability assessments performed to ensure they are effective at illuminating how vulnerabilities could be exploited and more importantly, how to safeguard the systems from an actual penetration.

Additional penetration testing could be achieved by working with industry groups to develop guidance for performing red-team exercises that clearly outline the terms of a red-team engagement. Such guidance would establish the approach, coordination, communication and methodology used to perform the test in accordance with the CIP standard's required vulnerability assessment. In addition, NERC can poll industry volunteers to share their results privately to other stakeholders to encourage greater voluntary participation in red-team exercises. NERC then can use this information in an anonymized manner in our outreach efforts.

Question 2: Mr. Cauley, I believe the smart policy the electricity sector needs is one where both cybersecurity and privacy concerns are met. And while I know that NERC and FERC do not formally have jurisdiction over distribution grid assets, I'm happy to hear you share my concern for the risk to the bulk power system created by distribution-level devices, including Internet of Things devices. Could you offer some suggestions on work that could be done, at NERC or elsewhere, to help secure the grid while guaranteeing privacy protections?

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

As more and more power is produced behind the meter, maintaining visibility for operators and addressing the modeling challenges for planners are important. The technical and engineering challenges of integrating distributed energy resources (DERs) on the distribution system are well understood, but the reliability implications on the BPS are less understood. This extends to security as well. The addition of 10,000 smart meters in a neighborhood expands the potential attack surface for malicious actors that could impact the BPS. While NERC's registered entities include some distribution providers that are connected to the BPS, necessary sharing of information associated with the behind the meter DERs, including aggregated resources, will require fundamental changes to modeling, planning, and operations. When addressing security of devices that may contain customer data, maintaining privacy protections is important.

The E-ISAC is one way NERC is working to address security challenges behind the meter. Distribution system owners/operators — both within and outside of the NERC footprint — that are members of the E-ISAC are able to securely share information with the E-ISAC and other asset owners and operators to understand current threats and vulnerabilities. They are also able to receive information from a variety of sources that might otherwise be unavailable to them to help better secure their systems. Participation in the E-ISAC fosters a learning environment from which distribution system owners and operators benefit.

Shortly after the first reported Internet of Things compromises in 2016, NERC released a non-public Level 2 alert to industry members. The alert detailed known information about the attack and recommendations for our sector members to evaluate their exposure to these attacks. NERC's E-ISAC also developed a public IoT White Paper[4] which provided recommendations including:

Industry companies perform the following evaluations:

- Inventory internet-facing devices and examine them for vulnerabilities
- Evaluate business justification for devices that are Internet-facing
- Evaluate protections for utility-owned and managed systems that are exposed to the Internet

We also recommended that companies take the following actions:

- Avoid permitting direct, unprotected, public internet access to ICS devices, to include security cameras, digital video recorders, printers, servers or controllers

[4] *See Internet of Things DDoS White Paper at* https://www.eisac.com/.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

- Evaluate entity's Internet address space to discover what components are exposed to the Internet
- Perform risk assessment of exposed devices to determine potential risk

In addition, NERC CIP standards afford protections and safeguards to the "Industrial" Internet of Things where over the past decade we have observed a substantial increase in the number of intelligent devices deployed throughout the bulk power system that, if compromised, could have real impacts to reliability. NERC's CIP standards have evolved to better address new and dynamic threats. As discussed in my testimony and above, Reliability Standards are a necessary foundation to address the vulnerabilities to utilities posed by IoT devices, but they are not sufficient alone to protect against these evolving threats. Monitoring and communication with timely information exchange is essential.

Question 3: Mr. Cauley, I asked the witness panel to express their views on encryption. It is my belief that weakening encryption used on the electricity grid, and in other aspects of our energy infrastructure, would be outlandishly bad judgment – and I have made it clear that I will fight this every step of the way. Do you believe encryption plays an important role in protecting the electricity grid? Please explain your answer.

Encryption and other security processes play an important role in protecting the electric grid. Organizations may consider use of encryption tools that conform to the National Institute of Standards and Technology Advanced Encryption Standard specifications, and not requiring government key escrow.

Encryption is fundamental to maintaining the confidentiality and integrity of the control data used to manage the electric grid. However, we also believe that companies should use a combination of tools to safeguard information, such as multi-factor authentication. Adversaries are becoming more advanced, and we need to continue to be agile. As new technologies become available, we need to assess their abilities to help us better protect our systems.

Questions from Senator Joe Manchin III

Question 1: Today, our reliability organizations and electric utilities are tasked with maintaining our electric grid in an increasingly challenging environment. A perfect storm of factors has put baseload units at risk and states are more frequently using out-of-market solutions to rescue these units and ensure their citizens and businesses have reliable affordable electricity.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

In the meantime, aging infrastructure, extreme weather events, the threat of cyber attacks, a rapidly changing fuel mix, and overregulation are increasingly testing our nation's electric grid. Several times throughout the month of January 2014, the upper Midwest and Mid-Atlantic experienced temperatures below zero. The Eastern portion of the PJM grid flirted with rolling blackouts. On January 7, a winter record was set when 141,132 megawatts of electricity was used. PJM, the nation's largest grid operator oversees 180,000 megawatts. That's cutting it pretty close in my book.

Interestingly, following the winter of 2014, AEP reported that nearly 90% of its coal plants scheduled for retirement ran during the Polar Vortex. Coal helped keep the lights on. Last week, PJM released a report that said it could keep the lights on with a generation portfolio that is 86% dependent on natural gas. Current installed capacity is 33% coal, 33% natural gas, 18% nuclear and 6% renewable. But more of that coal is going to be retired.

I understand that your organization's reliability assessment from last year did not flag PJM as having major near term reliability issues but I've got to ask, is PJM correct? It seems highly risky to depend 86% on one fuel in an environment when all we talk about is fuel diversity.

Based on data received for the 2016 NERC Long-Term Reliability Assessment (LTRA),[5] it is projected that in 2017 natural gas will comprise 35.8 percent of PJM's peak season total anticipated capacity. By 2021, this will increase to 38.7 percent. PJM has a reference margin level of 16.5 percent and exceeds that margin with an anticipated reserve margin of 31.1 percent in 2017 and 24.5 percent in 2026. For the next ten years the compounded annual peak demand growth rate in PJM is expected to be 0.5 percent. This analysis shows that PJM is expected to have adequate reserves to maintain reliability. As a result, PJM was not flagged as having any significant near-term capacity supply issues.

In *PJM's Evolving Resource Mix and System Reliability* report, PJM states that portfolios composed of up to 86 percent natural gas-fired resources maintained operational reliability. It is important to note that this scenario was run as part of a PJM resilience analysis, but is not reflective of their anticipated or prospective resources over the next ten years. In other words, it provides a sensitivity analysis around resource adequacy implications. While there are differences between the NERC and PJM analyses, NERC agrees with the overall conclusions of the PJM analysis, particularly as a platform to discuss policy implications to electricity and natural gas planning and regulatory processes.

[5] http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2016%20Long-Term%20Reliability%20Assessment.pdf

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Gerry Cauley

What do regulators need to do to help move natural gas into a position where it can serve as baseload and provide the 24/7 reliability attributes that coal and nuclear power offer?

To achieve attributes similar to coal and nuclear, baseload generation from natural gas requires firm transportation, dual fuel capability, and backup fuel. In NERC's 2016 Long-Term Reliability Assessment, NERC recommended that as natural-gas-fired resources continue to increase, system planners and operators should evaluate the potential effects of an increased reliance on natural gas as it pertains to BPS reliability. Natural gas provides "just-in-time" fuel; therefore, firm transportation and maintaining dual-fuel capability can significantly reduce the risk of common-mode failure and wider-spread reliability challenges. As part of future transmission and resource planning studies, planning entities will need to more fully understand how impacts to the natural gas transportation system can impact electric reliability. Regulatory action may be needed to better calibrate the growing interdependency of the electric and gas industries, considering regulatory differences in how infrastructure is planned, with reliability given due consideration.

As part of our consideration of gas-electric interdependence, NERC is in the process of developing a report on single points of disruption that analyzes the potential loss of a storage facility, natural gas pipeline, or LNG deliverability to gas-fired electric generators. This report is expected to be released in August, 2017.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Duane D. Highley

Questions from Chairman Lisa Murkowski

Question 1: The previous Administration's QER targeted the distribution level as an area requiring increased federal authority even though historically that has been the purview of the states.

a. **Is it correct that NERC's registry – the list of utilities and organizations required to comply with these mandatory reliability standards and that are subject to penalties of up to $1 million per day per violation – already captures those distribution assets that could impact the reliability of the Bulk Power System (BPS)?**
Yes.

b. **What are the challenges for a small rural cooperative to comply with the NERC standards? Is it a matter of funding? Personnel?**
Both. The few dozen smaller rural distribution cooperatives that have NERC standard compliance obligations are often faced with limited financial resources and a limited pool of qualified candidates to fill these key positions. Because of their smaller customer base, any costs, including those for compliance with NERC standards, are directly distributed across the member consumers, thereby increasing the cost borne by each of them. For this and other related reasons NERC is working with DOE to develop lower-cost solutions for small systems. The cooperative's trade association, NRECA, has received DOE funds under the DOE's *Improving the Cyber and Physical Security Posture of the Electric Sector* initiative to develop a three-year program for cooperatives called the Rural Cooperative Cyber Security Capabilities Program (RC3). RC3 is designed specifically to assist small- and mid-sized cooperatives in improving their cyber defense capabilities.

Question 2: Obtaining the appropriate clearance for cyber security professionals seems to be a challenge for the private sector.

a. **What do you see as the biggest challenge to the issuance of clearances?**
The biggest challenge for the private sector is the speed at which the government is processing clearances. What is causing this is a harder question. There are likely many contributing factors including the establishment of the National Background Investigations Bureau (NBIB) within OBM starting in October of 2016, reactions to federal data breach events, and other causes that we are not aware of. As co-chair of the ESCC, with a need to meet regularly with our government leaders on critical infrastructure cyber and physical security policy issues, I have had a TS-SCI clearance request pending since November 2016 with no response yet as of April 2017.

b. **What do you recommend to make this process more efficient?**

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Duane D. Highley

It would be useful to have an assessment and clear guidance on how, who, and when security clearances are given to critical infrastructure owners and operators under existing processes and procedures. This would enable industry and government stakeholders to have a benchmark that can be used to measure how any new processes can improve the time needed to process and receive a clearance, and to evaluate whether the critical infrastructure owners and operators are getting the appropriate level (secret, top secret, TS-SCI, etc.) clearances to receive the right information at a level and detail needed for it to be timely and actionable.

Question 3: Prior to leaving office, former Energy Secretary Moniz expressed interest in receiving Congressional authority for the Energy Department to direct utility action in the case of a natural disaster. You testified that the utility sector has vast experience responding to weather events and that "decades of lessons learned from supplying power" has led to the development of hazard recovery plans for industry and the government to work together in these situations. Is additional federal authority needed in this area? Why or why not?

The existing authorities, including the FERC/NERC Standards process and DOE Emergency Authorities, are sufficient in this area. As mentioned in my written testimony, these authorities allow for engagement with industry owners and operators, the experts of the systems, to cohesively identify functional solutions or standards to address threats. In the event of an emergency there are existing authorities in place, including the ability for DOE to direct emergency action to be taken when an emergency or imminent threat is declared. In such an event, the efforts of the public private partnerships in preparing for such situations would be stood up.

Question 4: Your written testimony notes that "[o]ften news headlines about cyber or physical threats to the electric grid focus on far-fetched scenarios or sensationalized claims…Many of the more dramatic scenarios would constitute acts of war on the United States that would directly impact more than just the electric sector." Are you referring to Electromagnetic Pulses (EMP)? Please explain.

EMP is one of most common sensationalized doomsday scenarios predicted for the grid and other critical infrastructures. An EMP event impacting the bulk electric system would likely be sponsored by a foreign enemy and/or nation state. Government has great resources for gathering intelligence and fighting wars. Now that private critical infrastructures like the energy industry are at the front lines of possible attack, we need a stronger partnership with our government defense and intelligence-gathering agencies to provide us with timely and actionable information that we can use to protect our critical infrastructure. My point in making this statement is to highlight that both government and industry need to partner in preparing for and responding to all hazards and not just those that get the most press and public attention. It is advantageous for industry and government to be proactive in building these relationship rather than reactionary.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Duane D. Highley

Question 5: **You note in your testimony that the ESCC has led to the formation of a Cyber Mutual Assistance (CMA) Program, akin to the industry's longstanding mutual assistance agreements to respond to emergency. The CMA will allow companies to share critical personnel and equipment in the event of cyber-related emergencies. To date, there are enough utilities participating to cover about 80 percent or 118 million electricity customers.**

a. **What are the barriers to full participation by the electric industry?**
Because this is a voluntary program, some utilities may choose not to participate, perhaps because they feel that they already have sufficient resources, or alternately because they feel that they do not have sufficient resources to offer help to others. Through communications with entities at both ends of that spectrum we can help them understand the benefits of participation. In addition, increasing access to cyber security training, such as that provided by DHS at the Idaho National Laboratory, will raise the capabilities of all the participants in CMA to provide assistance to one another.

b. **How long until you expect participation by more than ninety percent of the utilities?**
Since participation is voluntary this cannot be known with certainty. The ESCC is working to achieve a higher level of participation by year-end. NRECA's RC3 Program mentioned earlier is specifically looking at ways to increase participation by small- and mid-sized electric cooperatives.

c. **Can mutual assistance be expanded to include gas industry assets?**
Yes, to the extent that there are common control platforms deployed it would be of mutual benefit for us to partner on this.

Question 6: **Your written testimony identified two areas where you call for statutory "fixes": (1) to give the FBI authority to assist industry with fingerprint-based, criminal and terrorist background checks for certain industry personnel and (2) to clarify that a DHS declaration of a "qualifying cyber incident" bestows liability protections under the 2002 Support Anti-Terrorism by Fostering Effective Technologies Act. Neither of those asks are within ENR's jurisdiction but please elaborate for the Committee on why you believe further Congressional action in these areas is necessary. Have you encountered any opposition to these proposals? Given the backlog of FBI work on security clearances, do you think the Bureau has the resources to assist industry in this manner?**

Though we have not encountered any opposition as of yet to these proposals, per se, we have also not seen much movement on them. Part of the issue with the SAFETY Act clarification is twofold: some believe the protections already cover significant cyber incidents and no additional action is needed, and some believe that the existing language is sufficient and DHS's SAFETY Act Office simply needs to put out guidance providing the clarification.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Duane D. Highley

As to the FBI assistance in addressing the insider threat for electric utilities, the security clearance backlog should not be reflective of their ability to assist with this. The FBI is not the lead agency that provides the private sector with security clearances and is typically not considered responsible for the backlog. Based upon discussions we have had through the ESCC with the FBI to date, we believe the FBI will be supportive of this concept and that they have the capacity to provide the assistance.

Questions from Senator Ron Wyden

Question 1: Mr. Highley, in your written testimony, you mention that a "one size fits all" cybersecurity solution is unlikely to be effective for the electricity grid. For instance, as you explain, security issues for the bulk power system may differ significantly from the issues facing the distribution grid. Intel, which has offices in Oregon, expects there to be 200 billion Internet of Things devices connected to the web by 2020. This would include technologies involved in managing distributed energy resources, such as rooftop solar, smart appliances and electric vehicles. Can you please provide a brief description of some of the differences between the cybersecurity issues facing the bulk power system and the issues facing the distribution grid? Can you also please provide specific suggestions for how the federal government can work together with industry to help secure the explosion of devices that we expect on the distribution grid?

Utilities with assets that could potentially affect the Bulk Electric System (BES) are required to comply with mandatory, enforceable standards (Critical Infrastructure Protection, or CIP, standards as well as potentially other reliability standards). CIP covers both cyber and physical security in the NERC standards. As mentioned in the testimony of Mr. Cauley, these standards are developed at NERC utilizing a NERC/FERC-approved standard development process (and sometimes at the direction of FERC). Industry subject-matter experts develop the standards through use of the NERC/FERC process. Draft standards must then receive industry, NERC and FERC approval before they are considered mandatory and subject to NERC and Regional Entity audits and enforcement.

Most assets on the distribution system serve a localized area and are not considered by NERC to have the ability to impact the Bulk Electric System. The cyber risk profile at the distribution level is much lower than that of the BES, with generally fewer automated devices under remote control and fewer customers potentially impacted.

The industry, through the Institute of Electrical and Electronics Engineers (IEEE), is developing standards for the secure design of IoT devices[1]. They also offer education of design best-practices through the IEEE Center for Secure Design[2]. The government could support these

[1] P2413 - Standard for an Architectural Framework for the Internet of Things (IoT), https://standards.ieee.org/develop/project/2413.html
[2] IEEE Center for Secure Design, http://cybersecurity.ieee.org/center-for-secure-design/

efforts by partnering with IEEE in this work, leveraging the capabilities of DOE and the National Labs to assist IEEE researchers.

Question 2: Mr. Highley, I asked the witness panel to express their views on encryption. It is my belief that weakening encryption used on the electricity grid, and in other aspects of our energy infrastructure, would be outlandishly bad judgment--and I have made it clear that I will fight this every step of the way. Do you believe encryption plays an important role in protecting the electricity grid? Please explain your answer.

Communications to and from BES control centers and remotely operated facilities are required by NERC CIP standards to be on secure networks protected from the internet and from the utility's enterprise networks utilizing defense in depth protection schemes. Encryption is one of the options that can be used in these instances.

Question from Senator Steve Daines

Question: In Washington, DC we often forget about the rural part of our country. However, as you have stated in your testimony, our rural electric coops serve 75% percent of the nation's land mass. When speaking about tools and regulations we cannot forget this important piece of our infrastructure. It is even more important to remember that in Montana these small rural electric coops provide electricity to our ICBM's. Making it even more critical that they have adequate tools and guidance from the federal government. I have heard that current federal programs are not scalable or do not take into consideration the unique size and nature of our small and rural coops in Montana.

What tools are currently available for our small, rural coops to protect them from cyber threats, and what more can we do to make sure they are equipped to handle a cyber-attack?

I appreciate your question. Getting cyber security resources into rural areas can be challenged by the financial limitations of the cooperatives, the lack of options in cyber security providers and services that frequently occur in remote areas, and the lack of tools that are appropriate for smaller utilities that may have limited information technology staff. In addition to the tools and resourced mentioned in my written testimony that are available for the industry, there are efforts underway to engage directly with the smaller utilities. It is also important to realize that electric service provided to these ICBM facilities is nearly always at the local distribution level of the electric system. It is critical for the appropriate DOD and any other federal entities to reach out and establish ongoing relationships with the CEO/General Managers at the distribution cooperatives that provide electric service to the important facilities. Working closely together, the local distribution cooperative leadership and DOD officials can address the specific needs related to electric service to these facilities.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Duane D. Highley

Information sharing is a key tool in helping utilities identify and respond to cyber security threats. In addition to the Cyber Security Risk Information Sharing Program (CRISP), which was started with DOE funding and is now funded and managed by NERC and the E-ISAC, additional cyber security information sharing resources are needed. CRISP provides cyber security threat information and situational awareness to CRISP members, but CRISP membership is too expensive for many cooperatives to join. Through the E-ISAC, anonymized and more generalized CRISP-related information is provided to all entities signed up to receive E-ISAC reports, warnings, etc. However, NERC and the E-ISAC recognize these limitations and there are efforts underway at NERC, E-ISAC, DOE, and within NRECA to develop lower-cost information sharing options that can be used by utilities that have minimal or no cyber security experts on staff. Developing affordable and effective information sharing technologies and resources that meet the needs of small- and mid-sized utilities can benefit many of our members.

Recently the Department of Energy's Office of Electricity Delivery and Energy Reliability provided funding to NRECA and APPA to develop and implement programs to help small utilities, such as cooperatives and small municipals, to improve their cyber security capabilities. NRECA has used these funds to develop the Rural Cooperative Cyber Security Capabilities Program (RC3). RC3 is a comprehensive program developing tools and resources specifically designed for small- and mid-sized utilities to improve their cyber security posture and resilience. The Program emphasizes the separate but interdependent roles of people, processes, and technologies, recognizing that building resilience into a cooperative's cyber security program will require more than technological advances, and that, like safety, cyber security is a team effort.

A fundamental goal of the RC3 Program is to build tools, resources, and relationships that will last beyond the funding and will scale beyond the cooperatives that participate directly as part of the deployment and demonstration efforts. Many of the resources and tools developed under the RC3 Program will be publically available, and will be useful not just to small electric cooperative utilities, but to all small- and mid-sized utilities. In addition, the Program is developing resources for utilities at different stages of maturity in their cyber security programs. When a cooperative masters one set of resources appropriate for utilities at one maturity level, there will be another set of relevant resources to enable them to continue their efforts to reach the next maturity level. NRECA's cyber security staff believe that in order to meet the ever-changing threat landscape, a strong cyber security program is based on continual improvement, not a one-time-only effort. The RC3 program has been well received by our members, and we encourage Congress to continue to support DOE and our efforts for the full three-year period the Program has been designed to cover.

Questions from Senator Joe Manchin III

Questions: I think we would miss an opportunity if we did not mention electromagnetic pulses (EMPs) and the potential havoc they could wreak on our electric system. In the

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Duane D. Highley

Senate Energy Committee we included the "GRID Act" in the Energy Policy Modernization Act which would have directed the Secretary of Energy to develop the Department's technical expertise in the protection of electric systems (generation and transmission) against geomagnetic storms or malicious actors who use EMPs. There was similar legislation in the House.
Understanding that these EMPs could be manmade or intentional, I'm curious as to what technologies exist today and what technologies you are exploring to address this potentially devastating type of event.

What is your organization doing to protect against the threat of EMPs – naturally-occurring or intentional?

First, I would like to clarify why I did not mention EMPs in my written testimony. An EMP is typically viewed as a physical security threat rather than a cyber security threat, which was the focus of the hearing. Though an EMP can negatively impact the microprocessors in any critical infrastructure, as well as devices in a home or throughout a community, the impacts do not take a cyber route – an analogy might be if someone blew up a substation, we'd lose the electronics but NOT because of an attack in cyberspace. Second, it is important to understand that EMPs and geomagnetic disturbances (GMDs) from the sun are significantly different. GMDs are often referenced incorrectly as "natural" EMPs but they are not. They differ not only in the likelihood of occurring – lower impact level GMDs happen pretty much every week – but also in their causes, impacts, mitigation options, damage types, and warning times. Not to mention one, an EMP, would be an act of war, while the other, a GMD, is not initiated by a malicious actor and the electric industry already has standards to mitigate the impacts.

Arkansas Electric Cooperative Corporation, along with more than a dozen utilities, have voluntarily funded a multimillion dollar three-year research initiative at the Electric Power Research Institute (EPRI), in partnership with government entities, in order to determine the specific nature of the EMP threat, based on objective evidence, and to develop cost-effective strategies for mitigating the threat. Based on the outcome of this research we will evaluate our system for potential mitigation. This work was initiated at the request of the ESCC based on discussions with our Federal counterparts. The private sector stepped up to fund this research because of our concern with the threat, and also because we were unable to access the classified testing which has been performed at the National Labs. This classified testing could be of a tremendous benefit to industry but the results are not available for our use.

I believe Faraday cages have been used for many years to protect electronics and computer solutions. Is that a solution that can be explored for our bulk power system? Or is this a solution for the customer side?

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Duane D. Highley

Based on a recent study prepared published by Schweitzer Engineering labs[3], I believe that Faraday protection may be one of many potential solutions in combination with substation wiring and grounding practices, which could cost-effectively protect sensitive power electronics. Unfortunately the Schweitzer report was prepared based on public-source EMP waveform data; access to the classified EMP waveforms would better inform the study and allow industry to better prepare for cost-effective mitigation. However, industry has been unable to obtain access to this classified data from DOE.

The Schweitzer report also concludes, by testing and analysis, that commercially-available intelligent electronic devices designed to meet IEC (International Electrotechnical Commission) requirements are resilient to High-altitude Electromagnetic Pulse (HEMP) events. They also conclude that existing IEEE (Institute of Electrical and Electronics Engineers) substation design standards are sufficient to protect intelligent electronic devices from HEMP.

[3] *Understanding Design, Installation, and Testing Methods That Promote Substation IED Resiliency for High-Altitude Electromagnetic Pulse Events*, Tim Minteer, Travis Mooney, Sharla Artz, and David E. Whitehead, Schweitzer Engineering Laboratories, Inc., February 2017.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to the Honorable Dave McCurdy

Questions from Chairman Lisa Murkowski

Question 1: Obtaining the appropriate clearance for cyber security professionals seems to be a challenge for the private sector.

a. What do you see as the biggest challenge to the issuance of clearances?

Response: Clearances for private sector individuals who do not work for the federal government pose several questions and challenges. It appears that executives or others that may need access, as a "need-to-know" about specific physical or cyber security threats that affect their enterprise, presents an unusual category for clearance, i.e. most applying for clearance either work directly for or are contractors providing service to government. Standard Forms (SF) ask if you are an employee or contractor.

An additional challenge is that there are different processes for a DoD versus a DOE clearance. DoD has its own investigative agency, DOE does not. DoD and the intelligence community (IC) also have different security classifications than DOE. Whether it is a backlog of investigations, insufficient staff support or budget concerns, it should not take 18 months or longer to process clearances.

Per Senator Heinrich's questions in the hearing regarding my personal experience with clearance process, seven days after the Senate hearing, I personally received a call from the DOE security office to proceed with the process to elevate from a secret level to SCI level clearance. Even with their personal attention and expedited action, it will be over forty days from contact after the hearing to reach the final step of issuance of security badge.

Beyond the process of submitting the appropriate paperwork forms, you must go through the physical ID process (fingerprinting, etc.), and then a later scheduled briefing for SCI paperwork forms and an "indoctrination briefing." There is also a need to designate the sponsor agency which has ownership and incentive to move the application. In my case, I held a secret clearance from one agency, that was held by an outside sponsor which is now being switched to DOE to facilitate the process. If it takes more than a year for a person with a secret clearance (and intelligence and national security background) to be granted a higher clearance, logic would dictate that a private citizen or partner, such as a corporate executive, will question the lengthy and bureaucratic process. I am aware of two instances of Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC) leaders in the process for TS-SCI for more than two years without final adjudication and grant.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to the Honorable Dave McCurdy

Furthermore, there appears to be no procedure to find out the status of the clearance application.

b. What do you recommend to make this process more efficient?

Response: Ensure that there is a special category for a private citizen that has a need-to-know but is not an employee or contractor, and a designated sponsor agency with sufficient resources to conduct the investigation and grant the clearance. It would also help to consolidate the physical ID process and the clearance indoctrination briefing. In the private sector, we prefer a one-stop procedure. In addition, providing a defined process to ascertain the status of clearance process would be helpful.

Question 2: NERC has been directed by a FERC order to develop a standard on supply chain vulnerabilities.

a. How is the gas industry addressing supply chain?

Response: AGA has worked with its member companies to encourage use of the Cybersecurity Procurement Language for Energy Delivery Systems[1] guidance document. This resource "complements other cybersecurity efforts by providing organizations that acquire, integrate, and supply energy delivery systems with guidance on how to communicate cybersecurity expectations in a clear and repeatable manner." Building on this resource, AGA developed a Cybersecurity Procurement Language Tool for AGA members to assist them with identifying cybersecurity contract provisions for the procurement of hardware, software, and services relevant to natural gas operations and as appropriate for their tolerance of risk. Including cybersecurity as a requirement from the beginning is a critical step to enforcing supply chain security.

b. Has the gas industry paid attention to developments in the NERC process?

[1] This document was prepared by the Energy Sector Control Systems Working Group (ESCSWG), Pacific Northwest National Laboratory (PNNL), and Energetics Incorporated, with funding from the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) Cybersecurity for Energy Delivery Systems (CEDS) program, and in collaboration with the U.S. Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Duke Energy, Edison Electric Institute (EEI), the Electric Power Research Institute (EPRI), the Federal Energy Regulatory Commission (FERC), the Independent Electric System Operator (IESO) in Ontario, and the Utilities Telecom Council (UTC). Contributions were also provided by the American Public Power Association (APPA), American Gas Association (AGA), and Idaho National Laboratory (INL).

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to the Honorable Dave McCurdy

Response: Natural gas utilities apply a portfolio of security standards, products, and practices for a robust cybersecurity management program. Predominantly referenced is the Transportation Security Administration (TSA) Pipeline Security Guidelines and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. NERC products/standards are also referenced as applicable to natural gas operations. Given gas utility operations do not fit a single mold, the flexibility to select leading industry practices and standards allows the operator to go above a baseline level of security management. Also, a majority of AGA Member utilities have electric *and* gas, and there is close downstream energy coordination between the two subsectors. As such, gas utilities have a vested interest in NERC initiatives.

c. It seems the supply chain issues for the military would be the most advanced, given the need for critical defense systems to be manufactured in trusted locations. Has the gas industry paid attention to how the military is working to ensure security within its supply chain?

Response: There is a significant difference between defense system manufacturing and civilian system manufacturing. The private sector does not have the authority to dictate supply chain integrity requirements. Federal laws do not permit the private sector to collectively boycott a manufacturer that does not meet cyber integrity criteria. We can choose not to go with that vendor, but we cannot as an industry do this as the military may. The gas industry is in its own way educating the vendors/manufacturers of our cyber integrity needs and are using the AGA Cybersecurity Procurement Language Tool help drive these efforts.

Question 3: The electricity sector has a prominent Subsector Coordinating Council (SCC) known as the ESCC and comprised of electric sector CEOs that interacts with government leaders in order to better secure energy infrastructure.

a. Can you describe who sits on the similar SCC for the Oil and Natural Gas industries?

Response: The ONG SCC is staffed by physical security and cybersecurity leaders of member companies and pertinent trade associations, as well as the leadership of sector ISACs. Designated ONG SCC representatives have been empowered by their respective organizations to make decisions to effectuate ONG sector security policy and strategy. The representatives of the ONG SCC have proven time and time again that in time of need, they are able to bring their corporate leadership to the table. More importantly, the downstream energy coordination initiatives between the

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to the Honorable Dave McCurdy

ONG SCC and ESCC reinforce active engagement by the necessary levels of corporate leadership.

b. How many CEOs are members? How many are President of the Company?

Response: As stated above, membership of the ONG SCC consists of industry representatives designated by their top executive leadership to ensure their companies' interests are addressed and opportunities are identified for further action.

a. How would you describe the impact on security between the ESCC and ONG SCC? Downstream energy coordination is where the ONG and Electricity Sectors overlap.

Response: Our nation's critical infrastructure sectors are highly interdependent and as such, the ESCC and ONG SCC are also interdependent. Because so many gas distribution and transmission companies are combination gas/electric companies, this coordination is more than just a critical need. It's a corporate responsibility and necessity.

b. How many joint meetings have the ESCC and ONG SCC held?

Response: None to my knowledge.

c. Have you invited both FERC and DOE to the ONG SCC meetings?

Response: The ONG SCC meets regularly with the Energy Government Coordinating Council (GCC). This meeting is co-led by DOE, DHS, and the ONG SCC chairperson. This is more than a report-out or status meeting; rather it is a working meeting providing the opportunity for active engagement between the ONG SCC members and government representatives. TSA, U.S. Coast Guard, FBI, and the DHS Infrastructure Security Compliance Division always participate in these meetings. Only in more recent years has FERC accepted the invitation and attended. Further, many of DOE's security-related initiatives have been the result of ONG SCC support and partnership. So, not only is DOE present at joint meetings, but the ONG SCC is an advocate of DOE security initiatives which demonstrate value to the sector.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to the Honorable Dave McCurdy

Question from Senator Ron Wyden

Question: Mr. McCurdy, I asked the witness panel to express their views on encryption. It is my belief that weakening encryption used on the electricity grid, and in other aspects of our energy infrastructure, would be outlandishly bad judgement--and I have made it clear that I will fight this every step of the way. Do you believe encryption plays an important role in protecting the electricity grid? Please explain your answer.

Response: Encryption is one of many important tools in a defense-in-depth strategy employed by energy delivery companies. We have recently provided two educational webinars to our members on the quantum computing issue which threatens current encryption methods due to the exponential increase in computing power adversaries now possess. We intend to remain a resource in assisting natural gas delivery companies in utilizing strong encryption schemas in addition to other cybersecurity policies, practices and technologies to help secure their energy delivery systems.

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

Questions from Chairman Lisa Murkowski

Question 1: Obtaining the appropriate clearance for cyber security professionals seems to be a challenge for the private sector.

a. What do you see as the biggest challenge to the issuance of clearances?

INL observes that the most impactful challenge is availability of Office of Personnel Management investigators within INL's region of the country. The growth of INL's Homeland & National Security programs that require a security clearance has increased, and this trend is anticipated to continue. New employees are waiting 18-24 months for their clearance, and transfer of clearances between employing organizations are unpredictable. Some transfers occur immediately while others may take as long as 6-9 months.

Other challenges with the issuance of clearances primarily arise from the due diligence efforts of federal and contractor efforts to manage security risks. These challenges are encountered in our efforts to:

- Obtain sufficient 'prior-to-clearance' personnel privacy information within fair labor standards to better identify candidates who will eligible for security clearances;
- Select subcontractors and external private sector advisors that are not operating under "Foreign Ownership, Control or Influence" (FOCI);
- Resolve need-to-know access for National Security Information (NSI) requiring a Secret or Top Secret clearance relative to DOE clearance processes for Restricted Data (RD) requiring a "L" or "Q" clearance; and
- Provide physical access to the security infrastructure for cleared personnel who do not reside within immediate reach of our counterintelligence officers and our secured facilities, phones, and networks.

b. What do you recommend to make this process more efficient?

INL is supportive of addressing any efficiency which may be administered at a laboratory level with the understanding that issuing security clearances and dissemination of classified information are inherently federal decisions.

As such, INL within the thresholds our national laboratory's Government-owned/Contractor-operated (GOCO) authorities, routinely seeks opportunities to overcome challenges in the issue of clearances. We implement practices to obtain appropriate and relevant information earlier in the hiring and subcontracting processes. This allows the laboratory to optimize the use of resources for those individuals eligible for clearances and minimizes efforts pursuing clearances for ineligible persons and businesses. INL continues to improve federal-GOCO communication pathways to minimize delays when current inter-government agency 'reciprocity' can be applied to transition Secret/Top Secret clearances to DOE L/Q clearances. INL recently adopted a new employee orientation process to assist new employees to better complete security clearance questionnaires prior to starting their work assignments.

Question 2: In his testimony, Colonel Welsh highlighted that "federal efforts have principally emphasized efforts to prevent cyber attacks, rather than anticipate response considerations." What if anything are the national laboratories doing to be prepared in the event of a successful cyber intrusion?

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

National laboratories are working with federal agencies to solve current challenges, enhance protection measures, and take important steps to improve the security of the Nation's most vital critical infrastructure systems.

There are a number of DOE, Department of Homeland Security, and national lab initiatives underway that are intended to bolster U.S. energy sector cyber response capabilities. These initiatives address a broad spectrum of anticipatory actions including, and not limited to:

- Conducting research into next generation secure digital architectures, automated intrusion detection and response tools, intelligent resilient response methodologies, etc.;
- Sharing expertise during on-site vulnerability assessments, training and exercising; and
- Building a DOE core capability to respond and restore the grid during a major event.

In addition to examples provided in the submitted written testimony, additional examples include:

1. *National Grid Exercise Support:*

   INL and Pacific Northwest National Laboratory have supported the North American Electric Reliability Corporation's biennial national grid exercises, GridEx, including the next exercise planned for November of 2017. Conducted in 2015, GridEx III saw hundreds of utilities, dozens of regional coordinators and balancing authorities, and interagency participation. Overall, thousands of combined participants worked through challenging cyber and physical attack "injects" to test their response plans and procedures. INL's grid and power systems expertise and access to relevant grid systems is instrumental in assisting in the creation of realistic "injects" for the exercise. After action reports included lessons learned and recommendations for improvement that will inform the development of subsequent versions of the exercise. This year's GridEx IV will be more challenging, bring an increasingly cross-sector orientation to the conduct of the exercise, and include more participants than prior events. When invited, national laboratories, like INL, also support cyber exercises conducted by individual utilities, such as one performed by California utility Pacific, Gas & Electric (PG&E) in 2016.

2. *INL supports ICS-CERT capabilities providing utilities with situational awareness, site assessments that support preparedness, and fly-away response teams:*

   INL provides subject matter experts, facilities and other resources to support DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), as it serves U.S. electric utilities and other critical infrastructure owners and operators. Some of ICS-CERT's most important cyber response functions include fly-away teams of ICS cyber experts who can be called in to assist with forensics and restoration after an attack. INL also continues to improve our capabilities to respond over-the-phone and in-the-field by performing research in innovative modeling and simulation tools to perform better diagnostics and accelerate the training and education of our response experts.

3. *National Laboratories supporting DOE's Infrastructure Security and Energy Restoration:*

   INL, Oak Ridge National Laboratory, and Pacific Northwest National Laboratory support DOE's Infrastructure Security and Energy Restoration (ISER) organization, the seat of DOE's Sector Specific Agency authority for the U.S. electric grid. Leveraging the labs' expertise, ISER is standing up a cyber incident response and coordination (IR&C) capability and refreshing its outage notification system. DOE and the national laboratories are partnering in this effort with other sector security stakeholders, including the North American Electric Reliability Corporation's Electricity Information Sharing and Analysis Center (E-ISAC), Edison Electric Institute, the Department of Homeland Security, and others.

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

Question 3: You mention in your testimony that you were in Estonia last week to train individuals in the region on cyber security issues. What level of international cooperation exists when it comes to cybersecurity?

INL observes that international cooperation is increasing, as are the multiple public and private sector opportunities for international cooperation on cybersecurity. INL only participates in international cybersecurity efforts when we are invited and when there is a formal agreement between a U.S. Government organization and an international organization. Cooperative efforts have been endorsed through DOE's Office of Electricity Delivery and Energy Reliability, the DOE Office of Nuclear Energy, the National Nuclear Security Administration (NNSA); Department of Homeland Security, Department of State, or Department of Defense. Many of INL's international interactions are aligned with the security of nuclear energy facilities or the protection of our national defense facilities to assure reliable electricity and communications. Some examples include:

1. *Estonia Training for USAID*

   The training session I participated in was held in Estonia's capital city, Tallinn. It was organized by the National Association of Regulatory Utility Commissioners (NARUC) and was funded by the Unites States Agency for International Development (USAID). Based upon the positive reviews from the attendees, USAID is in the process of scheduling a similar event in Kiev, Ukraine, to teach cyber concepts to Chief Information Officers and Chief Operation Officers from the electrical transmission and distribution utilities in Ukraine, Armenia, Moldova, and Georgia. These sessions will include discussions of DOE-OE's Cybersecurity Capability Maturity Model Program.

2. *DHS Red/Blue Training*

   INL, at the request of the Department of Homeland Security (DHS), hosts international partner participants in Idaho Falls for the ICS-CERT Red/Blue (301) advanced training session. This course provides a unique hands-on approach to understanding control system network environments, identifying potential vulnerabilities, evaluating how these vulnerabilities could be exploited, and applying defensive and mitigation strategies. To date, over 4000 attendees have completed the advanced course, with attendees including DHS-invited international participants from multiple nations. Recently, sessions included participants from Australia, Canada, Chile, Denmark, Germany, Israel, Latvia, Netherlands, Norway, and Spain.

3. *International Nuclear Energy Cybersecurity*

   In support of NNSA's international nuclear security programs, INL nuclear energy cybersecurity experts are routinely invited to consultant on the development of cybersecurity principles and practices for the International Atomic Energy Agency's (IAEA) nuclear security documents (e.g., NST045 "Implementing Guide: Computer Security for Nuclear Security"). Recent cybersecurity training was provided in IAEA member states such as Ghana, Japan, Jordan, Kazakhstan, Mexico, Republic of Korea, Taiwan, and Ukraine. Also, INL provides research papers and demonstrations during IAEA's international cybersecurity conferences.

4. *International Research Conferences*

   In concert with expectations of a DOE national laboratory, INL researchers routinely present research results and provide training and demonstrations during conferences and symposium, many of which are attended by international peers and vendors. In addition to the IAEA conferences mentioned above, INL actively disseminates cybersecurity research results during

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

conferences and symposia sponsored by organizations such as SANS, IEEE, and the American Nuclear Society. Of special note, INL is the originator and primary lead in coordination of Resilience Week, an international symposium dedicated to promising research in resilient systems that will protect cyber-physical infrastructure from unexpected and malicious threats. This international research exchange symposium, now co-sponsored by IEEE, will occur for its tenth consecutive year - this year during September in Wilmington, Delaware.

Question 4: The National Laboratories play an important role in developing cybersecurity solutions for the grid. Can you share more about how the Grid Modernization Laboratory Consortium helps to leverage research dollars and improve cybersecurity?

There are several key areas of grid security and resilience that the Grid Modernization Laboratory Consortium (GMLC) concentrates its efforts:

1. Identify Threats and Hazards
2. Protect Against Threats and Hazards
3. Detect Potential Threats and Hazards
4. Respond to Incidents
5. Recovery Capacity/Time

GMLC R&D supports these five security and resilience efforts while also cross-cutting grid solutions in advanced storage systems, clean energy integration, standards, and test procedures. Individual projects within the R&D plan encourage multi-laboratory and industry collaborations to gain access to the best capabilities and ideas from the various participants. This cooperation assures that research dollars are leveraged to provide stakeholders, who have developmental technologies, with access to the experimentation and testing capabilities within the laboratories; and provides laboratory researchers with access to utilities, which have relevant requirements, operational expertise, and infrastructure.

Question 5: We are hearing more and more about the Internet of Things in the context of the energy sector. You say in your testimony that you are looking at this interconnectedness with a sense of foreboding and that cybersecurity is often pushed to the side for convenience and efficiency.

a. What kinds of internet enabled devices are being attached to the grid?

While the list is getting longer every day, here are a few illustrative examples:

Smart Meters – spurred by the recession-induced American Recovery and Reinvestment Act of 2009, and the Self-Generation Incentive Program – reflect utilities' investments in digital meters to replace often decades old electromechanical devices. Designed as wireless networked devices, smart meters are specialized computing devices, affixed to the side of commercial buildings and private residences. While some of these systems communicate with their utilities via wireless mesh and cellular protocols, others include standard Wi-Fi and Internet Protocol (IP) for standardization, convenience, and customer access.

Electric Vehicles – including the grid-connection systems for direct or wireless charging – present new pathways for connecting personal systems to the electric grid. Vehicles are increasingly more automated, requiring the use of more sensors and communications systems reliant on digital connectivity for safety, efficiency, direction mapping, and maintenance.

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

Industrial Automation Equipment – available from several large manufacturers of electrical equipment for automated industrial processes – are marketed as "cloud-enabled" and "Internet of Things (IoT) ready." Both of these terms convey the ability to connect to and communicate across the internet for efficiency in advanced manufacturing applications, on-demand inventory management, and equipment life-cycle optimization. In much of the associated marketing materials, cybersecurity gets scant mention, if it is mentioned at all.

b. What efforts are the national labs taking to mitigate the threat of cyberattacks through these new internet-enabled devices connected to the grid?

INL is not currently aware of specific DOE programs focused on the cyber research of these new internet-enabled devices connected to the grid. INL, like many other laboratories, utilizes its internal Laboratory Directed Research and Development program to explore early stage concepts on similar devices. INL's internal research is investigating cyber vulnerabilities and mitigations on systems on control systems within electric vehicles and building management systems. These projects are seeing sufficient progress for us to support a renewal of a program such as the multi-lab DOE National SCADA Test Bed (NSTB). The original NSTB program, which began operations in 2003, was fully terminated by DOE in 2014. During the NSTB lifetime, national laboratory cybersecurity subject matter experts performed extremely rigorous security assessments on the hardware, software, and firmware elements of hundreds of grid systems from dozens of global suppliers. Results from these assessments were shared with the manufacturers to assist in designing safer and more secure versions of their products.

A number of electric utilities attended a February 2, 2017 Section 9 meeting with DOE's Infrastructure Security and Energy Restoration (ISER) organization - the seat of DOE's Sector Specific Agency authority. During this meeting, multiple utility representatives requested a revival of the NSTB program to address lingering and now proliferating concerns about the security posture of the operational technology (OT) systems that run the nation's grid infrastructure. This capability, revived for the technologies in 2017 and beyond, would certainly include a focus on IoT and Industrial IoT-connected or enabled systems.

Question from Senator John Barrasso

Question: In the case of a cyber-attack on the grid, can you explain who is responsible? When does the liability fall upon the utility, the technology manufacturer (Smart Grid technology manufacturer), the government, or the consumer?

It may not be clear who is ultimately responsible, but it is clear that each the groups mentioned have something to lose if the system is compromised. While the question is grid and electric sector specific, the topic of liability transcends any one sector. It is our observation that as a nation, we are on a successful pathway to determining liability, not so much for placing blame, but rather, for determining a means of enabling each stakeholder to hold themselves accountable for cyber hygiene and risk management to avoid high consequence events.

INL, as a national laboratory, better serves the nation as an unbiased developer of technologies that enables each of these stakeholders to prevent, detect, mitigate and recover from such an attack. We are extremely proficient, if not the best, at analyzing threat actor capabilities, discovering vulnerabilities, and re-engineering malware with the objective of proactively protecting our grid. Also, in deference to answering a policy question regarding a stakeholder's specific liability, we much prefer to serve as technology leaders in developing and delivering solutions, training and education to better inform cyber-

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

secure designs for grid equipment and systems – with the objective of benefitting any of the stakeholders among government, vendors, utilities, regulators, or users.

Determining liability regarding cyber-related damages is an immature legal and/or insurance claim discipline. Uncertainties can arise in determining whether the consequences result from a defect in hardware or software; from a state-actor attack exploiting a known or zero-day vulnerability; or a teenager's nuisance attack that overruns even well implemented best practice cyber hygiene defenses. In a grid cyber attack scenario, a simple listing of potential litigants and liability may be the source of scores of legal volumes detailing liabilities against stakeholders responsible for product and service claims, compliance with regulatory requirements, and/or inadequate local, state or federal legislation. These stakeholders include, and are not limited to:

- Distribution utility responsible for serving the affected customer(s);
- Suppliers of the equipment and cyber services used by the distribution utility;
- Suppliers of consumer products and services responsible for back-up-power;
- Public utility commission charged with overseeing the prudence of the investor-owned utility;
- Regulatory agencies, or
- Emergency responders.

Questions from Senator Ron Wyden

Question 1: Mr. Bochman, I agree that truly critical infrastructure should be separated, or "enclaved" in technical jargon, from the grid to prevent possible cyberattack. However, the Oregon cybersecurity firm Galois has explained that many physical controls are actually digital behind the control lever. Could you elaborate on your vision for more physical controls on the grid while taking into account this caveat?

Just as we have demonstrated we can find a balance for functionality, safety practices, and physical security, at some point risk management and good business principles will evolve to include routine management of the cyber risk. Reaching this vision will require a corporate culture and regulatory environment that rewards cyber-informed engineering earlier in the digital system planning and design phase.

Innovatively engineering, cradle-to-grave, the right balance of embedded cybersecurity and physical security controls is, and will continue to be, an emerging challenge with the rapid implementation of automation. More and more previously electromechanical protection and safety systems are transitioning to fully digital technology for convenience, efficiency, reliability, and sustainability. Suppliers will continue to be rewarded for developing and marketing increasingly functional, highly-connected, intelligent digital hardware and software that replaces the manual methods we previously used to accomplish certain tasks. Chief executive officers and corporate boards will reward managers and engineers who pursue paths leading towards cost-saving improvements in efficiency and reliability. Similarly, with the availability of innovative cybersecure technologies and methodologies, good cyber-informed engineering will be rewarded.

Question 2: Mr. Bochman, I can appreciate your comment about "bolt-on" security measures in your written testimony. Both Xcel Energy and the Oregon cybersecurity firm Galois have made it clear: the electricity grid needs technology with functioning security measures built in from day one. What do you believe is the federal government's role in the innovation of such secure technology?

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

INL and several other labs, at the request of the Secretary of Energy, are preparing recommendations for the Secretary to support several actions that demonstrably improve grid security in the near-to-mid-term. One of these recommendations focuses on developing financial and other incentives for utilities that deploy increasingly secure equipment. We believe that, so incentivized, utilities would request, if not require, that their systems meet more demanding security standards. Another recommendation will pursue development of secure electric power system design best practices, standards, and certification procedures.

Separately, a number of electric utilities attended a February 2, 2017 Section 9 meeting with DOE's Infrastructure Security and Energy Restoration (ISER) organization - the seat of DOE's Sector Specific Agency authority. During this meeting, multiple utility representatives requested a revival of the National SCADA Test Bed (NSTB) program to address lingering and now proliferating concerns about the security posture of the operational technology (OT) systems that run the nation's grid infrastructure. A capability similar to the NSTB, revived for the technologies in 2017 and beyond, would certainly add a focus on new IoT and Industrial IoT-connected or enabled systems.

Question 3: Mr. Bochman, I am glad to hear about your participation in GridEx. I wonder if you could suggest ways the federal government could incentivize more electric utility and electric co-op participation in activities like GridEx?

Interest and participation among utilities large and small is already high and growing each year. But your point about getting smaller utilities, like co-ops, involved, is appreciated. Federal and state governments may be able to implement a variety of incentive opportunities, including cost-sharing grants for equipment and training. This type of grant may be able to assist smaller, very close to the margin, firms justify the cost, time and effort that is needed to prepare for and participate in GridEx and/or similar local or regional exercises.

As a national laboratory, we generally would defer these type of policy recommendations in preference to other organizations, possibly trade groups for the smaller and medium, non-Investor-owned utilities. These would include the National Rural Electric Cooperatives Association (NRECA) for the coops and the American Public Power Association (APPA) for the municipal utilities.

Question 4: Mr. Bochman, according to President Trump's announced budget plan, it is my understanding that the Office of Electricity is in for a budgetary buzzcut. I also see from your written testimony that Idaho National Lab is receiving a $15 million investment from the DOE-OE to research protective measures from both cyber and physical threats. Do you know if this investment is safe from the DOE program cuts outlined in President Trump's announced budget plan?

The investment already received from DOE's Office of Electricity Delivery and Energy Reliability is considered safe from any future budget adjustments. It is too early to speculate on how the budget request might impact programs.

Question 5: Mr. Bochman, I asked the witness panel to express their views on encryption. It is my belief that weakening encryption used on the electricity grid, and in other aspects of our energy infrastructure, would be outlandishly bad judgement--and I have made it clear that I will fight this every step of the way. Do you believe encryption plays an important role in protecting the electricity grid? Please explain your answer.

U.S. Senate Committee on Energy and Natural Resources
Hearing: April 4, 2017
Examining Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Mr. Andrew A. Bochman

Strong encryption, for data in-transit and at-rest, is one of several main tools in the cyber defenders' arsenal. Suffice it to say, that as technology advances year-on-year, today's hard-to-defeat strong encryption is tomorrow's inadequate encryption. Along with protection with strong encryption, INL recommends strong access control, enforced least privilege authorization policies, appropriate network segmentation, logging and log preservation, secure code development practices, recurring high-quality end user training, and a number of other now widely accepted cybersecurity best practices. These protections and the research to develop and innovate stronger protections are essential today, and will only grow in importance in the years to come.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Colonel Gent Welsh

Questions from Chairman Lisa Murkowski

Question 1: In your testimony, you discuss developing cyber response teams to help industry in the event of an attack. How would these teams differ from what the Industrial Control Systems Cyber Emergency Response Teams (ICS-CERT) already does?

Response:
This, at its basic level, is a capacity issue. DHS ICS CERT is primarily a tool to assist the Critical Infrastructure (CI) sector with day to day issues. ICS CERT does not have the capacity to respond to a large scale significant cyber attack in this country and they will freely admit that to you. There will be far more demand than capacity when (not if) we are hit by a devastating attack on our infrastructure. Also, especially in cyber, response assets need to already have established working relationships through exercises and training with the CI sectors in each state. This is about building trust and relationships BEFORE an attack happens…especially important since the majority (85%) of our critical infrastructure is in private sector hands. The best way to do that is use the model of National Guard Civil Support Teams, but for cyber. I've attached a one page information paper on that idea.

Question 2: Obtaining the appropriate clearance for cyber security professionals seems to be a challenge for the private sector.

a. What do you see as the biggest challenge to the issuance of clearances?

Response:
Biggest challenge…lack of imagination. The Federal Government (DHS and DOE) simply do not broadly think through the issue of "who needs a clearance" enough. The clearance nomination process across the critical infrastructure sectors is random at best and not guided by a deliberate process to understand what people and sectors will need access to US government classified material BEFORE and AFTER a significant attack.

b. What do you recommend to make this process more efficient?

Response:
Get rid of separate clearance processes at DHS, DOE, and DOD and find a way to unify effort. A clearance should be a clearance should be a clearance! There are unnecessary walls between those organizations. I'd put DHS in charge of the clearance process and charge the Homeland Security Advisors (who are appointed by the Governors) in each state and territory with the responsibility of nominating and tracking clearance applications for members of our CI sectors.

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Colonel Gent Welsh

Question 3: The testimony of Mr. McCurdy describes access to clearances as an issue in acquiring necessary intelligence. What about your experience with the National Guard in your National Guard, Title 32 status? That is, when acting in a state status, do you have access to Top Secret and SCI information that you need to do your job on cybersecurity threats? Or does the active military claim that Title 32 status should not have TS/SCI access, at least not until activated into an appropriate federal status?

Response:
Access to clearances is a HUGE issue for both the National Guard and the private/public sector. We are asking the private sector and the Government to form partnerships to deal with the cyber issues we face. But partnerships are built on trust and equal access. If one party (the Government) has all the data and info but is unwilling (or can't) share that data with their partner…there is no partnership. So, equal access to data is very important. We're all in this together…the front lines of the next conflict are at the firewall of every CI provider across this country. So, the information sharing imperative is already here. From a National Guard perspective, we have no issues with accessing classified information that would be of benefit to private and public CI sectors. But, we can't share what we know with the private sector unless they have a clearance and we comply with DOD policy.

When acting in a "State Active Duty" or SAD status, we can only access up to SECRET according to DOD policy. I've attached that policy known as "Coordinate, Train, Advise, and Assist" to this message. Generally, the SECRET level gives us the info we need to do missions in a SAD status. We do have access to TS/SCI in a Federal status, but our authority to respond to cyber events in a Title 32 (Federal status, but state controlled) is still a topic under considerable debate in Washington, DC.

If the National Guard had clear authorities to respond to "State" events using their existing Title 32 status, we would be in a much safer spot as a country. I'm not convinced that the DOD/DHS relationship in terms of who manages the cyber response all the way down to the actual incident level for a significant cyber attack is very clear. DHS has the mission, but they lack the resources and teams. DOD, especially the National Guard, have the teams and resources, but they lack the authorities in a Federal status because of PPD- 41.

Question 4: The Washington National Guard has recognized a tremendous asset in the number of your soldiers and airmen who are cyber professionals in their civilian life. Can you provide more information on how you leverage the expertise of these cyber professionals to have an impact on improving cyber security in your region?

Response:
The Washington National Guard employs many traditional guardsmen who work in cybersecurity in their civilian capacity. We leverage their expertise in a number of ways:

U.S. Senate Committee on Energy and Natural Resources
April 4, 2017 Hearing
Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats
Questions for the Record Submitted to Colonel Gent Welsh

In spite of tremendous progress and emphasis in recent years, DoD cyber-skills training remains in a relatively early developmental stage. The advanced technical expertise many of our guardsmen gain in their civilian career is applied to developing training curriculum and events to share with our cyber operators. This allows all of our guardsmen to be exposed to the latest thinking, techniques, and procedures in the cybersecurity world. This technical edge in many cases results in cyber operators with a significant advantage over their active duty counterparts. Additionally, our guardsmen's advanced knowledge of adversary tactics informs tactics improvement proposals for the DoD cyber enterprise so that the entire nation benefits from their expertise.

Often, our National Guard cyber operators work in extremely specialized information technology fields. For instance, they may work with critical infrastructure or for a company that develops Supervisory Control and Data Acquisition (SCADA) tools. We actively track these various areas of expertise and selectively apply them when and where necessary. We are able to leverage these specific and deep skillsets to tailor our teams to respond to a wide variety of defensive cyber operations.

Finally, our ability to build pre-incident relationships with Critical Infrastructure/Key Resource and other private cyberspace entities is greatly enhanced by employing guardsmen who work in those industries. These individuals can effectively work as a gatekeeper, facilitate relationships, and build trust in unique ways not available to most outside agencies. In many cases, this allows the Washington National Guard more effective outreach than would normally be possible for other DoD entities.

Question from Senator Ron Wyden

Question: Colonel Welsh, I asked the witness panel to express their views on encryption. It is my belief that weakening encryption used on the electricity grid, and in other aspects of our energy infrastructure, would be outlandishly bad judgement--and I have made it clear that I will fight this every step of the way. Do you believe encryption plays an important role in protecting the electricity grid? Please explain your answer.

Response:
While I am not familiar the encryption standards used in the Energy sector, as a general rule, more security provided through encryption is better than less. The Energy sector has a number of built in areas of concern to me, not only in the way their Information Technology and Operational Technology is configured with such things as multiple factor authentication, but also in the security of their data and radio transmission systems. Having encrypted links, data channels, etc is absolutely essential to stopping a determined adversary from penetrating networks outside of the normal way in through IT and OT systems. Once has to only look at the recent attack on the tornado Emergency Warning System in Dallas, TX to see the potential risks

to unencrypted transmission links. Encryption costs money and slows down processes, but there's just too much at stake here to not be as secure as we can be.

The Case for National Guard Cyber Civil Support Teams

For a generation now, leaders in every sector of our society have sounded the alarm about the need for cyber defense, and for more to be done to protect the public/private critical infrastructure sectors and key resources (CIKR) from cyber criminals and state sponsored cyber attacks. Words are easier than deeds, and in 2017 we find ourselves much further behind than we would have intentioned a couple decades ago.

Outside of mammoth organizations that maintain their own cyber warriors and network defense, very little capability or capacity to respond to a significant cyber incident within CIKR exists in the United States today. Most private entities would not know where to begin if they were the victims of a significant cyber-attack. The situation becomes far more dire if a coordinated attack was waged across multiple agencies and critical infrastructure sectors simultaneously.

In the aftermath of the Cold War, with the threat of loose nuclear and biological weapons emerging, National Guard Civil Support Teams were created as a quick response force to the emerging threat of a Chemical Biological Radiological Nuclear and high-yield Explosive (CBRNE) event. The National Guard of each state received at least one Civil Support Team to provide rapid advise and assist CBRNE capabilities to their communities. Creating National Guard Cyber Civil Support Teams now with some of the same looming threats would provide the same service in the cyber realm. There is simply no "cyber fire department" out there now to help fight the fire when it starts.

Current National Guard cyber force structure is simply inadequate to support significant cyber events in each state and territory. Although increasing numbers of states are blessed with talented National Guard cyber units, many states have absolutely no cyber units or capacity to respond to significant cyber events. Moreover, states with National Guard cyber units in them may find those units activated federally to address DOD problems during a significant cyber attack, thus making those capabilities unavailable to Governors. This "have, have not" gap needs to be closed.

We propose Congress authorize and appropriate sufficient funding for each state and territory to have a 10 person National Guard Cyber Civil Support Team comprised of full-time citizen-soldiers and airmen, trained and skilled in the cyber domain. Similar to National Guard CBRNE Civil Support Teams, these cyber teams will be ready to respond to significant cyber incidents when called upon by public and private critical infrastructure entities in our communities. National Guard members have the established relationships and trust necessary for private sector owners and operators of CIKR to feel comfortable asking for help, and letting them into their systems.

Cyber Civil Support Teams would be a fraction of the cost of their CBRNE counterparts because of the minimal equipment and facilities they would require. It is not the intent of these teams to compete with or diminish the FBI's cyber-crime mandate, or the Department of Homeland Security's role in domestic cyber. Instead, it provides each state and territory with a dependable and capable resource, partner, and a rapid response tool for our communities that are often unaware or unprepared for the cyber reality that surrounds them. Gone are the days of the battlefield front lines in some far off location…the front lines of the next conflict are in every state and every community. Will we confront this threat now, or will we realize our cyber response capability gaps when it's too late?

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 2 4 2016

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Policy Memorandum 16-002, Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities

EXPIRATION DATE: March 1, 2018

POINT OF CONTACT: For more information, contact the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security at (571) 256-4425

This policy memorandum provides guidance for the DoD to coordinate, train, advise, and assist (CTAA) cyber support and services provided incidental to military training to organizations and activities outside DoD and for National Guard personnel use of DoD information networks, software, and hardware for State cyberspace activities. The Under Secretary of Defense for Policy, in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff (who will coordinate with other appropriate members of the Joint Chiefs of Staff, including the Chief, National Guard Bureau, and with appropriate Combatant Commanders), the Under Secretary of Defense (Comptroller)/Chief Financial Officer, the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, the DoD General Counsel, the DoD Chief Information Officer, and other appropriate DoD officials, will issue additional guidance on DoD cyber support and services, including support and services provided pursuant to training authorities and under a request-for-technical-assistance process. The Under Secretary of Defense for Policy will seek the views, information, and advice of the Council of Governors, consistent with Executive Order 13528.

DoD CTAA Cyber Support and Services

The following definitions apply to DoD CTAA cyber support and services provided as assistance incidental to military training to mission partners only:

Coordinate: Sharing and synchronizing actions and information with and among mission partners in order to protect DoD information networks, software, and hardware and enhance situational awareness, to improve preparedness for DoD mission requirements, and to improve cybersecurity unity of effort.

Train: Engaging in training activities during which mission partners participate or observe for the purpose of sharing best practices and enhancing DoD cyberspace-related knowledge, skills, and capabilities.

Advise: Providing advice to mission partners that aids in the development of potential strategies, plans, and solutions for preventing, protecting, and defending against, responding to, mitigating the effects of, and recovering from cyber incidents.

Assist: Supporting mission partners in their prevention of, protection against, mitigation against, and recovery from a cyber incident.

Mission partners: Those with which the DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government, State and local governments, non-governmental organizations, and the private sector.

DoD CTAA cyber support and services provided incidental to military training within the United States and its territories will be conducted in accordance with title 10, U.S. Code, section 2012; DoD Directive 1100.20; DoD Instruction 3025.17; and other Under Secretary of Defense for Personnel and Readiness policies and guidance, as applicable.

DoD CTAA cyber support and services provided incidental to military training to mission partners other than Federal, State, local, territorial, and Federally and State-recognized tribal authorities within the United States and its territories may be approved on a case-by-case basis by the Secretary of Defense or the Deputy Secretary of Defense.

Outside the context of CTAA training activities, DoD Components (including National Guard units serving in a title 32, U.S. Code, duty status) may consult with government entities and with public and private utilities, critical infrastructure owners, the Defense Industrial Base, and other non-governmental entities, as needed, in order to protect DoD information networks, software, and hardware, enhance DoD cyber situational awareness, provide for DoD mission assurance requirements, and in order to provide cybersecurity unity of effort. Such consultation for the above purposes is not considered to be CTAA cyber support or services.

DoD CTAA cyber support and services do not include Offensive Cyberspace Operations or Defensive Cyberspace Operations-Response Actions, which may only be conducted pursuant to Presidential Policy Directive 20 and under the procedures set forth in Chairman of the Joint Chiefs of Staff Manual 3139.01. DoD CTAA cyber support and services do not include support for civilian law enforcement purposes, which is provided in accordance with DoD Instruction 3025.21.

National Guard Personnel Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities

Military property issued by the United States to the National Guard remains the property of the United States (title 32, U.S. Code, section 710). DoD information networks, software, and hardware, like non-cyber-related equipment and property issued by the United States to the National Guard, are available for Governors to use for State purposes, subject to the conditions and limitations in law and policy. State use of DoD information networks, software, and hardware issued to the National Guard for State cyberspace activities will comply with applicable Presidential and DoD policies, State and Federal laws, and licenses and contracts

associated with such information networks, software, and hardware. States are also responsible for reimbursement (or replenishment in kind) to the Federal Government for any DoD information networks, software, or hardware lost, damaged, destroyed, or misused while used for State purposes.

State use of DoD information networks, software, and hardware must also conform to laws and DoD policies governing access to and protection of Federal Government classified information and systems, and controlled unclassified information and systems. National Guard personnel in State active-duty status may not access DoD information networks, software, hardware, systems, tools, tactics, techniques, and procedures beyond the classification level of SECRET. A case-by-case exception to this classified information restriction may be granted only by the Secretary of Defense or the Deputy Secretary of Defense.

This Policy Memorandum has been developed consistent with Executive Order 13528, Establishment of the Council of Governors, which was required by section 1822 of Public Law 110-181.

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF, NATIONAL GUARD BUREAU
COMMANDERS OF THE COMBATANT COMMANDS
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
SENIOR INTELLIGENCE OVERSIGHT OFFICER
DOD PRINCIPAL CYBER ADVISOR

POWERPACK GROUP™

1800 Diagonal Road, Suite 600
Alexandria, VA 22314
PH: 703-647-7539

The Power Pack Group, LLC
Testimony Submitted for the Hearing Record
Committee on Energy and Natural Resources
United States Senate

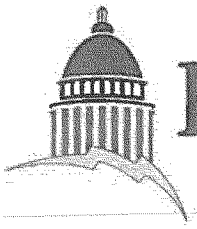
"Efforts to Protect U.S. Energy Delivery Systems from Cyber Threats"

April 4, 2017

Chairman Murkowski and Ranking Minority Member Cantwell, the Power Pack Group appreciates the opportunity to submit the following testimony for the record of this important hearing today. We believe that protecting the integrity of our energy resources from cybersecurity and other external threats is a matter of national security and cannot be ignored under any circumstances.

The Power Pack Group, LLC represents a partnership between Kotuku Energy and Vital Construction & Electric, LLC that manufacturer LED lighting for outdoor and indoor venues. These companies are a Service Disabled Veteran Owned Small Business with master licenses in California, Oregon, Washington State, Virginia, Maryland, Utah, and Alaska. The company also has licenses to operate in 23 other states, including (MT, ID, WY, SD, NE, MN, OH, WV, KY, NC, TX, OK, NM, AZ, and NV. The company also has very extensive expertise in using solar energy technology and solar energy farms to power LED lighting technology.

The value of these resources is that part of a security system to protect our energy resources is in proper and appropriate lighting, whether the energy delivery system is an electric utility substation in the mountains of Montana or the Alaska pipeline. LED lighting technology is particularly suited for protecting energy delivery systems because unlike many other lighting resources, the VCE-Kotuku a high-tech specialty LED lighting technology that is blast resistant and can operate in temperature tolerances from - 40 degrees F to + 160 degrees F. When coupled with security cams reporting real time video feeds, the system could go a long way to preventing terrorist attacks on a pipeline such as the Alyeska pipeline or any electric utility substation anywhere in the United States. An attack upon our energy system is a major National Concern.



POWERPACK GROUP™

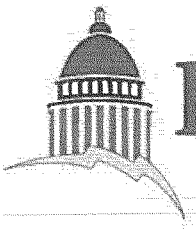
1800 Diagonal Road, Suite 600
Alexandria, VA 22314
PH: 703-647-7539

As early as 2004, Congress has expressed concern about such an attack. According to a 2004 report from the Congressional Research Service entitled, "Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism"

> The U.S. electric power system has historically operated at such a high level of reliability that any major outage, either caused by sabotage, weather, or operational errors, makes news headlines. The transmission system is extensive, consisting mainly of transformers, switches, transmission towers and lines, control centers, and computer controls. A spectrum of threats exists to the electric system ranging from weather-related to terrorist attacks, including physical attacks, as well as attacks on computer systems, or cyber attacks. The main risk from weather-related damage or a terrorist attack against the electric power industry is a widespread power outage that lasts for an extended period of time. Of the transmission system's physical infrastructure, the high-voltage (HV) transformers are arguably the most critical component. Utilities rarely experience loss of an individual HV transformer, but recovery from such a loss takes months if no spare is available. Conversely, utilities regularly experience damage to transmission towers due to both weather and malicious activities, and are able to recover from this damage fairly rapidly. While occasionally causing blackouts, outages resulting from these attacks generally have not been widespread or long lasting.

While there are countless suggestions on how to guard against an attack on our energy systems, keeping these systems properly illuminated is a significant contribution to this solution. A substation or significant pipeline such as the Alyeska pipeline in Alaska is at a significant loss appropriate lighting is not available. LED lighting does not create high temperature like other lighting which in turn will provide extended life of product to minimum of 50,000 hours, eliminating maintenance costs for the duration of the warranty.

Several witnesses at the April 4 hearing suggested the importance of the Cybersecurity Risk Information Sharing Program (CRISP). As the Committee is well aware, The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by the U.S. Department of Energy's (Department) Office of Electricity Delivery and Energy Reliability (DOE-OE) and industry. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and develop situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure and key resources.



POWERPACK GROUP℠

1800 Diagonal Road, Suite 600
Alexandria, VA 22314
PH: 703-647-7539

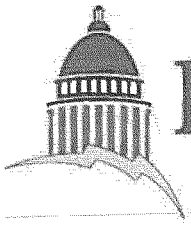
From this perspective, we recommend that the Department of Energy ensure that DOE provide relevant cybersecurity information with industry stakeholders, such as the LED lighting industry if they are involved in providing security lighting for electric utility installations.
The same practical advice should also be applicable to the Alyeska Pipeline.

On July 7, 2015, Alyeska Pipeline president Adm. Tom Barrett spoke at the Greater Fairbanks Chamber of Commerce luncheon Tuesday afternoon, July 7, 2015 at the Carlson Center. He said that aging infrastructure and declining oil flow are well-known challenges facing the trans-Alaska oil pipeline, but that cybersecurity threats present another critical danger. He said that Alyeska Service Co. is bombarded with thousands of attempted online intrusions each month. He said Alyeska devotes considerable resources to warding off such attacks. He was quoted, "You would be astonished at all the people who try to penetrate our systems from all over the world," He said the origin of such attacks is difficult to determine, but he doesn't believe Alyeska is being singled out. In sectors such as energy and banking, cyber attacks are frequently launched by everyone from casual hackers to sophisticated entities.

Barrett said Alyeska has been "highly successful" in repelling the attacks but acknowledged that some efforts aren't detected until they begin to cause problems. He said the attacks range from inconveniencing people ... to serious attacks by people who have malicious intent behind them.

Of the three primary threats that Barrett mentioned to the Chamber crowd, the other two are more familiar: The aging pipeline requires "significant upkeep," and decreasing flow is making it less efficient. He stressed the fact that to combat the decreased flow — the pipeline is carrying about one-third the amount of oil it was designed to transport — Alyeska is doing more research on how to prevent waxy buildup throughout the line. Barrett said that there also have been several recent reminders of potential problems with the aging pipeline, however, including a tiny leak discovered near Pump Station 10 last month. A landslide near the pipeline by the Yukon River also highlighted the dangers of melting permafrost, Barrett said. He continued by stating that Alyeska plans to spend $330 million to renew and repair its infrastructure this year. He said spending varies, but about $300 million is typical for its annual budget in those areas. He pointed to the fact that the pipeline was a brilliantly engineered line, but it is 38 years old.

It is important to realize that the physical integrity and of the pipeline could be enhanced through the use of high tech LED lighting technology.



POWERPACK GROUP™

1800 Diagonal Road, Suite 600
Alexandria, VA 22314
PH: 703-647-7539

According to the Department of Energy LED lighting is a more energy efficient and less costly means of outdoor lighting protection of our energy resources. In a report issued in 2016, the DOE measured the energy and cost efficiency of LED lighting compared with other forms of outdoor lighting in a report issued by the Building Technologies Office in a Fact Sheet entitled "Caliber: Snap shot Outdoor Area Lighting, Lighting Facts (August 29, 2016)":

> Outdoor area lighting is a major contributor to nationwide energy use, and the market segment has been an important player in the transition to solid-state lighting. Lately, the segment has also been making news based on concerns about the difference in spectrum between conventional and LED sources. Although LED Lighting Facts® does not capture data for products' spectral power distributions, which limits examination of these issues in this report, understanding the basic characteristics of available products is more important now than ever before. LED outdoor area luminaires now easily outclass conventional products, such as fixtures using high-pressure sodium (HPS) lamps, in terms of energy efficiency. Some LED products offer the same amount of light for one-third of the power of an HPS-based luminaire, more so for lower-output versions, such as 70 W HPS. At the same time, these LED products can provide superior color rendering, which can improve visibility. As the energy efficiency of LED outdoor area lighting has improved, there has also been a shift toward products with a warmer color temperature, which is perhaps a response to concerns about glare, light pollution, and health effects of nighttime lighting.

We hope that this testimony will be important in building a record of possible solutions to a national security issue that requires solid and practical solutions.

Thank you very much.

An Integrated Fully Autonomous Architecture for Mitigating Cyber Threat in Near Real-time

September 2016

Richard E Malinowski, ISACA CRISC

TABLE OF CONTENTS

EXECUTIVE SUMMARY

General Overview

REM Technology Consulting Services, Inc. ("REMTCS" or the "Company") is a leading management and technology consulting firm specializing in cyber security products for the public and private sectors. The Company has successfully pioneered and developed a proprietary artificial intelligence ("AI") system designed to replicate neural speed computing and human-like cognitive learning with applications primarily focused on managing, defending and countering all types of cyber related attacks on organizations of all sizes. Specifically, the Company specializes in assisting organizations with establishing security and risk management processes including external threat protection, internal threat protection and other risk management functions.

The Company's proprietary core technology, Artificial Neural Network Intelligence ("ANNI"), is radically different from existing forms of artificial intelligence in that computerized processing functions incorporate a fully autonomous behavioral analysis. As such, the Company's proprietary ANNI technology provides users with the ability to program, control and begin learning immediately upon initial setup.

The Company has successfully incorporated its proprietary ANNI technology into a variety of AI driven applications. As a foundation platform for operating the AI applications, REMTCS engineered and developed a biologically inspired custom-built High-Performance Computing ("HPC") system that incorporates hardware designed to replicate neural speed computing and human-like cognitive learning.

The primary component of the Company's HPC system comprises the BELLE or "Bio Electronic Linguistic Layered Equipment", which serves as the foundation for all AI driven applications. The HPC system incorporates a patented contextual processing design that facilitates "task oriented" computing and thus accounts for the cognitive processing capabilities incorporated into the Company's AI applications.

Current applications incorporating the Company's fully autonomous behavioral analysis cyber security lines include the following:

ProActive Security Systems – Fully Autonomous and behavioral analysis based computer network defense products including special-use, high-performance computer (HPC) system designed to perform, in near real-time, all the functions normally executed by an information security team.

ANNI Endpoint – A suite of endpoint solutions for computer networks designed to protect mobile devices and other digital assets.

ANNI Drive – An artificial intelligence-driven security system designed to protect automobiles against digital threats and physical electronic failure.

ANNI Electric – A network security product designed to protect and limit threats to electrical infrastructures and utility grids.

Established, Ground Breaking Advanced Autonomous Intelligence Technology – Company has successfully developed, and deployed in critical national defense and global businesses settings, a comprehensive Autonomous Learning technology comprising its proprietary ANNI technology that has been incorporated into a variety of Behavioral Analysis driven applications. All the computer code associated with the Company's technology is written, active, and in production. As a foundation platform for operating autonomous behavioral analysis applications, REMTCS engineered and developed and deployed a biologically inspired custom-built High-Performance Computing ("HPC") system that incorporates hardware having the capability in design to replicate near real-time computing and human-like cognitive learning. The Company has amassed a portfolio of technological patents, trade secrets, and intellectual assets centered on artificial intelligence, machine learning, software and hardware applications, cyber security in general, and related technology.

Portfolio of Established Products with Large Addressable Markets – The Company's portfolio of products address the critical digital security needs in several primary industries including computer network security, smart utility grids, smart vehicles and other applications representing markets with combined gross revenue in the hundreds of millions/billions. All products have an existing installed based or are soon to be deployed, and are being actively marketed on a global basis. The Company is beginning discussions with a top-tier global automotive manufacturer to package the Company's technology in its upmarket and luxury vehicles. In addition, the Company is about to secure several large contracts for its core PASS computer network security and ANNI EndPoint products.

Advanced High Powered Computer Systems and Special-Use Appliances – REMTCS' product portfolio includes a few special use IT hardware products. These products include super-computer class central processing units, custom designed chipsets embedded with the Company's AI software, and custom designed network interface cards. These components are tailored to enhance the speed and capabilities of REMTCS' technology. In addition, REMTCS has designed and tested several other special-use devices. The company has designed, manufactured, and tested a special-use device for automotive security. This device, which is small enough to hold in your hand, is embedded with the Company's signature PASS technology and is easily integrated with today's "smart" automobiles.

Experienced Developer – Experienced senior management team with in-depth engineering expertise in supercomputing, specifically it's Fully Autonomous Behavioral Analysis and information security. The Company has creative research and development capabilities in infrastructure design, and IT computing, with a focus in IT strategy and operations. Founder has C-Level IT executive experience and over thirty years of experience developing infrastructure technology, security systems, and software development. Founder has extensive experience designing and managing systems at tier-one global banking and brokerage, hedge fund, health/biotechnology, and companies in many other industries. Experience includes quantitative analytics, commodities and equities modeling, systems architecture design and implementation, operational risk mitigation, operational risk assessment, enterprise security, and other capabilities.

Additional Growth Opportunities – In addition to the significant growth from its existing portfolio of products, REMTCS' core technology is capable of being adapted to numerous, as yet undeveloped, applications. Key potential in which REMTCS' technology would be suitable include; facial recognition and other imagery, medical and life-sciences, HIPPA and other insurance management, financial market analysis and trading, transportation management, and many other potential applications.

Notable Milestones and Recognition

- The competitive marketplace has begun to embrace REMTCS' groundbreaking technology as it has recognized the cutting edge benefits they provide simply cannot be delivered by the mainstream security marketing machine. Interest for the products have been consistently increasing in proportion to the rising frequency of cyber-attacks and the decreasing viability of competitors' offerings.

- Existing installations of REMTCS products include ANNI Endpoint at a U.S. Defense contractor, and PASS installations at a U.S. Defense contractor, and three Hedge Funds. These installations have functioned as designed and have displayed outstanding reliability.

- Imminent installations include a $2.5 million Phase 1 contract with an international customer which will result in additional gross revenue of $1.2-$1.3 million in Phase 2. This project is a progressive step towards a reselling relationship with the customer. Their client base includes 8,000 plus customers which could easily yield an additional stream of $20 to $50 million per year minimum in gross revenue.

- Related to, but separate from, the aforementioned imminent installation are discussions with a single international vehicle manufacturer for installation of ANNI Drive into their product line which would minimally result in $250-450 million revenue per year, not including subscription fees.

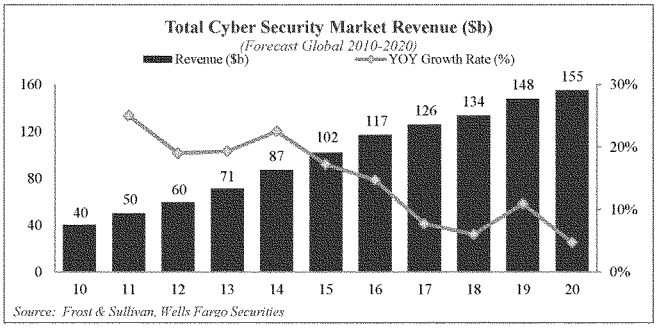
- Serious discussions that are expected to close within 90-120 days include contract negotiations with a medium sized U.S. Defense contractor resulting in sales of PASS, ANNI Endpoint, HPCs etc. as well as a product listing on the US Government GSA Schedule. Resulting sales could exceed $20-80 million in annual revenue, as well as additional product exposure to key government market sectors is anticipated

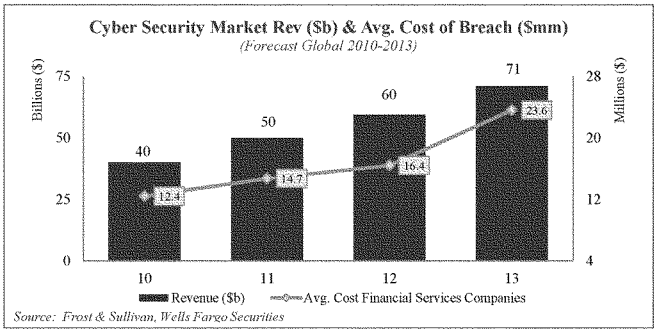
- As confirmation of REM Technology's competitive posture and leading edge technologies, REMTCS was named to the "20 Most Promising Technology Solution Providers for The Defense Industry" list by CIO Review magazine.

INDUSTRY OVERVIEW

The Cyber Security Industry

Broadly speaking, cyber security refers to the tools, policies, and practices employed to prevent the theft, damage, or misuse of information or data within the digital infrastructure. The cyber security industry includes manufacturers, software designers, and service providers offering products and services for a wide array of security threats. Frost & Sullivan estimates that expenditures on cyber security will reach $155 billion by 2020 and grow at a compound annual rate of 13.4% between 2010 and 2020. Though spending on cyber security (broadly defined) increased by approximately 18% from 2012 to 2013, the average cost of a cyber-breach increased 44% over the same period. What is more, the potential cost of a breach can be many times greater than the average. For example, it is estimated that Target's out of pocket costs, net of insurance, came to $173 million, and lost sales estimates range as high as $750 million[1].





[1] Wells Fargo Securities

The Economic Cost of Cybercrime

Per McAfee the cost of cyber crime is estimated to be four times the amount spent on security solutions[2]. The high-profile Target Corporation breach in 2013 provides insight on the true cost of a large-scale breach. One report estimates Target lost $400 to $600 million because of the breach. Target reported estimated direct breach costs of $173 million, net of insurance payments. Target's security spending prior to the breach is estimated to be $70 million.

Key Developments in Cyber Security[3]

Technology Demographics – As society has become more distributed, global, and interconnected through social media, businesses and other organizations have followed this trend. Many employees now work remotely, access corporate data using a variety of personal devices, and increasingly use cloud computing.

Rise of the Advanced Persistent Threat – In recent years, malicious software (malware), formally a one-time event, has increased significantly as it has evolved into the Advanced Persist Threat (APT). APTs are continuous, stealth based attacks that can cripple a network. Legacy technologies are no longer effective at detecting APT attacks.

Rise of the Cloud – As "public" cloud-based computing platforms become more popular, businesses that currently rely on internally owned and operated computing platforms will be under pressure to adopt a cloud-based IT model.

"Underinvestment" in IT Security – Several factors suggest that there is significant room for increased spending on IT security. IT security spending as a percent of total revenue is estimated to be approximately 0.25% of total revenue. In a recent Wells Forgo Securities survey[2], 21% of respondents indicated that IT security spending is a top priority versus 15% in 2013.

The Old Stuff Doesn't Work – Signature-based protection has not been able to thwart evolving threats. In addition, the advent of the cloud, social, software as a service, mobile connectivity, and bid data have surpassed the capabilities of today's IT security solutions.

Cyber Security Becomes a Board Level Priority - Target's CEO and CISO lost their jobs due to the 2013 breach. As the number of similar high-profile cyber breaches has escalated, corporate boards have made cyber security a board-level priority.

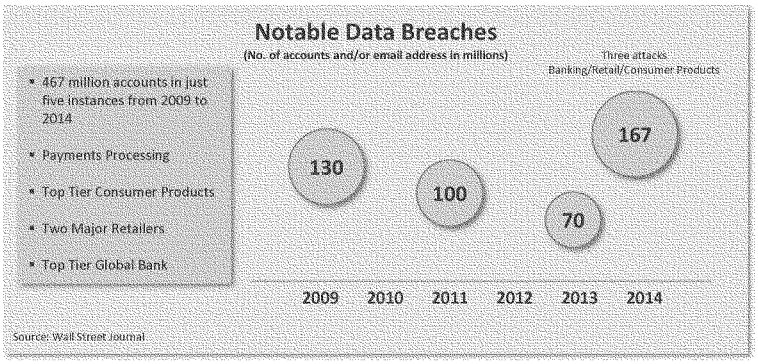
---

[2] *The Economic Impact of Cybercrime and Cyber Espionage*, McAfee. July 2013
[3] Much of this section is taken from *Cybersecurity: Security Empowers People,* Wells Fargo Securities. October 30, 2014

THE CYBER SECURITY CHALLENGE

The Cyber Security Imperative

Recent highly publicized security breaches at major banks and retailers have shown that despite having what is deemed to be the latest intrusion detection and prevention systems (IDS/IPS), and a highly trained security staff, these measures do not always translate into action to stop a security breach before damage could occur.



National Security - Outnumbered and Outgunned

REMTCS management believes that, the U.S. is outnumbered and outgunned in the national defense cyber domain. Some of the U.S.'s adversaries utilize an extremely efficient multi-level, business model-like approach similar to crime syndicates to develop exploitation methods and to infiltrate critical infrastructure, commercial and consumer interests in the U.S. Other adversaries throw hordes of humans at the goal of compromising US government and commercial entities for the purposes of intellectual property theft, and gaining political advantage and economic leverage. Public and private sector organizations alike will likely never be able to protect their interests while they insist on playing "catch-up" with the enemies of varying operating models. Then, there are insider threats, unintentional and otherwise. The common denominator is the human being. REMTCS believes that, through the effective use of its proprietary products, the human factor can be removed from virtually all the vulnerable management life-cycle for the purpose of defending faster than the threats can manifest.

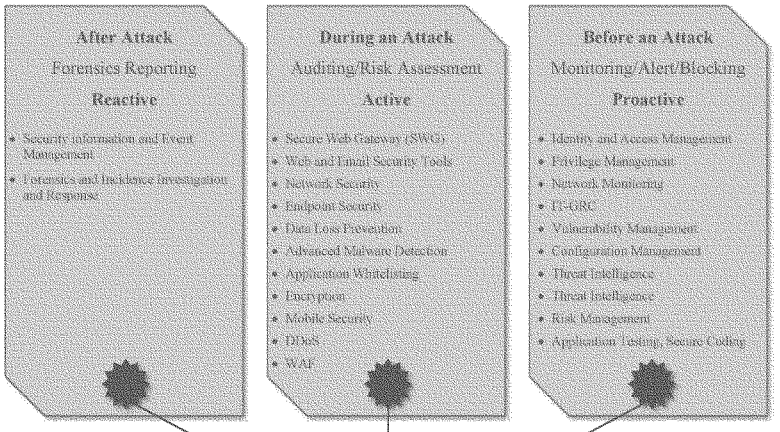
REMTCS estimates that current security best practices and digital strategies have the shelf-life of a little over two weeks. Security professionals cannot detect or produce antidotes fast enough to keep up with the rate at which threats from cyber criminals can evolve. REMTCS poses the question, how do organizations and security professionals combat against an enemy that innovates continually? REMTCS's solution to these challenges is to urge organizations to proactively address this security challenge by adopting and practicing an offensively focused digital security policy. As noted above, REMTCS' products are designed to address the challenges of this cyber security environment.

Fault Lines in Cyber Defense

Cyber-attacks can exploit weaknesses unique to a particular system. However, REMTCS has identified five key general flaws in the current overall approach to cyber security, and has designed its products to mitigate these flaws:

Human Error – Humans in the loop reduce response effectiveness and lower response speed.
Attacks Evolve – The sophistication of attacks evolves while security systems remain static.
Lack of Integrated Approach – The current patchwork of a many systems approach presents cyber criminals with many avenues through which they can gain access to a system, and increases the complexity of managing system security.
Slow Response Times – The standard information security infrastructure, including personnel, is slow compared to the rapid evolution of cyber threats.
Institutional Apathy – The status quo of "maintaining compliance" may mean protection from regulators, but not from cyber threats.

Types of Cyber Attack Prevention

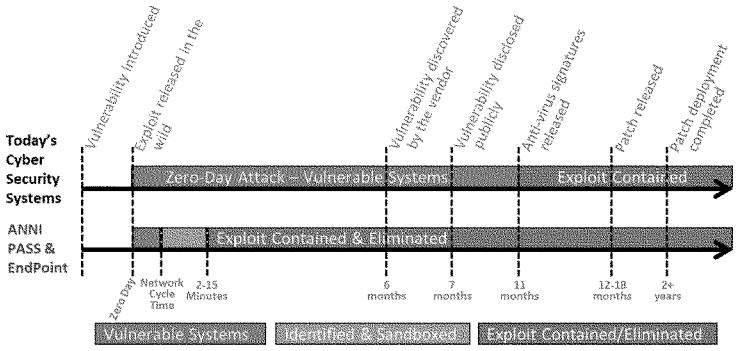


- **REMTCS Provides Advanced Solutions in All Three Categories and for All Applications.**
- **By Design, REMTCS Fully Autonomous Behavioral Analysis Technology Accomplishes These Tasks in Real-Time.**
- **REMTCS Machine Learning Integrates Active, Reactive, and Proactive defense into one continuous, near real-time process.**

The Zero-Day Attack: A Case Study in Latent Threat

"Zero-day attacks" are cyber-attacks using previously unknown vulnerabilities in information systems. Much of today's software consists of many layers of prior computer code. Some layers can be decades old. This old code can contain vulnerabilities that have been long forgotten. As cyber attackers become more sophisticated, zero-day attacks is an ever-growing threat.

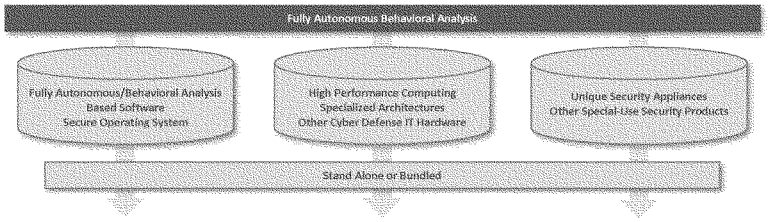
- These types of attacks can take six months or longer [on average] for a vendor's forensics team to discover, reverse engineer and mitigate. One recent attack proliferated on the internet ("in the wild") for six years before being discovered.
- They often lead to unwanted media attention that can pose a negative reputation risk to the company and leave customers and potential investors leery.



THE REMTCS SOLUTION

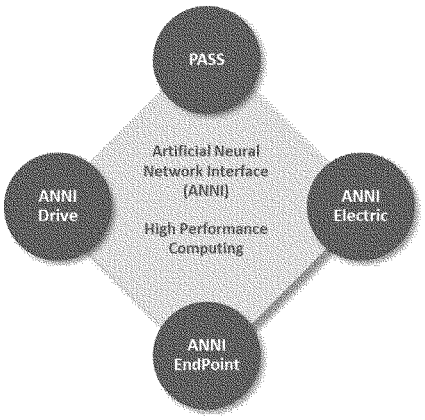
REMTCS's Product Overview

REMTCS provides a suite of enterprise-level cyber security products for the digitally connected economy. The Company's cyber security solutions are founded on the Company's patented Artificial Neural Network Intelligence (ANNI) a fully autonomous behavioral analysis architecture, and its unique, patented, special-purpose digital appliances (hardware).



Product Suite

The Company's products provide cyber defense for computer networks, electrical grids, digitally controlled vehicles, and several other digital environments. REMTCS is not just another network security product provider, rather, the Company provides enterprise level, special-use cyber defense products designed to protect critical components of the infrastructure assets for the digitally connected economy.



ProActive Security System (PASS) – Computer network defense products

ANNI Endpoint – Anti-virus software enhanced with artificial intelligence

ANNI Drive – Digital defense product for the automotive industry

ANNI Electric – Digital defense for electric and other utility grids

Core Technology – Fully Autonomous Behavioral Analysis

The Company's cyber security solutions are founded on the Company's innovative and patented Fully Autonomous Behavioral Analysis intelligence technology. This unique, innovative software technology is designed not only to detect new forms of malware and proactively identify and defend against them before networks are compromised, but also to predict potential threats and evolving threats. When PASS detects a threat, all packets are deep inspected, the malware is decompiled, scrubbed, inoculated, and identified/destroyed – in near real time – across network elements including PCs, servers and other remote laptop devices. This framework represents the cyber security industry's first comprehensive end-to-end, automated enterprise security solution.

PASS operates through a series of proprietary algorithms derived from the search-and-destroy behavior of human antibodies. The algorithms are stacked and sequenced in a manner that gives PASS the power to learn and detect variations of known threats, as well as, to identify new or unknown threats. PASS performs a machine learning process based on a variety of techniques and languages. The PASS software system utilizes machine learning technologies in combination with REMTCS' proprietary cluster, or combinatoric sets, of algorithms to achieve optimal learning of patterns. (Combinatorics is a branch of mathematics concerning the study of finite or countable discrete structures.)

PASS's Learning Process

PASS's "machine learning" capability is a vital aspect of the technology, and its automated, continuous learning is the primary factor that distinguishes REMTCS products from other cyber security products. The four key components in PASS's learning process include: detection, learning, intelligence, and data set creation.

Detection (Reading) – At the moment of data ingestion, PASS reads all incoming network packets; any form of data at up to 56G line speeds.

Learning – Learning and filtering of data-sorts through the data structures using data sets, heuristics and 195 algorithms including the ability to utilize advanced combinatorics for faster determination.

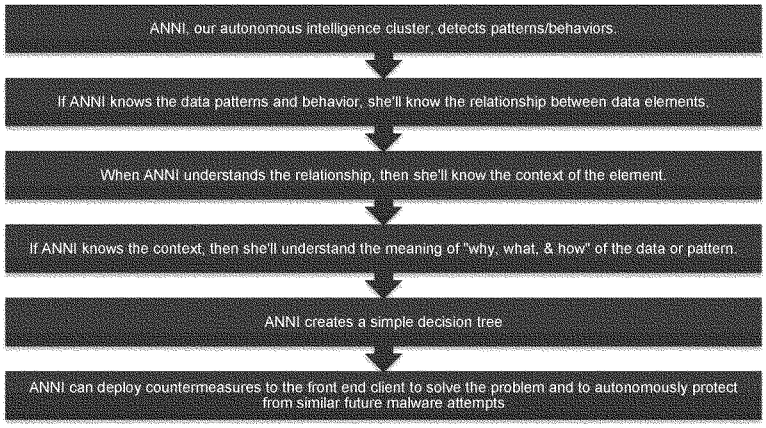
Intelligence – Indemnifies associations, relevancies, and patterns. PASS detects every byte without any human intervention autonomically by spawning computational and data cells as it responds to external sensors and APIs throughout the protected network.

Data Set Creation Engine – PASS's data set creation engine, developed using industry standard data mining technology to absorb and read data from various network sensors (sensor fusion), virtual sandbox and code analysis results, as well as other network detection technologies into a "data study" that ultimately becomes / updates the systems dynamic Centralized Threat Information Database (CTID) of malware detection. The CTID is dynamic in the sense that it feeds threat information directly to the EndPoint protected clients as they are discovered by PASS.

PASS grows and gains strength in two ways. The first is by continuously learning and characterizing activity in the network that establishes and refines baseline behaviors through the discovery of malware. The second is through interactions with the external environment and other PASS systems to learn from each other's decomposition of threat activity and intent. PASS "learns" from past examples enabling it to detect hard-to-discern patterns from large, noisy or complex data sets. In this way, PASS can predict and defend against not only known threats but also unknown threats that carry the same, similar, or partial structure (variant identification) as well as through behavioral analysis. This machine learning approach can substantially improve the accuracy of predicting cyber threat development, progression, and expected network deployment. Thus, specific PASS modules can be built to support life cycle health of the network.

How REMTCS Fully Autonomous Behavioral Analysis Process Works

REMTCS ANNI works through a sequence of clustered algorithms, and is designed to learn and respond in milliseconds.



Key Aspects of REMTCS' Fully Autonomous Behavioral Analysis Intelligence

- Behavioral Analysis based on the latest technology that studies behavioral analysis of the data and its interactions with the infrastructure
- Machine learning Network Response System
- VM Safe Boot Zone
- Virtual sandbox reverse engineers malware in near real time
- Multiple sequenced clusters of learning algorithms/frameworks
- Machine to Machine learning using our distributed Centralized Threat Information Database
- Real-time continuous monitoring for malware identification at the transport level
- Pattern matching engine combined with countermeasures within the domain
- Variant Analysis
- Immune System / Near Real Time Defense Correlation Engine
- Endpoint Detection / Reverse NAC System
- Cloud Behavioral Data mining Servers
- Digital Signatures act as a DNA Database

ANNI– Algorithm Data

- Using content analytics and data mining association rules via network sensors and global trending engines, the system feeds data of behavioral and malicious patterns into PASS's CTID engine which computes the data by following a cluster of formulas/and learning algorithms.

Other Features of the PASS Technology

- Proactive anti-malware de-engineering
- Comprehensive near real-time forensic data, incorporating complete reporting, diagnostic and audit trails, malware
- ANNI is a correlation/compliance and interpretive sensor fusion engine; she learns meaning by detecting patterns and associations (Behavioral Analysis).
- Event re-play
- Once malware is discovered ANNI automatically spawns a countermeasure that is deployed to the specific malware on a specific device to inoculate / destroy the malware.

PROACTIVE SECURITY SYSTEM

REMTCS' ProActive Security System (PASS), is a code embedded appliance, special-use, high-performance computer (HPC) system designed to perform, in near real-time, all the functions normally executed by an information security team. PASS has three primary components: PASS coupled with ANNI EndPoint based software, REMTCS special purpose HPC, and the Sentinel countermeasures.

Key System Components

Autonomous Intelligence Driven Software – Each PASS system bundled with ANNI powered cyber-security software. As discussed above, ANNI's key innovation is that it can, through behavioral analysis, identify new forms of malware, in near real time, and identify and defeat them. ANNI operates through a series of proprietary algorithms derived from the inherent search-and-destroy behavior of human antibodies. Network malware is identified, decompiled, scrubbed, inoculated, and destroyed -- all in seconds-minutes. PASS learns in near real time through behavioral analysis, derives context from the data it assimilates and continuously monitors the network to discern malicious intent.

Sentinel Special-Use Hardware – The Sentinel special-use hardware package includes an ultra-high speed network interface card (NIC) array embedded with REMTCS' ANNI technology, and a Centralized Threat Information Database that employs technology similar to that used in DNA metagenomics sequencing applications.

REMTCS High-Performance Computer (HPC) System – The REMTCS high-performance computer (HPC) appliance provides the architecture for the PASS fully autonomous code to perform at ultra-high speeds. The REMTCS HPC platform comes equipped with a proprietary, "low overhead", and special-use operating system. The combined effect is threat protection that functions in near real-time.

In addition to near real-time threat detection, the ANNI/PASS system performs other critical cyber security functions, including:

Captures Attacking Malware packets at the gateways or in transit in network – Captures new forms of malware and places it in a "safe container" for analysis.

Reverse-Engineering Malware – The Sentinel system delivers the malware to the ANNI enabled HPC where the malware is de-engineered and a digital signature is identified.

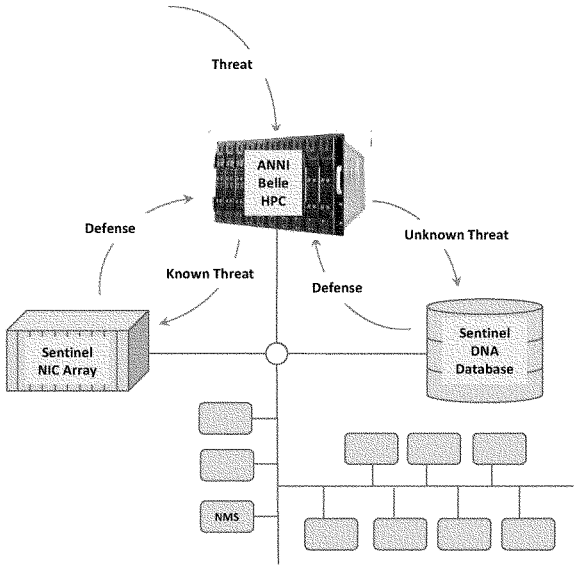
Devises Counter Measure – PASS independently develops a vaccine or inoculation to keep your enterprise safe from the attacking malware and deploys the appropriate response. This is accomplished in near real-time.

Stores Digital Signature – PASS provides a User Interface report to the system operators, and stores the signature in the Centralized Threat Intelligence Database.

Roamer – This feature is another truly unique weapon within the PASS arsenal. It 'lives' behind your firewall and is deployed by ANNI after an attacking malware has been foiled and the "digital signature" has been captured. Armed with this "digital signature", the Roamer works in conjunction with ANNI EndPoint to search for a single identified malware file within your domain devices (as identified by its associated IP) and in addition to software lying dormant in your network. PASS has been taught to never be complacent in regards to your enterprise security and many malware types are designed to be delivered in small undetectable units, to be reassembled when all the components have penetrated your defenses.

ANNI EndPoint (Predator) – This feature is deployed by PASS once an attacking agent is to be destroyed. PASS bi-directionally communicates with ANNI EndPoint to releases the Predator (a single/multiple search and destroy to neutralize malware on any client device. It is the ultimate offensive countermeasure within PASS.

Figure: ProActive Security Systems (PASS) system schematic.



Additional Features and Benefits of PASS

In addition to the key elements noted above, REMTCS' PASS systems provide many other features and benefits

Integrates with Existing Systems – PASS integrates with all existing security platforms and vendor equipment, monitors network activity through behavioral analysis, reverse engineers suspected malware on the fly to determine intent and behavior, automatically deploys countermeasures to stop any found threat from continuing in a manner that could harm the organization, and then notifies the appropriate personnel of the actions taken. PASS also provides a patented, corrective action web interface to add or change active rules/false positives.

Internal Threat Protection and Data Loss Prevention (Future feature) – PASS doesn't stop at external threat protection, it will also protects firms from insider data theft and corporate espionage by building a "profile" on every user of a piece of technology in that firm (PASS can be integrated within the client's compliance engine) .

By identifying and profiling user behavior on the network, boundary conditions can be established that trigger insider threat thresholds. Combined with data loss prevention, the REMTCS solution will provide comprehensive security for complex network environments in a speed and thoroughness that current processes and methods are unable to duplicate. Note: (Confidential data must be tagged)

Acquisition Development Cost Reduction – The PASS solution provides the opportunity to significantly reduce network life cycle costs by augmenting administrative teams with a decision speed unachievable regardless of human effort. By identifying and disrupting intentional and/or unintentional data breaches in near real time, organizations mitigate the cost of breach forensics and damage assessments/security investigations. At the same time, the PASS system will identify vulnerabilities in REMTCS software system, leading to faster, more robust software development, reliability, resilience and system security.

Automated Accelerated Implementation & Configuration – Typical "next-gen" systems require upwards of a year to fully implement and remove false-positives from the system. PASS, with its uniquely designed fully autonomous engine coupled with its Centralized Threat Information Database, can be implemented and be totally responsive in a fraction of the time (even in larger networks), bringing the benefits of the investment to realization much faster.

Risk Reduction – Reducing the risk from the automation of tactical security decisions typically made by humans, and by detecting and stopping malware in near real time.

Workforce Optimization – The automation of security functions such as network monitoring, response, and forensics, augments your security team and acts as a force multiplier. PASS is equivalent to 8-16 highly trained security analysts working 24/7/365.

Cost Efficiency – Efficiency from PASS' ability to leverage your existing security investments, rather than replacing them. PASS grows stronger and more effective over time, instead of the current "next-gen" products which require humans to keep up with the evolving threat landscape.

Gold Disk – REMTCS has developed a PASS "Gold Disk" in support of all PASS technology installations

Secure Operating System (OS) – REMTCS' patented, secure, low-overhead operating system software is packaged with each PASS system.

ANNI ENDPOINT

ANNI Endpoint is a suite of products, including software and special-use high-performance computing devices, designed to provide endpoint security solutions for enterprise computer networks. ANNI EndPoint was designed to protect enterprise computer hardware (personal computers, servers, laptops). The endpoint suite includes a malware & anti-virus product (ANNI Scan); a USB key scan that can detect and repair a disk or devices infected with malware (ANNI Rescue; a future service- an online pay-as-you-use service, where a person or company logs into the REMTCS' website and pays the fee to scan remotely (ANNI Inspection). The suite components can be purchased separately or as a complete ANNI Endpoint package. ANNI EndPoint is included with the purchase of a PASS system. In addition, REMTCS has developed a "Gold Disk" in support of ANNI Endpoint technology, and packages REMTCS' proprietary, secure, low-overhead operating system software is packaged with each ANNI Endpoint system.

Key Differentiator: Optimal Endpoint Efficiency – Endpoint protection software is typically a resource-draining product designed in a "cookie cutter" approach, in which client endpoint software is loaded down with all necessary data, services, and features to protect many differing platforms across large networks. As a result, processing speeds and user functionality can decrease as much as 50% to 60%. Moreover, with this approach the device vulnerability increases due to standard, or generic, installation code and methods might not be suitable for all threats. Another significant shortcoming of the cookie cutter approach is that the decreased processing speed can induce users to bypass or disable certain security features as they seek to reclaim their processing speed.

To counteract these shortfalls, ANNI EndPoint's driven software scans a device (desktop, laptop, server, etc.) and creates an optimal endpoint package specifically for that device. This approach significantly decreases CPU utilized by the endpoint software compared to other similar competitor products. ANNI EndPoint's Predator is able to scan for the file and destroys it typically within ½ second.

Key Differentiator: Threat Response – Conventional endpoint security products have another critical flaw that renders their products unable to keep up with the reality of today's ever-changing threat landscape. Specifically, they use people to discover, reverse engineer, and manually create signatures for malware. This process is slow and inherently reactive, and can never get ahead of new and evolving threats. Additionally, traditional anti-virus products are completely unable to deal with zero-day attacks. It takes, on average, from 6 to 12 months for a traditional security vendor to discover, reverse engineer, test and release signatures on a new threat. Moreover, once the signatures are in place, they can easily be defeated by simply creating a slightly different variant of the malware, which restarts the threat response cycle. In this environment, conventional endpoint products leave systems continually vulnerable to infection or breach. The Company's ANNI EndPoint coupled with PASS' Centralized Threat Information Database driven product eliminates these vulnerabilities by automatically detecting malware variants.

Internal Threat Protection –In addition to protecting against external threats, the REMTCS endpoint package protects against internal threats using the Company's advanced PASS technology to "learn" behavioral patterns of malware, takes defensive action and compiles forensic information when it detects improper use of company assets and data.

ANNI DRIVE (Due out in 1st quarter 2018)

As electronic control sophistication increases, the potential opportunity for malicious activity is increased without sophisticated protection in today's market. The rapid adoption by auto manufacturers as well as the latest global market trends of integrating "next-generation", "smart" communications and digital technologies within mobile vehicles is changing how we use and drive our vehicles. However, digital criminals are adapting to the new technology. Criminals can take command of a digitally controlled vehicle and obtain personal information, steal the vehicle, or conduct digital terrorism. Vehicle systems are like most advanced communications systems and digital technologies that have global web access or networking capabilities. For this reason, the vehicle becomes a leading target of cyber criminals.

http://www.cbs.com/shows/60_minutes/video/1D1j5fa5mCssVRFw2PkluiW94Fzbjo8Z/darpa-dan-the-swiss-leaks-selma/

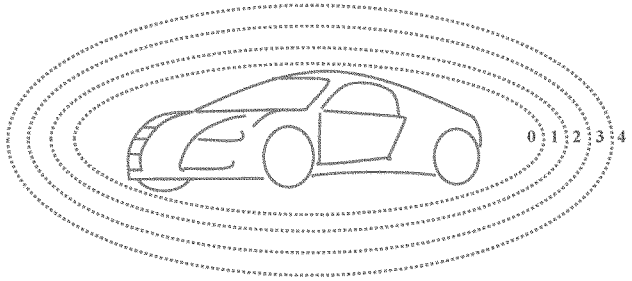
Electronic devices control a range of key vehicle operating functions, including the engine, brakes, tire inflation, and other functions. Control of a vehicle can be either hijacked or disabled without physical intervention. Mobile or vehicle-related malware or viruses are becoming more prominent. Cyber criminals can obtain route information on commercial vehicles, disable them, steal the vehicle or its cargo, employ it for terroristic purposes, and other malicious activities.

ANNI Drive is an application of the PASS technology specially designed for today's electronically control vehicles. The product is embedded in the manufacturers electronic control system/microprocessor. After an initial 300-mile self-configuration in which ANNI Drive "learns" an individual's normal operating and electronic communication pattern within, and between, the vehicle ANNI Drive will detect and protect the vehicle from abnormal activity. In addition, ANNI Drive has the capability to detect intrusions that didn't exist at the time of installation due to its unique machine learning capability.

Figure: ANNI Drive special use appliance.

Five Layers of Protection

Zero Layer –	REMTCS' proprietary secure operating system	Third Layer –	Communications integrity, intrusion detection
First Layer –	Anti-injection/malware defense	Fourth Layer –	Network access control via a white list of authorized users.
Second Layer –	Communications integrity, intrusion detection		



ANNI Drive Benefits

Theft Prevention and Misuse – In addition to the 'white-list" access control, ANNI Drive will learn the owner's driving behavior, and will know if someone other than the owner is driving the care. Moreover, ANNI Drive can detect unsafe, erratic driving such as speeding, driving under the influence of alcohol or drugs, driving affected by sleep deprivation, and other unsafe driving circumstances.
Extends the Life of the Vehicle – Protects both consumers and manufacturers by optimizing vehicle performance and reducing nuisance warranty claims.

Reduces Unanticipated Repairs – By optimizing a vehicle's performance and protecting against malware intrusion, ANNI Drive limits emergency expenses, and unplanned repairs.

Reduces Harm to Vehicle Passengers – ANNI Drive detects unusual driver behavior patterns such as those caused by medical conditions. Examples include erratic driving behavior caused by diabetes, reaction to medications, alcohol consumption, etc.

Can Improve Driving Skills – ANNI Drive can improve driving skills by detecting changes in driving behavior or detecting certain preset parameters such as driving speed.

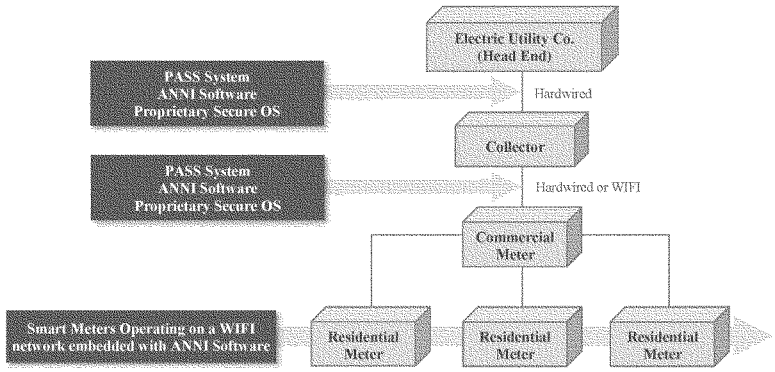
Additional Safety Options Available – ANNI Drive can be synced to a health monitoring device worn by the driver, and customized to monitor many health conditions such as diabetes. ANNI Drive will notify the driver before their driving can be affected by their condition.

ANNI ELECTRIC (Project Based)

ANNI Electric is a network security product designed to tackle commonly discussed, yet frequently unaddressed, critical threats to electrical, gas, and water infrastructure. With the proliferation of "smart meters" throughout the grid, the entire end-user segment of the power grid is being converted to a large, wireless computer network. Thus, a more vulnerable, attack-friendly vector has been introduced into the electric, and other utility grids. This poses significant public safety and national security implications - it is only a matter of time. Recognizing this threat, REMTCS has developed a special-use, ANNI based technology to protect against it. This product consists of software that is loaded into the smart meter, and systems at the headquarters and regional levels to manage threat protection for the whole grid.

The Electrical Grid Demystified

The electric utility industry is organized in a unique fashion. For every so many meters there is a hub, called a collector. This hub aggregates usage and other metrics for a particular region of the grid. Above the collector level is the so-called "head-end" or headquarters for the electricity provider utilizing a C12.22 protocol. This structure requires cyber threat protection at all three levels; meter, collector, and head-end. REMTCS has designed an ANNI based system specifically for this structure.



Utility Grids – The Big Picture

Other utilities use a similar structure. REMTCS can supply the threat protection solution to match the grid structure. The following highlights provide an overview of the U.S. market for this product offering.

(millions)

Type	Electric	Gas	Water	Total
Households	130	60	60	250
Businesses	30	30	30	90
Total	160	90	90	340

Source: Management

Case Study – Hacking the Grid

A meter interruption occurs by a hacker whose intent is to cause simple chaos. An attack on the wireless connection between the meter and the utility is created and the credentials needed to perform a massive distributed denial of service (DDoS) attack are intercepted. Once the meter controller goes offline, the meters in the field are delivering commodity without the able to collect data or bill the customer correctly. ANNI Electric works by first integrating with the current Advance Metering Infrastructure (AMI) network's security layers, coupled with triggering sensors, to detect the attack. Once known, ANNI performs immediate countermeasure steps to absorb the attack while performing forensics. Once the attack is absorbed ANNI begins the legal identification process. The Stem-Cell component virtualizes a backup network environment to restore services while making it appear to the hacker that the attack has been successful. Once ANNI completes the forensics process, she automates countermeasure actions to disconnect the attack and prevent the hacker from re-entering the network. At this point, ANNI Electric will begin the network healing process by disinfecting, generating post-attack reports and sending them to the relevant security teams.

ADDITIONAL COMPANY INFORMATION

Biography of Richard Malinowski, Founder

Richard has a 25-year background in managing IT and operations for Fortune 500 Financial Services, Biotech and Software Development industry companies. Richard is the former head of IT for Citibank's Money Market and Treasury divisions where he managed both divisions for IT and logistics and built two of the world's largest trading floors at that time.

Richard went on to become the Head of IT the Western Hemisphere (including parts of the UK and Asia) and Project Management for Union Bank of Switzerland/UBS Securities as well as 7 subsidiaries where he managed 27 divisions for IT, Project Management, Quantitative Analytics and Operations. Richard ran the Crisis Management Team for over 8 years.

Richard founded REMTCS Consulting Services where he successfully completed over 150 projects in Capital Markets, Banking and Trust, Brokerage, Insurance, Biotechnology and E-Commerce designing and building over 54 of the largest trading floors in the US and Europe. He has developed over 220 quantitative analytic trading models. Richard implemented the first supercomputer on Wall Street and went on to design his own High-Performance Computer system for REMTCS as well as implemented these systems for 3 hedge funds startups where he is a principal in each.

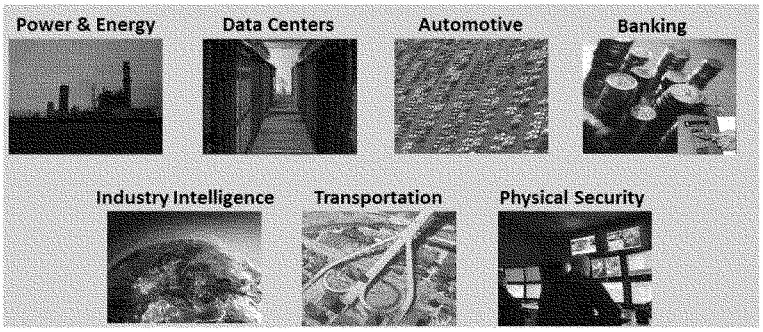
Richard has been involved with 8 successful startups, 3 of which became "Top 50"/" Fast 50"/corporations; Culturefinder, Infogate (sold to AOL as AOL Financial), Albridge Solutions- sold to PNC Bank for $385MM.

He has over 18 years of experience consulting for Fortune 500/1000 companies in the US, Europe and Asia.

Richard is an enterprise architect, a security systems visionary, an expert in real-time systems networking, applications development, infrastructure design and IT strategy for multi-tiered environments including Web technology, and high volume online transaction, non-stop and clustered computing.

Additional Technology Applications

In addition to the significant growth from its existing portfolio of products, REMTCS' core AI technology is capable of being adapted to numerous, as yet undeveloped, applications.



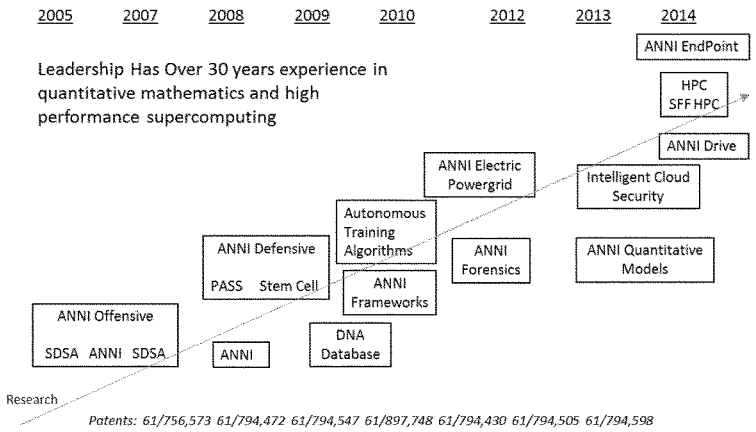
Other Applications:

Financial trading algorithms

Legal

Digital Rights Management

Technology Development Time Line



Intellectual Property Considerations

REMTCS has obtained over fifty patent claims covering artificial intelligence, fully autonomous reaction to identified malware, behavioral analysis computer hardware, processes, and other items. These patents have been obtained. Full Patent Cooperation Treaty (PTC) International Patents are pending.

These filings are intended to secure protection over a variety of ANNI system elements, including:

- Integration into any existing network infrastructure inclusive of firewalls
- Core components, such as a unique real-time detection and defense engine, including disabling of any infected assets
- Proactive anti-malware engineering
- Comprehensive near real-time forensics, incorporating complete reporting, diagnostic and audit trails, and sourcing of any malware

In addition, the Company maintains a large body of proprietary intellectual property including 195 algorithms.

For questions please call Mr. Charles H. Viator, Jr. on 703 (569-8154)

April 4, 2017

Utilities Technology Council
Statement for the Record
Senate Energy and Natural Resources Committee

Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats

The Utilities Technology Council (UTC) appreciates the opportunity to submit a Statement for the Record in the U.S. Senate's Energy and Natural Resources Committee's hearing to "Examine Efforts to Protect U.S. Energy Delivery Systems from Cybersecurity Threats." UTC is a global trade association representing for-profit and not-for-profit electric, gas, and water utilities on issues involving utility information and communications technology (ICT). Our members work every day to ensure the safe, reliable and secure delivery of electricity. UTC appreciates the Committee's hearing to highlight the tremendous amount of work that electric utilities have done to mitigate the ever-evolving cyber threats they face.

Electricity is recognized by government and the private sector as one of the most critical of the critical infrastructures. Life as we know it today is dependent on the reliable delivery of electricity. What is not recognized often enough, however, is the absolutely critical need for electric utilities to have access to the information and communications technology they need to maintain not only day-to-day operations, but also operations during times of restoration and recovery from a variety of hazards, including natural disasters and cyber attacks. Given its jurisdiction, the Senate Energy and Natural Resources Committee can play an essential role in ensuring that discussions around utility ICT needs, such as access to spectrum, are an integral component of discussions about securing the country's energy infrastructure.

As the international trade association for the telecommunications and information technology interests of electric, gas and water utilities and other critical infrastructure industries, UTC has a unique perspective into the ICT needs of utilities around the world. Created in 1948, UTC continues to advocate for policies that promote the development of telecommunications and IT to support the safe, reliable, efficient and secure delivery of utility energy and water services to the public at large. Our members include all types of utilities -- large investor-owned utilities that may serve millions of customers across multi-state service territories, as well as smaller electric cooperative and municipal utilities that may serve a few thousand customers in rural areas and isolated communities.

UTC would like to emphasize the following:

The public private partnership embodied in the Electricity Subsector Coordinating Council (ESCC) is a robust and essential element of our members' critical infrastructure protection activities and should be supported at every opportunity. Our members serve on the ESCC, and UTC's President and CEO is an invited guest of the ESCC. This public private partnership has been instrumental in 1) improving the communication between the government and the private sector on the threats and vulnerabilities that exist, 2) addressing the obstacles to expanding the real-time situational

1129 20th Street, NW • Suite 350 • Washington, DC 20036 USA • 1.202.872.0030 • FAX: 1.202.872.1331

awareness electric utilities need to mitigate these rapidly-changing threats, 3) educating industry about cybersecurity best practices, and 4) identifying technology gaps to better inform research and development. The Department of Energy's (DOE's) role in this effort has been foundational to its success and we would encourage the Committee to build upon and strengthen this well-functioning structure.

Standards alone will not get us the security we need. The carefully constructed relationship that exists between industry, the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO), and the Federal Energy Regulatory Commission (FERC) is working well and should continue as is to ensure that industry and government can address the most critical issues from a risk-based perspective. UTC's members are also actively involved with NERC – both with the Electricity Sector Information Sharing and Analysis Center (E-ISAC) and the development and implementation of the Critical Infrastructure Protection (CIP) standards. Each of these functions within NERC play important and different roles needed for mitigating the threats. UTC believes that existing NERC CIP requirements have helped bring a much-needed spotlight on utility security. These baseline standards in conjunction with the efforts of the E-ISAC, the ESCC, the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and others to teach best practices on how to mitigate the threat, are the type of multi-pronged approach that is needed for protecting these critical systems.

We must closely examine cross sector interdependencies and enhance cross sector collaboration. We urge this Committee to take a leading role in ensuring that as we explore how to protect the electric grid from all hazards, we include how cross sector interdependencies can impact grid resilience. It is critical for electric utilities to have access to the ICT they need to maintain not only day-to-day operations, but also operations during times of restoration and recovery from a variety of hazards, including natural disasters and cyber attacks. Utility ICT needs, such as access to spectrum that is free from interference and congestion, are an integral component of discussions about securing the country's energy infrastructure. Unfortunately, electric utilities, despite their criticality to homeland security, face increasing challenges in accessing spectrum. The need for spectrum becomes even more acute as we move to more wireless technologies, smart grid, and the Internet of Things (IoT). We must think about how we appropriately weight electric utilities' need for spectrum so they have access to the ICT they need for reliable and secure electric service operations. Reliable communication systems are essential for getting the lights back on more quickly.

UTC appreciates the testimony of Mr. Duane Highley, Arkansas Electric Cooperative Corporation, Mr. Gerry Cauley, NERC, the Honorable Dave McCurdy, American Gas Association (AGA), and Ms. Patricia Hoffman, DOE, as all of these statements detail the extensive efforts UTC's members and the industry have undertaken to understand the threats, learn best practices for mitigating those threats, and continually working to improve the resilience of their systems. UTC will continue to work with our member utilities and our government partners including DOE, FERC, DHS, NIST, the Federal Communications Commission (FCC), and others, lending our expertise on the vitally important ICT and communications needs of the electric sector. We look forward to assisting the Energy Subcommittee as they work to understand all that is being done to provide safe, secure, and reliability electricity, which is essential to our country's economic and national security.

1129 20th Street, NW • Suite 350 • Washington, DC 20036 USA • 1.202.872.0030 • FAX: 1.202.872.1331