AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 114–721

ASSESSING THE SECURITY OF CRITICAL INFRASTRUCTURE: THREATS, VULNERABILITIES, AND SOLUTIONS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MAY 18, 2016

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE

23–709 PDF WASHINGTON : 2017

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire
JONI ERNST, Iowa
BEN SASSE, Nebraska

THOMAS R. CARPER, Delaware
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota
CORY A. BOOKER, New Jersey
GARY C. PETERS, Michigan

CHRISTOPHER R. HIXON, *Staff Director*
BROOKE N. ERICSON, *Chief Counsel for Homeland Security*
JOSE J. BAUTISTA, *Professional Staff Member*
SERVANDO H. GONZALES, *U.S. Customs and Border Protection Detailee*
GABRIELLE A. BATKIN, *Minority Staff Director*
JOHN P. KILVINGTON, *Minority Deputy Staff Director*
ABIGAIL A. SHENKLE, *Minority Professional Staff Member*
MATTHEW R. GROTE, *Minority Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
BENJAMIN C. GRAZDA, *Hearing Clerk*

CONTENTS

WITNESS

WEDNESDAY, MAY 18, 2016

ALPHABETICAL LIST OF WITNESSES

APPENDIX

ASSESSING THE SECURITY OF CRITICAL INFRASTRUCTURE: THREAT, VULNERABILITIES, AND SOLUTIONS

WEDNESDAY, MAY 18, 2016

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:01 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Portman, Lankford, Ayotte, Ernst, Sasse, Carper, McCaskill, Tester, Heitkamp, Booker, and Peters.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. I want to thank all of our witnesses for taking the time to join us here and for your thoughtful testimony. I am looking forward to the hearing.

Senator Carper is at a different committee hearing right now. He will be joining us later. And, we have a number of Members that also will but are running behind, but I would like to get started and be respectful of your time.

When I first took over the Chairmanship of this Committee, coming from a business background as a manufacturer, I certainly found that developing a mission statement for any organization is pretty helpful. It directs the activity of the organization. So, working with Senator Carper, we developed a pretty simple mission statement: to enhance the economic and national security of America. They are inextricably linked.

This Committee is really two committees in one: Homeland Security and Governmental Affairs. It is like the House Oversight Committee and Homeland Security.

On the homeland security side of the Committee, we established four primary priorities; border security, cybersecurity, protecting our critical infrastructure, including our electrical grid, and then doing whatever we can to combat Islamic terror and other violent extremists to keep the homeland safe. We have been pursuing that mission statement. We have been addressing those top priorities.

I guess it was about a year ago when we held our first hearing on the potential threat of electromagnetic pulses (EMP). We had former Central Intelligence Agency (CIA) Director James Woolsey. We had Dr. Richard Garwin, who worked with Enrico Fermi. I believe Dr. Fermi referred to Dr. Richard Garwin as one of the few

true geniuses he had ever met. So, some smart people who even though some people consider, for example, the threat of EMP hokum, I asked pointblank these individuals, "Do you think it is hokum?" The answer was an unqualified, "No, absolutely not."

Mr. Koppel, I truly appreciate the fact that you have written this book to raise public awareness of the vulnerabilities that we have with our electrical grid.

In the 2001 National Defense Authorization Act, they authorized EMP commissions to take a look at the potential threat posed by things like EMP and potentially geomagnetic disturbances as well. That 2008 commission established some recommendations that were to be undertaken by the Department of Homeland Security (DHS) and the Department of Energy (DOE). I am going to take time to read them. They go A through O, and I just want to take time to read what the 2008 EMP Commission recommended:

"A. To understand system and network-level vulnerabilities, including cascading effects."

"B. Evaluate and implement quick fixes."

"C. Develop national and regional restoration plans."

"D. Assure availability of replacement equipment."

"E. Assure availability of critical communications channels."

"F. Expand and extent emergency power supplies."

"G. Extend black start capability."

"H. Prioritize and protect critical nodes."

"I. Expand and ensure intelligent island capability."

"J. Assure protection of the high-value generation assets."

"K. Assure protection of high-value transmission assets."

"L. Assure sufficient numbers of adequately trained recovery personnel."

"M. Simulate, train, exercise, and test the recovery plan."

"N. Develop and deploy system test standards and equipment."

"O. Establish installation standards."

Now, again, I realize that is kind of short, bullet-point form, but to me those are some pretty reasonable recommendations. The Secretary of the Department of Homeland Security and the Secretary of the Department of Energy were basically—it was recommended that their agencies start addressing these quick fixes, these recommendations.

In our hearing, a report of the Government Accountability Office (GAO) basically reported that none of these had been done. This was, again, 2008, the results of a 2008 EMP Commission. Here we are in 2015, now here we are in 2016. None of this has been done. People are not taking this threat seriously, and we have to.

So, again, the purpose of this hearing is to lay out the realities, the very complex problem. Again, I am not an electrical engineer, but we have to start looking at exactly what the vulnerabilities are. We have to identify it. We have to define it. And, from my standpoint, we have to take that first step in solving any problem, which is admitting we have one, which is the purpose of this hearing.

Now, I do have a written statement for the record that I would ask to be entered,[1] without objection.

---

[1] The prepared statement of Senator Johnson appears in the Appendix on page 45.

We will wait for Senator Carper. When he comes, we will see if he wants to offer an opening statement. But until that point in time, it is the tradition of this Committee to swear in witnesses, so if you will all rise and raise your right hand. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

General DUNBAR. I do.

Mr. FARMER. I do.

Mr. KOPPEL. I do.

Mr. AARONSON. I do.

Chairman JOHNSON. Thank you.

Our first witness is Major General Dunbar. General Dunbar is Wisconsin's adjutant general. In this role, General Dunbar commands the Wisconsin National Guard and is responsible for emergency management. He also serves as Wisconsin's homeland security adviser, chairs the Homeland Security Council, and is the senior State official for cyber matters. Previously, he served in the U.S. Air Force, the Washington Air National Guard, and National Guard Bureau.

General, thank you for your service, and we would welcome your testimony.

TESTIMONY OF MAJOR GENERAL DONALD P. DUNBAR,[1] ADJUTANT GENERAL, STATE OF WISCONSIN

General DUNBAR. Thank you, Senator. Good morning, and good morning to Members of the Committee. Thank you for the opportunity to speak today. I am the adjutant general for the State of Wisconsin, and although I appear before you today in uniform, I want to stress that I am appearing on behalf of the State of Wisconsin in a State status. I am not on active duty orders, and no one in the Defense Department (DOD) has seen, reviewed, or approved my remarks.

I am privileged to command Wisconsin's National Guard. As you know, the National Guard is constitutionally unique. It has two foundational roles: We are the primary combat reserve of the U.S. Army and the U.S. Air Force and the first military responders in the homeland.

You mentioned my other roles. Thank you for that. It is an honor to appear before the Committee to discuss critical infrastructure.

Critical infrastructure is a shared responsibility. The Federal Government has a substantial role as do the industry leaders who generally own and operate the infrastructure. However, States have a leadership role as well. I will touch briefly on our organization, our strategy, and our efforts at addressing the threats to critical infrastructure in Wisconsin.

We did not create a separate agency to manage homeland security, choosing instead to rely on existing roles and responsibilities. Our Governor created a Homeland Security Council, which includes representatives from State agencies and first responders who are joined by Federal partners and industry leaders regularly to attend and participate.

---

[1] The prepared statement of General Dunbar appears in the Appendix on page 48.

Our homeland security strategy is updated quadrennially after each gubernatorial election and provides a framework to guide continuing efforts in preparation and protection of our communities and citizens. It also guides our investment of State and Federal resources. The strategy seeks to ensure that our first responders are trained and equipped, that our critical infrastructure is safe and secure, and that we continue to plan and prepare for emergencies and disasters that may impact our State.

This strategy is our keystone document. It has four priorities: cybersecurity, preventing and protecting against asymmetric/terrorist threats, catastrophic incidents, and capability sustainment. Each priority has identified goals and objectives designed to be specific and measurable.

Time does not allow for an in-depth discussion on all aspects of our efforts, but we are working on lines of effort to mitigate the threats to critical infrastructure. I will highlight just a few.

In cybersecurity, we have developed at State expense a framework of five State cyber teams prepared to assist State and local government with cyber response. Three of these teams consist mainly of State and local professionals who, by agreement, have permission to respond when activated for response. We are developing a fourth team consisting of industry leaders which will also be available to respond, and our fifth team will come from the National Guard. We currently have in the National Guard a computer network defense team that helps protect our portion of the DOD network.

The new team that we are building will be a computer protection team in collaboration with the Illinois Army National Guard. This team will be operational by the end of 2019, and although trained to meet the Army's military requirements, it is fully available for State active duty at the Governor's discretion.

The Wisconsin National Guard is finalizing an agreement with several of our utility companies. Our agreement is aimed at information sharing and the potential for National Guard physical support. We initiated this relationship after learning of certain real-world events, such as the attack in Metcalf.

Wisconsin Emergency Management (WEM) and the Department of Natural Resources partnered with our railroad commissioner and major rail lines and have arranged for a cache of critical foam to be stored regionally at no expense in case we have an oil spill and fire on our rail lines.

We have also revamped our HazMat structure, creating more versatile and regionally diverse teams that are strategically located consistent with population density and key lines of communication.

We are working with our Public Service Commission (PSC) and our utilities to understand better the threat to our electric grid and actively seeking ways to mitigate potential effects.

As an example, we are working with our public water and sewage utilities, all of whom have generator backup for their systems. However, all of these systems require diesel fuel, and we are working hard to make sure we have a solid plan for delivery in an outage.

Another area we are discussing, although this is much more difficult given our utilities' sophistication, is the physical backup to

utility systems. I am no expert, but I took note of the recent cyber attack in the Ukraine which disrupted their power system. Clearly, Ukraine is not a system on par with the system of the United States; however, when they understood that the attack was a cyber attack, they switched to manual backup. Based on open-source reporting, this occurred after about 6 hours. The cyber network may yet still be infected, but the power disruption lasted only 6 hours. To my mind, that is a powerful lesson worth exploring, and we are working with our PSC to ask these questions of our utility partners.

Last, I will mention that our National Guard works closely with emergency management across the board in planning for and exercising our emergency plans. We are certainly not alone in this aspect, as the National Guard across the Nation has unique relationships with law enforcement, firefighters, Federal agencies, and industry partners. Always ready, always there, we provide our Nation's Governors with a surge force that is highly trained and relevant across the domestic response spectrum.

I have submitted my written testimony for the record and greatly appreciate the opportunity to appear today and offer these brief remarks. I look forward to any questions you may have.

Chairman JOHNSON. Thank you, General Dunbar. By the way, your written testimony is entered into the record.

Our next witness is Tom Farmer. Mr. Farmer is the chair of the Partnership for Critical Infrastructure System (PCIS) Cross-Sector Council. Mr. Farmer worked with the lead representatives for each of the critical infrastructure sectors and with senior government officials in coordinated efforts to advance priorities and capabilities in critical infrastructure protection and resilience. He also serves as assistant vice president for security for the Association of American Railroads. Mr. Farmer.

TESTIMONY OF THOMAS L. FARMER,[1] CHAIR, CROSS-SECTOR COUNCIL, PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY

Mr. FARMER. Thank you, sir, very much. Chairman Johnson, Members of the Committee, and staff, thank you very much for this opportunity to address the priorities and cooperative efforts of the Partnership for Critical Infrastructure Security Cross-Sector Council in critical infrastructure protection.

As the current Chair, I am privileged to speak for a group of dedicated professionals across industries who volunteer their time and efforts to take on leading and organizing capacities in their respective sector coordinating councils, those forums formed in the National Infrastructure Protection Plan (NIPP) that enable industry to communicate and coordinate effectively with government.

It is the respective efforts of these professionals that merit attention, for they represent a sustained commitment to partnerships and action, partnerships within their sectors, across sectors, and with Government.

The written statement submitted to the Committee addresses a sampling of their efforts. Their scope exceeds the time available for

[1] The prepared statement of Mr. Farmer appears in the Appendix on page 57.

a fuller delineation here, but as I prepared for the hearing, a representative of the dam sector, the Chair of the Dam Sector Coordinating Council well captured their scope in a delineation of his sector's activities: preparedness planning, exercises within the sector among dam facilities, cross-sector exercise with government officials and representatives of other industries, information sharing, cybersecurity guidelines and tools that are developed in partnership with government, training and webinars focused on security awareness and preparedness.

Each of the sectors' leads consistently delineate very productive, proactive efforts on behalf of their respective sectors. Across sectors we are supporting these efforts by outreach and capabilities offered by government organizations. They include the Department of Homeland Security, the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), the various sector-specific agencies, and State fusion centers. The support in these areas is fundamental to enhance and sustain effectiveness in critical infrastructure protection, areas like intelligence assessments, information sharing, risk assessments, resiliency assessments, tailored training and exercise programs, guidance materials for organizational and sector-based preparedness planning, and focused engagement on particular threats or security concerns.

This extensive body of work creates opportunities that draw insights, that glean lessons learned, to apply them practically in security posture, and in protective measures. A colleague in the Sector Coordinating Council well captured the concept with the phrase "next-level analysis," and priorities of our council emphasize this concept.

What we are talking about is knowing what we can know as thoroughly as possible, about using information proactively, about analyzing the wealth of experience gained by the expansive and effective work undertaken by DHS, FBI, and other components, particularly focusing on trends, on patterns, on indicators of recurring concerns.

Terrorism provides one example. Investigations of attacks and attempts and disrupted plots reveal over and over again indicators that were experienced, observed, and encountered that preceded the event. But their significance often was not understood, even if they were reported.

Similarly, active shooter investigations reveal similar behavioral indicators that preceded the events. We must and can learn from this adversity, through analysis that highlights those recurring indicators of preparations, analysis that enables professionals in industry and government to identify the opportunities for security measures, and activities to make a difference.

We are very familiar with the "See Something, Say Something" campaign. It works. But we can make it better. With this type of analysis, we can advance and information the "See Something, Say Something" concept, emphasizing those observable indicators and activities and preparations that have preceded acts of lethal and destructive violence time and again, and apply that information in security, training, and awareness initiatives with employees across industries to inform their vigilance both on the job and in their home communities.

In cybersecurity, as we contemplate the hundreds of onsite and virtual assistance visits provided by DHS and FBI in response to cyber attacks, as we look at the in excess of 1 million indicators of concern that have been disseminated by DHS to the private sector, opportunity emerges again, for analysis that produces a cyber threat profile, a profile we can update on a recurring basis, to help organizations across sectors understand what they are most likely to see in terms of how cyber threats materialize. What are those vulnerabilities that are so often exploited? What are those protective measures too often found lacking?

Now, as these analyses are produced why dissemination is essential, we need to make sure we have depth of penetration across government and industry. In the Cross-Sector Council, we have partnered with DHS to do just that, leveraging existing councils in government and industry to ensure that information in a timely manner reaches those who are best equipped to get it out to their respective constituencies.

We have also introduced the capability to share classified information and tested it on April 26. Two components of the Wisconsin fusion center participated. And, as part of that effort, we focus on ensuring that as the intelligence community (IC) produces products that are classified, they also produce an unclassified "tear line," a version that all who attend the briefing can take back to their organizations to inform vigilance and security measures.

The efforts of the respective councils are sound. They are proactive. No one is resting on laurels. We consistently seek opportunities to progress, and our shared objective of enhancing critical infrastructure protection is attainable.

I thank you very much for this opportunity to participate in this esteemed forum today.

Chairman JOHNSON. Thank you, Mr. Farmer.

Our next witness is Ted Koppel. Mr. Koppel is the author of the book "Lights Out"—I have a copy. Unfortunately, I do not have the cover. When I actually read books, I take it off. It is "Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath." He is also a 42-year veteran of ABC News where he served as anchor and managing editor of the "Nightline" program from 1980 to 2005. And, I would point out this is actually my brother's book. He gave it to me. I would say he is a little alarmed. "Did you know this?" I was aware.

Mr. Koppel, thank you for coming here. I look forward to your testimony.

TESTIMONY OF TED KOPPEL,[1] AUTHOR, "LIGHTS OUT: A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH"

Mr. KOPPEL. Mr. Chairman, Mr. Ranking Member, Members of the Committee: Your late colleague, the distinguished Senator from New York, Daniel Patrick Moynihan, liked to say that each of us is entitled to his own opinion; we are not, however, entitled to our own facts. That observation, which once seemed both sensible and self-evident, can no longer be taken for granted.

[1] The prepared statement of Mr. Koppel appears in the Appendix on page 64.

In a political climate where even the President's status as a natural-born American citizen remains the object of doubt for more than a quarter of our population as he nears the end of his second term in office, in that climate it will be difficult to settle the far more complex issue before the Committee this morning: Is the Nation at risk of a crippling cyber attack against elements of our infrastructure in general and against one or more of our electric power grids in particular? After more than a year of research into the question, I believe the answer to be "yes."

Simply stated, the electric power industry is made up of 3,200 separate companies linked in a network that both generates and distributes electricity. For the system to function, a perfect balance has to be maintained between the amount of electricity being generated and the amount being distributed. Only the Internet is capable of maintaining that exquisite balance at all times. The Internet was never designed to be defended. The Internet remains vulnerable to cyber attack. Evidence of that vulnerability is accumulating every single day in private industry, government agencies, and in breaches of our personal data. General Keith Alexander, the former head of the National Security Agency (NSA), likes to say that there are only two kinds of companies—those that have been hacked and those that do not yet know it.

Members of this Committee are certainly familiar with the conclusion of our intelligence agencies that the Chinese and the Russians have already mapped and penetrated the systems that control our electric power grids. Iran is not far behind. Nations like North Korea and Syria are enhancing their cyber warfare capabilities. It is surely only a matter of time before a terrorist group, unrestrained by any geopolitical interests, acquires the capability to attack one of our power grids.

The problem, as Tom Ridge, our first Secretary of Homeland Security, noted, is that ours is a reactive, not a pre-emptive society. In the wake of the attacks on September 11, 2001, the United States embarked on actions and expenditures that would have been inconceivable only a week earlier.

My message to this Committee this morning is simple: The Nation cannot wait for a cyber attack on the grid before making preparations for its consequences. It is my belief—and again, this Committee has access to more information on this subject than—I believe that while the Department of Homeland Security has plans for dealing with the consequences of hurricanes, blizzards, floods and earthquakes, it has no discrete plan for dealing with the aftermath of a cyber attack on one of the Nation's power grids. The Department's recommendations for each disaster are essentially the same: a 2-to 3-day supply of food and water for each person, a plan for families to meet at a pre-arranged point, a supply of essential medicines, flashlights, and a battery-powered radio.

A cyber attack against one of our electric power grids could deprive tens of millions of Americans of electricity for a period of weeks or even months. I asked Homeland Security Secretary Jeh Johnson what, exactly, he would be telling Americans on their battery-powered radios after an attack that he was unwilling or unable to share now. He gestured toward a shelf carrying several

white binders: "I am sure there is a plan up there somewhere," he told me. I do not share the Secretary's confidence.

We have neither the adequate food supplies to take care of those millions who decide to shelter in place, nor the collaborative plans with State governments to house and feed what could amount to tens of millions of internal refugees. If we began tomorrow, Mr. Chairman, implementing such plans would still take a couple of years.

I thank the Committee for its attention to this critical issue.

Chairman JOHNSON. Thank you, Mr. Koppel.

Our final witness is Scott Aaronson. Mr. Aaronson served as the managing director for Cyber and Infrastructure Security at the Edison Electric Institute (EEI). Prior to joining EEI, Mr. Aaronson served as a senior adviser to the Chairman of the House Foreign Affairs Committee and Senator Bill Nelson. Mr. Aaronson.

TESTIMONY OF SCOTT I. AARONSON,[1] MANAGING DIRECTOR, CYBER AND INFRASTRUCTURE SECURITY, EDISON ELECTRIC INSTITUTE

Mr. AARONSON. Thank you, Chairman Johnson and Members of the Committee. I am glad to be here today to discuss security of the power grid. We appreciate you holding this important hearing and that Mr. Koppel chose this subject for his book. As owners and operators of some of the Nation's most critical infrastructure, we share his concern and the Committee's to ensure that the grid is secure and resilient.

From some of the headlines and movie script scenarios out there, you might think that we are not doing anything and being complacent, that a month-long power outage is inevitable. If there is one thing that you take from my testimony today, it is to understand that the industry is doing an amazing amount of work at all levels all of the time to defend the grid and to respond to an incident.

You have to remember, we live and work in the communities that we serve. Our infrastructure is our most important asset, so we have every incentive to make security a major priority.

Since these topics can be sensitive, and even classified occasionally, we may not talk about them a lot in public, but do not take that lack of discussion for inaction. My written testimony has more extensive details on how electric companies address threats, so I will not read that to you. But I do want to go through what we effectively call the three legs of the stool that make up security for the electric grid.

The first leg of the stool is standards. The electric industry has mandatory and enforceable critical infrastructure protection (CIP), regulatory standards for both cyber and physical security. These are not lax, lowest common denominator standards. These are rigorous requirements that improve the industry's security posture. Failure to comply can cost up to $1 million per infraction per day, so suffice it to say there is a lot of incentive to comply. But compliance does not equal security. Security is not a check-the-box exercise; if I do X, Y, and Z, I am secure. No. You have laid a foundation for security.

[1] The prepared statement of Mr. Aaronson appears in the Appendix on page 66.

The second part of what makes for full security, and the second leg of the stool, are partnerships. It has already been said—I think it was Major General Dunbar—that protection of critical infrastructure is a shared responsibility. In order to be prepared for an ever-changing threat environment, industry and government are partnering at an extremely high level. In addition to my role at EEI, I also am part of the secretariat for the Electricity Subsector Coordinating Council (ESCC). Along with the cooperative and public power segments of the industry, the ESCC is made up of 30 Chief Executive Officers (CEOs) from across the sector. These CEOs are meeting regularly with senior government officials from the White House, DHS, DOD, FBI, intelligence community, and the Department of Energy—our sector-specific agency.

They do not just meet to simply update each other or pat each other on the back and say, "We are doing a great job." They are setting a strategic vision for how we can improve the security posture of the industry and, by extension, the Nation, bringing together government and industry capabilities in a concerted way.

So, the ESCC focus is on four major issues, and I will go through each of them briefly.

The first is deploying tools and technology. The focus here has been moving government-developed tools to industry applications to improve situational awareness, and the best example of that is the Cyber Risk Information Sharing Program (CRISP), which you can find in my testimony.

The second is improving the flow of information, making sure the right people are getting the right information at the right time. From classified briefings for executives to actionable intelligence for operators, government and industry are sharing threat information more often and more easily.

The third is coordinating with other sectors. While electricity is always described as the most critical of the critical—everybody relies on us—without water we cannot generate steam or cool our systems; without telecommunications, we cannot operate; without transportation and pipelines, we cannot move our fuel or move our equipment. There are a lot of ways to impact the grid short of attacking the grid.

To address these interdependencies, the power industry is actually working across sectors. And, in fact, Tom Farmer and the Nation's railroads have been great partners as we work together, for example, to move large transformers during incidents.

The last area of focus for the ESCC also happens to be the last leg of the stool. So we have standards; we have partnerships. The last is preparations for response and recovery. Simply put, electric companies have to be right 100 percent of the time, and the adversary has to be right only once. Given those odds, preparation for an attack is just common sense.

First of all, we have a history of working together to restore power after an incident through mutual assistance networks where workers from unaffected companies descend on the affected company to restore power. We also have robust spare equipment sharing programs, including bilateral and multilateral arrangements, as well as a fully developed and legally binding plan called the Spare Transformer Equipment Program (STEP), that requires the

sharing of large, hard-to-replace spare transformers during a national incident.

We exercise regularly. Of particular note is the North American Electric Reliability Corporation (NERC's) GridEx series, which brings thousands of owners and operators and executives from across North America in the largest exercise of its kind. And, now we are developing a cyber mutual assistance program to coordinate resources for companies affected by cyber incidents.

The bottom line is this. We are constantly working to manage risk, but understand that we can never entirely eliminate it. There is not enough money in the world to protect against every threat in every location, but we are working to prevent incidents from having long-term or devastating impacts. We understand that the service we provide is critical to the life, health, and safety of Americans. From CEOs to operators, the power sector has shown it takes this responsibility seriously and is committed to constantly improving its security posture as these threats evolve.

Again, I appreciate the opportunity to be here and look forward to answering your questions.

Chairman JOHNSON. Thank you, Mr. Aaronson. Let me start with you. You just talked about the STEP program, about these replacement large power transformers. In our EMP hearing, I asked Dr. Richard Garwin how many are critical. What is the number of large power transformers that we really need to protect. He gave me a ballpark of somewhere between 200 and 700 of these large power transformers. Would you agree with kind of around that assessment?

Mr. AARONSON. In fact, I do. That is a fair assessment, and depending on what criteria you are using, someplace in there the number is going to fall.

Chairman JOHNSON. So, how many replacements do we have for those that are basically ready to be moved into place in case, either through a kinetic attack or a cyber attack or EMP or geomagnetic disturbance (GMD), those large powerful transformers are destroyed?

Mr. AARONSON. So, the STEP program is actually governed by a nondisclosure agreement, so the specific number I cannot give you, but I can tell you this:

No. 1, we are sufficiently spared.

No. 2, outside of those spares that are dedicated through the Spare Transformer Equipment Program, other companies have, first of all, operational spares that they use for obvious reasons. You will use a spare when you are doing maintenance on an active transformer, so you have that in place regardless. We have other ways of sharing equipment beyond just the Spare Transformer Equipment Program.

Chairman JOHNSON. Let me ask you, so would I be able to—with nondisclosures, could I as a United States Senator find out how many we really have to satisfy myself that we really are covered?

Mr. AARONSON. I would have to go back to the industry to see if we would be able to breach the nondisclosure for that purpose.

Chairman JOHNSON. I would appreciate that, because if you do not have spares, what is the length of time to replace some of these large power transformers?

Mr. AARONSON. So, the number that we have heard all of the time is an 18-month lead time. That is not entirely accurate. Under duress, there are ways to procure transformers more quickly. You also have to understand that there is a significant amount of excess capacity in the system. So, when I say that we are looking to be able to operate under duress, we may go to a suboptimal State. One of the lessons that was learned out of Ukraine is going to a more manual operation. So this rush to automation is great because it gives us wonderful efficiencies, but it also increases the attack surface. So by diminishing the attack surface and looking at the ability to operate manually, the ability to operate suboptimally, the ability to focus resources on more critical load, whether it be hospitals, first responders, military installations, those are all things that, because of this CEO leadership, we are developing that capability.

Chairman JOHNSON. Based on public reports, my—"assumption" is probably not the right word, but it sounded like the reason Ukraine actually restored power 6 days——

Mr. AARONSON. 6 hours.

Chairman JOHNSON. 6 hours, is because they actually had manual breakers, which we really do not have nowadays because we are more advanced. We have it all computerized. Correct?

Mr. AARONSON. The answer is, "It depends." I always hate giving that answer, but the answer is, "It depends." In some cases, there is the capacity to operate manually. In others, we are going to need to continue to develop it.

Chairman JOHNSON. OK. General Dunbar, in your emergency planning, Mr. Koppel talked about in general we have plans to have provisions for 2 to 3 days. Is that pretty much what you have planned for Wisconsin in your capacity, in your responsibility?

General DUNBAR. Our plans for a long-term power outage, taking care of the public, quite honestly our goal is to try and keep the people in their homes so they do not add to the problem by a mass evacuation. We do rely on the industry for the food stocks. It is a concern of mine because one system is very efficient as you know, and if something shuts down, it can quickly deplete it out. We do not have in Wisconsin a supply of meals ready to eat (MREs) beyond what you would expect for the National Guard, and even that is limited because at the DOD level it has those kinds of supplies.

Chairman JOHNSON. Mr. Koppel, I was pretty impressed with the level of reporting and the digging you did in your book. You did not seem particularly convinced. You seemed to certainly ask some pretty hard questions, and you were not getting particularly good answers. Do you agree with Mr. Aaronson that we are probably sufficiently backed up in terms of large power transformers?

Mr. KOPPEL. Well, first of all, I am in no position to agree or disagree with him because I do not have access to the numbers either. What I have heard, and what was in a Department of Energy report back in 2014, is that the number of large power transformers is quite literally in the tens of thousands. So, I am frankly a little bit astonished at the notion that we are only talking about—what did you say?—250 or so.

Mr. AARONSON. 200 to 700.

Mr. KOPPEL. 200 to 700. I think, A, the number is greater. B, I think that we are dealing with a problem of unique pieces of equipment that cannot easily be interchanged. And, C, Mr. Aaronson sort of dismissed the notion that it takes up to 18 months to get a new one, but most of these large power transformers are not constructed in the United States. The majority—I think about 70 percent of them—are constructed overseas. And, by the time you order these and have them built, we are talking about pieces of equipment that weigh between 400,000 and 600,000 pounds. It takes at least a year and up to a year and a half to order a new one and have it delivered. And even once you get it to the United States, delivering these things is incredibly difficult because they tend to overstress pieces of infrastructure like failing bridges.

Chairman JOHNSON. Mr. Farmer, in your testimony you were really concentrating a lot—and this is, of course, good—you know, on coordination and communication and planning, that type of thing. But can you talk about what we have actually done to prepare and protect—physically, what we have done in terms of infrastructure to improve our survivability and improve our ability to stand the power grid back up?

Mr. FARMER. Well, I am not specifically qualified to discuss in detail the electrical sector. What I can say, though, is that there have been very productive partnerships fostered through the Cross-Sector Council that enable industries to identify interdependencies and then work in concert to enhance their resiliency, to enhance their preparedness, to address concerns. Scott Aaronson addressed in his testimony the cooperation with the railroad industry and preparations to move large transformer equipment should we be in a situation where, due to some form of damage, a transformer is taken out of operation. And the electrical industry, the electrical sector approached our industry. We have worked in close coordination to do a number of things. One is to have preparedness plans in place for railroads to move the equipment. We have identified the types of rail cars that move the equipment. We maintain a current inventory of where those rail cars are. We have worked with the electricity sector through exercises the last 2 years.

Each year, the railroad industry holds an annual security exercise. In that exercise, we take actual events and take them to another level through realistic terrorism and cyber scenarios to stress our industry's security planning, to stress our procedures, our decision-making, our actions to address concerns, our coordination with Government.

We have integrated that exercise the last 2 years, scenarios involving damage to large power transformers, and then the electrical industry calling upon our industry for support in their movement. So this inventory is maintained by a group called Rail Link that provides informational technology (IT) support to our industry. We can generate an updated inventory within a matter of minutes to identify where the cars are specifically. And during the exercises, railroads' operational leads have worked with representatives of power utilities on what the transportation plan would look like. We are confident that, provided notice of a need, within a matter of hours we would have a rail transportation solution in place.

Chairman JOHNSON. OK. Thank you, Mr. Farmer. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER[1]

Senator CARPER. Thank you. Thank you so much, Mr. Chairman. I want to apologize to our witnesses. As you know, we serve on a number of committees, and one of my committees, the Senate Environment and Public Works (EPW), was holding what we call a markup today, voting on a number of bills, several of which were mine, and I needed to be there to defend them. And, so, I cannot be in two places at once, but I am pleased to be here and thank you all for joining us today on a really important subject. So, I am going to go ahead and use this time to give an opening statement, and then maybe we will have a second round for questions, and I can ask some questions of all of you.

Obviously, what we are discussing today is of immense importance—it is in Delaware, and I know it is in the other 49 States: the security of our critical infrastructure. And, when we talk about critical infrastructure, we are not just talking about the grid and supply of electricity, but also the dependability of our water, even our financial system that supports our economy.

Unfortunately, our electricity and water utilities, as well as our banks, are at risk every day in a number of ways. We have heard a lot lately about criminals and terrorists targeting them online, but these critical services are also at risk due to any number of other hazards such as violent storms, earthquakes, and even failure due to aging and underinvestment.

Fortunately Congress, our Administration, and the private sector have been hard at work to address vulnerabilities in a number of these areas. We have passed legislation in recent years to help make our critical infrastructure more secure and more resilient. I will mention just a couple of examples.

In 2014, Members of this Committee worked for many months to enact legislation to reauthorize and enhance something called the Chemical Facilities Anti-Terrorism Standards (CFATS) program at the Department of Homeland Security. This program is our frontline defense against terrorist attacks against companies that store, manufacture, and process hazardous chemicals.

That same year, 2014, the President signed legislation from this Committee to enhance the cybersecurity center at the Department of Homeland Security that works with critical infrastructure owners to prevent and respond to cyber attacks. That same year we also gave the Department of Homeland Security that authority that it needed to hire the best and brightest cyber talent that is out there.

Just last year, the President signed cybersecurity legislation that the Chairman and I and almost every member of this Committee played a key role in drafting. That crucial new law makes collaboration between the Federal Government and companies grappling with cyber attacks easier and faster while protecting privacy concerns.

---

[1] The prepared statement of Senator Carper appears in the Appendix on page 46.

This year, we are working hard to ensure proper implementation of these and other laws. We are also working to streamline and strengthen the office within the Department of Homeland Security that helps protect critical infrastructure. I have never cared for agencies that have a name that does not really explain what they do, and we have one that we call the National Protection and Programs Directorate (NPPD), that is within the Department of Homeland Security. It does not tell you a whole lot about what they do, but what they do is important. And, as the Chairman knows, my staff and I have been working with the Department of Homeland Security on legislation to streamline this office so that it can be a better partner with industry. We do this in part by elevating its cyber functions and making sure that physical and cyber threats to our critical infrastructure are assessed jointly so the left hand knows what the right hand is doing.

We also want to change the name of the agency so people have some idea of what they actually do to name it the "Agency for Cyber and Infrastructure Security." Doing so will make it clearer that when there is a problem with a vulnerability in the electric grid or some other piece of critical infrastructure, there is no question about who in the Federal Government can help, should help, and who can be held accountable when things go wrong and may be singled out from time to time when there is praise that is due.

As we know, unfortunately, bad things sometimes happen, and the important thing is to be prepared for that when they do. So, I want to credit the men and women at the Department of Homeland Security, including in NPPD and elsewhere, for the hard work they do to ensure our critical infrastructure is secure and resilient. As one example of this important work, the Department conducts onsite assessments and incident response for dozens of critical infrastructure companies every year.

When we talk about critical infrastructure—especially systems that we cannot afford to lose even for a few minutes—this means building resiliency into our policies and practices. Today's discussion about critical infrastructure reminds me of one very promising technology that is already helping to make our country more resilient to electric grid outages. I was a naval flight officer for a number of years during the Vietnam War. When we were over in Southeast Asia, we were stationed at Moffett Field Naval Air Station, and we basically shared that large air station with the National Aeronautics and Space Administration (NASA). And later on, when Moffett Field was closed to active-duty purposes, some private sector companies came in and partnered with NASA and have done all kinds of amazing things. One of them is called "Bloom Energy." They manufacture fuel cells that basically—some of them are manufactured in California. They do a lot of the research and development (R&D) in California, but they also manufacture fuel cells in Delaware. These stationary fuel cells do not require additional transmission capability to move electricity to the end user, meaning reliable electricity can be provided even when the electric grid goes down. Innovative solutions like these can help us be a lot better prepared for a variety of threats in the future.

With that, I want to thank you all for coming, and I look forward to asking you in a few minutes a few questions. Thank you so much.

Chairman JOHNSON. Thank you, Senator Carper. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS

Senator PETERS. Thank you, Mr. Chairman, and thank you to our panelists for your testimony today. This is certainly a very important topic, especially given the changes we are seeing in our society in terms of being interconnected in ways that are difficult to fathom. Critical infrastructure, operational, whether it is dams and bridges, grids, will all be connected through the Internet of Things. We are looking at millions and millions of objects all connected on this elaborate grid, even to the point that our electric toasters will be on the grid. So any sort of attack on a grid could have, without question, a catastrophic impact on society as we know it.

We will talk about a variety of things. Hopefully we will have some additional time, if possible, to talk about some of the cyber issues and physical attacks. But one that I want to take a little bit of time on is an area that I focused on as a result of my work as the Ranking Member on the Space and Science Subcommittee as well as being on the Homeland Security Committee. And, this is something that we know will happen that will be potentially catastrophic to the electric grid if we are not fully prepared. And, that is space weather events where you have mass coronal ejection from the Sun, which sends particles to us here on Earth; it has the impact of compressing the magnetic field if it is large enough, which puts huge pulses of electricity through pipes, through electrical transmission lines, blow up transformers, and shut down vast parts of the grid for the country.

We know it will happen. It happens regularly. Some of them are very large. The largest one that we know of is the Carrington Event, which occurred in 1859. We did not have a whole lot of electricity back then. We only had telegraphs. But all of the telegraphs went down in the country. They were all shut down as a result of this event. The sky lit up. Folks thought it was daytime. They got up, started making their eggs and breakfast. It was the middle of the night. But the sky was illuminated so brightly from the storm. Our scientists believe these storms occur about every 150 years they hit the Earth. That last one was 150 years ago, so it has been a while since we have seen it.

We did monitor a storm of that magnitude in 2012 that missed the Earth by 7 days, so we can come very close to having one of that magnitude as well, which will have a significant impact.

And, so, I have been working with my colleague Senator Booker, who is on both committees with me as well. We have introduced legislation to provide additional research and data, working with the National Oceanic Atmospheric Administration (NOAA) and NASA and all of the Federal agencies, including the Department of Homeland Security. And, the numbers are quite concerning, and the fact that Lloyd's of London estimated that if we get hit with another Carrington-type event, the impact to our economy would be anywhere from $600 billion to $2.6 trillion. That is what we are looking at as an impact from one of these storms. And, we could

see up to 40 million Americans without power. And, as we have had this discussion, talking about the large transformers, some of that could be a year or two. You could have 40 million folks, particularly along the eastern seaboard, which is particularly susceptible to these kinds of solar events. So just think of New York City without power for a year. That is not a good thing. New Jersey without power, which is why Senator Booker has been very engaged in this as well, a very concerning thing, as well as for me in the State of Michigan.

We have to do a better job of preparing for that, and so I would like to ask Mr. Aaronson specifically what sort of research and information do you believe electric utility companies need from us as we are working on legislation to provide more information, more advance warning? What specifically do you need to prepare for this event? And how do you view it?

Mr. AARONSON. So, specifically what you said about your role on the Space and Science Committee, notice is incredibly valuable when it comes to space weather. We actually have GMD standards in place. The North American Electrical Reliability Corporation, because this is something we have known for quite some time could happen, had developed GMD standards which dictate operational protocols to mitigate the impact of a serious coronal mass ejection.

So a big part of that is, again, advance notice from an operational perspective so that operators can take action to shut down certain systems in a graceful way, let the solar flare do what it is going to do, and then be able to start back up, again, using something called—and it has been discussed already—"black start capability," which is basically starting the grid from scratch.

Black start standards are in place, GMD standards are in place, and additional notice from some of those geostationary satellites that give us—I think right now we get about 15 minutes' notice. Increasing that even to 30 minutes would be invaluable.

Senator PETERS. Well, that is an important factor, that we may not have a lot of advance notice. Our prediction capabilities for space weather are not as advanced as they should be. Folks have described it to me that we are where we were with hurricane predictions in the 1930s when it comes to space weather events. So we have a long ways to go; where we may know something is happening, we do not know the magnitude, we do not know where it is going to hit. And hurricanes have a significant impact on us, but a $2.6 trillion impact to the grid that shuts down everything obviously is a major concern.

So if you had just perhaps 18 hours' notice, is that enough time? And what sort of protocols are in place if NOAA, or whatever the relevant agency is at the time as we work out some of these protocols, says, "we think this storm is coming?" This may mean you would have to shut down vast amounts of the grid in the United States.

Mr. AARONSON. So, another thing to note is this is something that, as we have said, we have known about or know could happen for quite some time. And, in fact, there have been examples of impact because of GMD, particularly at the higher latitudes where the impacts are more pronounced.

So there have been examples of GMD impacting the grid, but for minimal amounts of time. You will note that telegraph lines from the 1850s are significantly different than the infrastructure we own and operate today. Mr. Koppel during his answer to Chairman Johnson was talking about the fact that there are literally tens of thousands—45,000, actually, substations in the United States, 55,000 in North America. With that comes an exceeding amount of redundancy.

So the reason that the number is closer to between 200 and 700 of the most critical substations is because those others represent excess capacity and redundancy throughout the system. It is inaccurate to say that a single geomagnetic disturbance would have a universal and unilateral impact across the entire grid. So really what you do have to look at is as much notice as possible to take those operational protocols to shut down the grid to prevent damage, understand that in certain instances like that, you have what is called "voltage collapse," which means that the systems fail safe, and that we are, again, able to restart it through black start procedures. And then, obviously, the redundancy and ability to move transformers around in order to restore power should a particularly damaging geomagnetic storm impact the grid.

Senator PETERS. And I appreciate that comment, which I think highlights the fact that we need to do a whole lot more research into these storms. Because as you mentioned, it does not have a uniform impact across the entire grid, but you need to know where it is hitting, and that is why I made the analogy to hurricane research. You need to know where it is going to actually hit in order to prepare, not the whole eastern seaboard but those particular areas where you think its path—so the same thing for this research for space weather to make sure the resources and the coordination are available for all of the Federal agencies—NASA, NOAA, et cetera—to provide that information to you.

I also wanted to make sure that I highlight the fact that the critical infrastructure are these major transformers, as Mr. Koppel talked about as well, that for the most part are not made in the United States. They are made in Europe, the primary manufacturer for them, and a large space weather event has the potential of not only destroying transformers that exist in the United States, but actually destroying or at least shutting down the facilities that manufacture the transformers in Europe at the same time. A large storm would actually shut down the manufacturing, so then you could not even make these until first you repair the entire infrastructure to even create transformers before you make them and then ship them to the United States. So this is something that I look forward to continuing to work closely with the utilities. I know you are focused on it. I know this is an issue that you have been following as well. But we have got to make sure these protocols are in place and we are really thinking this through.

Mr. AARONSON. And I can say fairly unequivocally that helping to get more advance notice and increasing domestic manufacturing capacity for transformers are two things that the industry would be happy to work with you on.

Senator PETERS. Right. Thank you.

Chairman JOHNSON. Senator Peters, first of all, thank you for that line of questioning. I want to just follow up just briefly. In a previous hearing, we were told, I think, in testimony that about $2 billion damage annually because of other types of solar events. So this is just happening all of the time. But the massive ones like the Carrington Event is something—I do not know how many orders of magnitude greater.

Mr. Aaronson, I just have to ask you, if the protocol gave warning, 15 to 30 minutes, so we can shut down systems, who is going to make that call? Who is going to make that call under a massive geomagnetic disturbance that nobody knows how many of these transformers could be affected, nobody knows, who is going to make that call to shut them offline, take them offline so those effects do not go through those wires and destroy those large power transformers that cannot be replaced?

Mr. AARONSON. So, grid operators are tightly aligned. We have talked about the fact that there are 1,900 entities that make up the bulk electric system. There are regional transmission operators and so on.

Chairman JOHNSON. Who makes the call? I mean, who makes the call we are going to shut them all down in 30 minutes, in 15 minutes?

Mr. AARONSON. It is not as simple as cut the power. That is not how this is going to work. But there is, again, this shared responsibility among the sector——

Chairman JOHNSON. Yes, who makes the call?

Mr. AARONSON [continuing]. To be operating this—I do not know the answer to that question.

Chairman JOHNSON. I think that is what Mr. Koppel is talking about.

Let us see here. Senator Tester.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Thank you, Mr. Chairman. I want to thank you all for your testimony.

I want to talk about a little different kind of infrastructure since you are here, General Dunbar, and that is the infrastructure of our intercontinental ballistic missiles (ICBM) forces. It has been—well, currently we have Hueys that fly our personnel out for protection purposes. We are looking to get some Black Hawks in a couple of years, earlier if we can but in a couple of years at the latest.

There have been some that have suggested that maybe we ought to use the Army National Guard for defense of our ICBMs to make sure that they are secure. Fire season aside—if we use them for that, they will not be available for fire season. It seems like the fire seasons are becoming more and more significant every year in Montana. In fact, they are.

From your perspective, what kind of training needs to go in—or are they already trained—for National Guard soldiers to be able to protect our ICBMs?

General DUNBAR. Senator, thank you for that question, so let me start by, again, making clear for the record that I am here speaking on behalf of the State of Wisconsin as a National Guard officer, not for the United States Air Force. That is a very important Fed-

eral mission, and I would not propose that I speak in any way for the United States Air Force on that issue.

In terms of the National Guard, the National Guard's advantage to the country is it is a highly trained Army and Air Force to do certain missions for the Army and the Air Force, and from that comes a surge capacity for all kinds of missions.

So, in California and other States, National Guard members have been used to fight fires, both on the ground and in flying helicopters. I can talk in the State of Wisconsin that we have our Black Hawk pilots—not all of them but some of our crews—trained to fly Forest Fire Missions with Bambi Buckets to help put out those fires that you talk about.

In terms of moving personnel from Point A to Point B, it is pretty much square within a Black Hawk's mission that most crews have that capability in their wheelhouse.

In terms of whether it is a good idea, I know you know this, sir, but the National Guard is a State military force until we are mobilized for active duty. So, if the Air Force needed the Guard to do that mission, then they could ask for volunteers. If the Governor thought that it would interfere with the State's response to firefighters, the Governor could push back and say, "I am not going to authorize volunteers." And then, of course, the Federal Government could trump that, as it always can——

Senator TESTER. Bingo.

General DUNBAR [continuing]. And say we are going to be on active duty.

Senator TESTER. OK. I am just curious. I mean, we can solve this whole problem by getting the Black Hawks in quicker, but that is not within your purview.

I want to talk to Mr. Aaronson for a second about transmission and the threats—on the grid, I should say. And excuse me if it has been asked already, but is that threat mainly in transmission or in generation?

Mr. AARONSON. So, I guess I would answer it this way: The threat is mostly in transmission. Generation, there are so many generation assets lending electrons to the grid. Those are assets we want to protect, but transmission is really where it is at.

Senator TESTER. And, so, is this due to our reliance—because I know nothing about, quite frankly, how this whole system works, so we are starting at zero. But is this due to our transmission reliance on the Web, or why should we be concerned about this from a terrorist standpoint? Or are we talking about bombs blowing stuff up?

Mr. AARONSON. So, a lot of answers to that question. First of all, you are not alone, Senator, in not knowing a lot about how the electric grid works. Most people just figure you turn on the light switch and the lights turn on.

Senator TESTER. As long as they turn on, it is good.

Mr. AARONSON. And that is our goal, too. We do not want you to have to think about all of the things that are happening behind it.

Senator TESTER. Yes.

Mr. AARONSON. There are a lot of threats to the grid, and we like to say from squirrels to nation-states. And, frankly, there have been more blackouts as a result of squirrels than nation-states.

Senator TESTER. Right.

Mr. AARONSON. The various threats—the reason the transmission matters, think of transmission as the——

Senator TESTER. I know why it matters, truly, because my lights do not come on without transmission.

Mr. AARONSON. That is right.

Senator TESTER. If we do not connect it all up. The question is: Why is transmission a target? Is it because of the Internet? Or is it because of something else?

Mr. AARONSON. It is because it is a soft target by definition. There are 45,000 substations in the United States. There are long lead lines everywhere.

Senator TESTER. You are right. And, by the way, those substations have been around a long time.

Mr. AARONSON. They sure have.

Senator TESTER. When we were in conflicts in World War II, there were substations. In conflicts in Vietnam, there were substations. Conflict in the first Gulf War, there were substations. Why now? What is different than Vietnam? Why should we be concerned now when we never heard anything about it in the late 1960s?

Mr. AARONSON. The threats continue to evolve. You can look at geopolitical situations. You can look at the fact that we used to be——

Senator TESTER. OK, so the threat level is greater.

Mr. AARONSON [continuing]. Superpower, the line that we were a nation with friends north and south and bordered by oceans.

Senator TESTER. OK. So the threats have raised, is what you are saying.

Mr. AARONSON. That is correct.

Senator TESTER. The threats of people wanting to do damage to the homeland have raised, and they were not necessarily—Ted, do you agree with that?

Mr. KOPPEL. No, Senator, I do not. What has changed is that the electric power industry has become deregulated. We now have 3,200 companies. I am as much of a novice at this as you, so I have reduced it to a very simple analogy.

Senator TESTER. That is what we like.

Mr. KOPPEL. I want you to imagine a balloon that has 3,200 valves, and half of those valves are letting air into the balloon, and the other half are letting air out of the balloon. As long as you maintain a perfect equilibrium between the amount of air coming in and the amount of air going out, your balloon stays inflated. Too much air in, the balloon blows up. Too much air out, the balloon collapses.

The electric power industry is made up of 3,200 companies. You have to maintain a perfect balance between the amount of electricity that is generated and the amount of electricity that is used. Too much electricity in, you have a problem. Too much electricity out, you have a problem.

Only the Internet has the capability of maintaining that exquisite balance. There was no Internet back in the days of Vietnam. There was no Internet back in the days of World War II. You were dealing with a totally different kind of electric power industry.

Senator TESTER. And I appreciate that answer because that is what I had surmised. And I will tell you that the technology has done a lot of really good stuff for efficiencies and predictability and dependability. I come from agriculture, and, interestingly enough, I had a guy get on my combine—I actually still drive my combine. I do not have a GPS unit on it. And I had a guy get on my combine last year, and he said, "How do you know where to cut? Because you do not have a GPS unit that is telling you where to harvest."

The point here is this: If we want to talk about preemption, I think that you have to run back and try to figure out how you can still manually control this stuff. And if it is impossible—as you may be correct, Ted, the Internet is the only way to control it—then we have to figure out different ways to do this.

I will tell you that the comments about tens of millions of refugees, which is probably true, I mean, we have to work on preemption, because I do not see how we ever deal with a situation like that. It amazes me, flying into this city, how we feed people in this country, much less how we would feed them under a catastrophic situation.

Go ahead.

Mr. AARONSON. If I might, I would like to add a little bit of context to what Mr. Koppel said because he raises an important point about the fact that it is 3,200 entities, 1,900 that make up the bulk electric system.

First of all, it is not controlled by the Internet. We are talking about operational technologies, supervisory control. These are not Internet facing. So, yes, it is through that digital overlay is exceedingly helpful in providing these efficiencies, but it is not uniquely capable of keeping the grid operational.

Think back to just 20 years ago. We operated the grid for the better part of a century without digital overlay. There is the capacity to keep electrons flowing regardless of having supervisory control.

Senator TESTER. You are correct, and the only thing I am saying is if the threat has emerged because of the Internet, we need to go back to that system as a fail-safe.

Mr. AARONSON. And we are.

Senator TESTER. OK.

Mr. AARONSON. People have looked at what happened in Ukraine at the end of last year as this eye-opening experience for the electric sector. It was not eye-opening. It was something that we were aware could happen and have been preparing accordingly.

Senator TESTER. Thank you, Mr. Chairman.

Chairman JOHNSON. And I want to point out it was highly sophisticated, so the use of the Internet, those operators thought the systems were working properly when they were not. And I think the greatest threat is taking that a step further and having the destruction of those large power transformers that we cannot replace, that takes something from a 6-hour shutdown to days and weeks and months. And that is what I continue to be concerned about. My

primary concern is the destruction in some way, shape, or form from various threats of these large power transformers.

Again, I think that you are minimizing what that is. I think that you are just trying to be a little too soothing in this process.

Next, Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you, Chairman, and thank you and Senator Carper for holding the hearing. It is an incredibly important issue.

I want to talk about something that is specific to a threat to our infrastructure, and that is the increasing evidence out there that we have ransomware that has infected not just individuals' computers but commercial systems. I recently had the opportunity to get a briefing from the FBI on this, and I noticed that they sent out something on their website just a couple weeks ago warning people. There is a unique, I suppose, warning out from the Canadian Government and our government right now on ransomware based on some information.

To me, this seems to be a growing problem, and yet it is underreported because my understanding is a lot of companies are not eager to talk about their ransomware payments. For those who do not follow this, this is when you have an infection in your system, and you find your system has been encrypted to the point that it is blocked, and you get a notice saying, "If you pay this amount of money during this time period"—and sometimes there is a clock that shows you apparently what your time period is—"we will pull the malware off, and you will be able to operate your system."

There have been some unfortunate instances of this that have gotten a lot of attention. One was the Hollywood Presbyterian Medical Center in L.A. earlier this year. For weeks, they had to shuttle their patients to other facilities because they were locked down with a malware problem.

I guess my question probably is best to you, Mr. Farmer, because you are here as Chair of the Partnership for Critical Infrastructure Security. I am sure you have seen this report. The Institute for Critical Infrastructure Technology (ICIT),[1] issued this report, and its headline is kind of jarring. It says, "2016 will be the year ransomware holds America hostage." Maybe the title of your next book, Ted.

So, Mr. Farmer, could you tell us—and I know this data is difficult to come by because, again, it is not always reported. But based on what the FBI has said and based on this report and based on some of these specific instances that have come to the media's attention, what is the nature of the problem? Is it, in fact, increasing dramatically, as some say? And what are some of the ways in which we as legislators could be more effective in dealing with it?

Mr. FARMER. Thank you, sir, for that question. I do think the problem is expanding, and the FBI's attention to it and DHS's attention to it is reflective of that. The media coverage highlights those cases where ransomware has not only had an effect but actu-

[1] The report submitted by Senator Portman appears in the Appendix on page 75.

ally worked. And I think like anything else, so long as the tactic is working, the interest in pursuing it is going to expand.

There are two avenues to focus on in terms of whether incidents get reported. Often an affected organization will report a matter to the FBI as a law enforcement concern. The FBI will handle that matter through its investigative procedures with the affected entity. Whether it gets shared more broadly is a determination that entity might make with its sector partners, with DHS. But I think there is a lot of reporting which is informing the FBI's efforts and providing these awareness bulletins in terms of entities affected by this trying to deal with the problem and seeking law enforcement assistance. So, I think on that side, you have a lot of good reporting, and because of the manner in which the FBI handles its investigations, that is generally with the affected entity.

Now, because of the FBI's experience—and I give the FBI a lot of credit here—they have done a great deal of work in taking what they are learning from these law enforcement investigations, stripping out the indicators of the affected organizations, and then publishing for wider dissemination guidelines and advisories, in particular, papers that focus on indicators.

One of the things we focus on in the Cross-Sector Council is we are not necessarily interested in who the perpetrators are. That is investigative information that is not necessarily important to us. What is important is the tactics. How is it that these events are taking place? And, in particular, how does the intrusion occur onto the affected networks?

The focus of our cybersecurity priorities collectively is on that aspect. What can we learn from all that work the FBI does in its investigative efforts? As I mentioned earlier, from all that assistance DHS provides in terms of onsite work with affected organizations and sharing indicators, let us take that next analytical step and understand better how these events happen.

So, what makes it to the media is the effect: the computers are no longer accessible, the hospital cannot get to the records. So, the effect makes it. But what is far more important from a cybersecurity perspective is how did that happen. And, I think as Mr. Koppel can point out just from the work that he did in connection with this book, too often the means of intrusion are perilously simple, and there is a lot of work that we can do based on that next level of analysis, understanding what those tactics are that are used most often, understanding what vulnerabilities are most often exploited. That can be passed in advance, understanding what protective measures when that support is extended were found lacking.

I will give a comparative example. In Australia, their equivalent of the United States' Computer Emergency Readiness Team did an analysis of times when the Australian Government—I think it is the Signals Directorate in Australia—had to provide assistance to private entities in Australia affected by cyber attacks, and that analysis found that in 85 percent of those cases, if four categories of protective measures had been taken, those attacks never would have materialized as they did.

And, so, we look at that from the U.S. perspective. We credit DHS and FBI for that expansive work, and we say let us take that

next step of analysis and build a very good cyber threat profile that we can pair with the Cybersecurity Framework issued by the National Institute of Standards and Technology (NIST), and sectors can then look at that and say for organizations of varying sizes, this is what the threat looks like; these are what the vulnerabilities are that are most often exploited; these are the protective measures you really need to pay attention to; and marry those with objectives of the framework.

Senator PORTMAN. Mr. Farmer, I would say, with all due respect to that analysis that has been done and the information that is out there, I am looking at a bulletin right now that is on the FBI website. It is tips for dealing with ransomware threat, and yet it is dramatically increasing, as I understand it and as this report says, and I think you confirm that.

Mr. FARMER. Right.

Senator PORTMAN. So, despite our ability to understand how these ransomware attacks are happening and this information that is out there, it is expanding. And I think one reason it is, from what I understand, is that sometimes the ransomware folks are asking for a relatively small amount of money, small enough that, frankly, they are not being investigated, so let us say $10,000. I am told that is kind of the sweet spot. My view would be we need to up the enforcement of that and investigate all of them because it is sort of the broken windows analogy on the policing side.

Mr. FARMER. Yes.

Senator PORTMAN. You cannot let some of this ransomware happen. And then, second, how do you encourage people to report? As you are saying, some do report it as a law enforcement matter. Some do not, particularly if it is at this relatively low level.

And then the final thing is—and this is where I think Ted Koppel has done a great service—talking about what restrictions are there that we could help with both at the regulatory level and at the legislative level to allow people to protect themselves better. The great example that I have in some research that my team did was hospitals that are told under the Health Insurance Portability and Accountability Act (HIPAA) rules, they have trouble defending themselves following these very tips that are being laid out. And, I think you wrote something about actually an Ohio incident where there was a brownout in Ohio, and some regulatory issues affected the way people were able to defend themselves.

Is that accurate or am I missing——

Mr. FARMER. I think you are accurate, sir, in terms of the nature of the threat. You are accurate as well in terms of the expansion. I do believe a similar widespread publication of investigative actions and successful prosecutions that result in serious penalties for this behavior would be helpful as a deterrent factor.

I will say this, though: I do not agree, though, that——

Senator PORTMAN. So going after people more aggressively who are participating in this and increasing the fines or the criminal penalties.

Mr. FARMER. Increasing the criminal penalties, but also taking that Step 2 of ensuring that those sorts of penalties are well known. Again, often the focus of attention is on what happened in the particular event and what the impacts were. We do not pay

enough attention afterward to how that was resolved in terms of someone was prosecuted, someone went to jail because of the actions they took.

And there is one area, sir, where I do want to make a point. I do not think we have done so well yet at highlighting for organizations across the board, particularly those smaller in size that do not have a lot of resources. Hospitals become a good target because they have limited means to protect themselves. I think we really need to focus on understanding better through analysis what the intrusion mechanisms are that enable the ransomware attack to happen and help organizations understand what they can be doing better in terms of narrowing—the term that gets used—the "attack surface," narrowing that opportunity.

So, I think it is a two-pronged approach. We do a really good job of highlighting ransomware as a problem. We do not do nearly as well a job of saying this is how ransomware intrusions based on analysis are happening, and here are some things you can do to narrow the risk profile of your organization.

Senator PORTMAN. Let us follow up on that. My time has expired. Again, thank you all for being here. And I think you are right. It was hospitals maybe among institutions that were most vulnerable initially and smaller hospitals that did not have a more sophisticated system. My understanding is it is now moving to larger hospitals and other entities that have even a bigger impact on our critical infrastructure.

Thank you, Mr. Chairman, and maybe we will follow up, Mr. Farmer, if that is OK, with some follow up questions.

Mr. FARMER. Yes, sir.

Senator PORTMAN. Thank you.

Chairman JOHNSON. Senator Ayotte.

OPENING STATEMENT OF SENATOR AYOTTE

Senator AYOTTE. Thank you, Chairman.

I would like to ask you, Mr. Koppel, based on the book that you wrote, "Lights Out," what are the top three takeaways you want us to have today in terms of the action that we could take as a priority?

Mr. KOPPEL. Thank you, Senator.

Thank you for the question, Senator. I think you are exactly right. We are focusing a little bit on the wrong issues, and I think the key issue we need to focus on is even some of the most potentially successful measures that the industry is taking to defend itself, I think Mr. Aaronson will concede, are still some time off in terms of their real effectiveness. The CRISP program that he referred to before, when Mr. Aaronson and I spoke about a year ago, I believe he told me that the goal was that by the end of 2015, something like 0.4 percent of the industry would be covered, and I would like to give him an immediate opportunity to respond. Maybe you are way ahead of that by now.

Mr. AARONSON. It is 0.4 percent of the number of electric utilities covering approximately 75 percent of all customers.

Mr. KOPPEL. OK. But it is still a minuscule percentage.

Mr. AARONSON. It is the right ones.

Mr. KOPPEL. OK, except that the right ones and the wrong ones are all connected.

Mr. AARONSON. So to that point—and it is an important one—socializing the information, CRISP is wonderful for the companies that deploy it because they get near-real-time feedback about the impacts on their system. Shortly after, that information goes to classified databases, is compared to those databases, and then is actually socialized through our Electric Information Sharing and Analysis Center (EISAC), to all of those 3,200 entities that you reference. So the few who are deploying this technology are helping the whole.

Mr. KOPPEL. Except that the deployment of that information in the age of the Internet, where we are talking about fractions of a second——

Senator AYOTTE. With very quick development of new technology.

Mr. KOPPEL. With very quick development, exactly—is somewhat less than useful.

My point is I think we may be focusing on the wrong area at this moment. I think we have to conclude, whether it is from EMP, whether it is from some space weather incident, or whether it is from a cyber attack, that the United States needs to begin preparing for the consequences of a successful cyber attack on the grid in particular, because the grid indeed just does have such an impact on so many other parts of the infrastructure.

We do not have enough food. We are focused primarily on MREs, which, because they only have a life span, a shelf span of 5 years, the government has not bought in sufficient quantity because it does not want to be sitting there with millions of MREs which are going to be no good after 5 years.

Even if we turn to freeze-dried food, which I think is going to be the long-range answer, and if we were to begin today to try to accumulate the necessary amounts of freeze-dried food, it would be 2 to 3 years, if we started right now, before we had an adequate supply.

We do not yet have adequate plans for evacuating, if that indeed is what has to happen—let us say a major city like New York is hit, and a large part of the East Coast is without electric power. And some people—and we are talking about tens or hundreds of thousands of people—decide to evacuate, where are they going to go? And I think it is a question that perhaps General Dunbar can address, the degree to which each State is prepared to accept large numbers of internal refugees. I think we need to begin making plans. I think we need to begin communicating State to State, Federal Government to State government, and vice versa.

I know of at least one State on the East Coast whose preparations are that they would activate the National Guard, they would have their sheriff's department, they would have the State police standing there with maps, a bottle of water, and a sandwich. And as refugees from nearby cities came through, they would give them the water, the food, and the map and show them where the nearest way out of town is.

Senator AYOTTE. Wow.

Mr. KOPPEL. We assume, because we are all Americans, that every State is going to welcome vast numbers of internal refugees.

I would suggest to this distinguished panel that that is not necessarily the case.

Senator AYOTTE. Thank you, Mr. Koppel.

Mr. Aaronson, I wanted to follow up. When I heard 0.4 percent of those that cover 75 percent of the infrastructure, I guess I have to agree with Mr. Koppel in terms of describing that as a very small, if not minuscule amount. But here is a question I have for you: What is your association's position on the installation of devices that would protect transformers that may be susceptible to damage from solar storms or EMP attacks?

Mr. AARONSON. So there is a lot of misinformation out there that there is a particular technology that would protect everything from everything. Early on, we were discussing EMP, and there are very different natures of an electromagnetic pulse. You have a high-altitude nuclear weapon as one source——

Senator AYOTTE. Well, let me ask you this: Are you opposing installing——

Mr. AARONSON. No, certainly not.

Senator AYOTTE [continuing]. Devices to protect transformers?

Mr. AARONSON. Certainly not. And, in fact, we are doing it, though, in a responsible way. Our real concern here is unintended consequences. The point——

Senator AYOTTE. What kind of unintended consequences?

Mr. AARONSON. Potential impact to the grid. When you put new widgets, whatever they may be—blockers, capacitors, resistors—on the grid, energy has to go someplace. And to Mr. Koppel's point, I will agree completely that it is a balanced system, and new stuff can throw that balance——

Senator AYOTTE. But here is our problem: So we are worried about new stuff, but we are facing a potential blackout situation that could cause mass chaos in our country. So as we look at the risks we are facing versus deploying new technology—and, obviously, there are always new undertakings with new technology—wouldn't you agree with me that this is a very important issue for industry to step up and address?

Mr. AARONSON. A hundred percent. And, in fact, we are. There is a lot of money right now behind the Electric Power Research Institute, which is looking at just this. What would the threat be from the various kinds of EMP, whether it is a direct energy weapon, a nuclear weapon, or a geomagnetic disturbance? And what are the appropriate mitigation strategies so that we do not have those unintended consequences?

We agree, this is one of the risks, and we need to mitigate against it. But we do not want the solution to be worse than the threat, especially——

Senator AYOTTE. I am not sure what could be worse than a blackout where we are handing people a sandwich and a bottle of water and giving them a map.

Mr. AARONSON. Well, let us be clear with especially—let me break down each of the threats. If you are looking at geomagnetic disturbance, this is something that already happens all of the time and that, in fact, we do have standards in place to deal with.

Chairman JOHNSON. Excuse me. Not at a massive level. Let us be clear. Not at a massive level like the Carrington Event.

Mr. AARONSON. The geomagnetic disturbance standard is ambivalent to whether it is a Carrington Event or just your typical solar max that we get every 11 years. It is operational procedures to protect the grid in the event of a coronal mass ejection.

If you then look at direct energy weapons, these are things that are mostly localized in impact, not all that different from throwing a Molotov cocktail or a bomb into a substation. It is bad, but with 45,000 substations, we have a significant amount of redundancy.

The last one, looking at a high-altitude nuclear weapon, this is absolutely something that could happen, but I would posit it is a high-impact but exceedingly low-probability event. This is not happening tomorrow. So let us do the right thing to ensure that as we work to mitigate against this and many other threats that we are doing so in a risk-based and responsible way.

Senator AYOTTE. With all respect, I think that government has a really important role when it comes to thinking about a nuclear attack. But let us just be clear. I serve on the Armed Services Committee, and we have Iran testing ballistic missiles right now. We have North Korea testing ballistic missiles. So we have a role in this. I get it, in terms of this. But what concerns me is that that is not the only source for potential EMP attack in terms of what could have an impact on this grid. And, so, what I would like to see is making sure that industry steps up.

My time is up, but I have a follow up question, so perhaps I will wait.

Chairman JOHNSON. Because I want a quick follow up. How do you explain that 8 years after the 2008 EMP Commission, the GAO reports to this Committee that we have done none of these—performed any of these recommendations? Is GAO just wrong or——

Mr. AARONSON. No, Chairman, I appreciate you actually running through the litany of the 2008 report, and I sort of took notes as you were doing it. My understanding is the GAO report was looking at some of the things that government may or may not have been doing over the course of the last 8 years.

I can say—and this goes to Senator Ayotte as well—with respect to understanding the threat and what it might do to the grid, understanding the mitigation and the appropriate way to protect should an event like that happen, the industry is well underway in not just investigating but in some cases investing in mitigation. As companies build new control centers, as companies are building new substations and new control housing, they are doing things to shield against EMP.

I note that we talked about restoration and replacement of equipment. The Spare Transformer Equipment Program started in 2006, but has evolved dramatically with an eye toward any number of existential threats, whether it is combined cyber physical attacks, really big storms, solar flares, or even EMP. Going down the line, looking at critical interdependencies, there is a lot of work happening in this space that mirrors the recommendations of the EMP Commission's report.

Chairman JOHNSON. OK. And, again, I will reiterate my request to get that information on those replacement transformers. Senator Heitkamp.

Senator HEITKAMP. Kelly can finish.

Senator AYOTTE. Thank you. I just have a follow up question. As I understand it, DOD has developed some technologies that the utilities could actually use hardware devices to protect electricity generators and pipeline compressor motors from certain cyber attacks. And I wanted to ask you, has the industry installed those hardware devices using some of the developments from the Department of Defense? And if not, why not?

Mr. AARONSON. So, I am not familiar with the specific devices that you are referring to, but I will say this: An enormous part of what the Sector Coordinating Council that I am privileged to serve as part of the secretariat for is looking at technology transfer from the government to the industry.

I will also say, as you pointed out in your question before that this is something that government can help with as well. The Department of Defense in particular has had to contemplate how they would prosecute a nuclear war and had some really interesting information about what the impact of a nuclear weapon might look like to the grid. The more we can do to get that information into the hands of the folks who are doing this successful to apply it to the grid would be invaluable.

Senator AYOTTE. So, I am going to submit for the record a follow up question because, as I understand, you have the information and you have the ability to do this, and so I will ask a very specific question and follow up for the record on this to get a more specific answer from you.

I would like to thank all of our witnesses for being here and the Chairman. Thank you, Senator Heitkamp. I really appreciate it.

Chairman JOHNSON. Thank you, Senator Ayotte. Senator Heitkamp.

OPENING STATEMENT OF SENATOR HEITKAMP

Senator HEITKAMP. Thank you, Mr. Chairman.

Mr. Aaronson, a miracle happens every day. We walk over to the light switch, and we turn it on, and lights come on. That is a pretty remarkable thing, and it has been a huge reason why this country has developed the way it has. So we all see huge consequences when we do not have access to power.

Also, we are talking a lot about high-tech threats and challenges. I would tell you that as a veteran of the utility industry, you should also worry about low-tech. my guys would tell you that a .22 in the right place could do almost as much damage as anything we are talking about today. And, so, with some knowledge, we know that a lot of our substations are not protected, they are not securitized. I would add that to the list of things that we ought to be thinking about as we look at protecting the grid.

Mr. AARONSON. If I can react to that—and, again, in my opening statement I remarked that we do have standards in place. Standards in and of themselves are not security. If you mandate a 10-foot fence around everything, the adversary brings a 12-foot ladder. So you want to make them bring that ladder, but you do not want to pretend that just because you have that, you are secure.

Another component to security is this idea of resilience and redundancy. As you know—and I have mentioned a few times and so has Mr. Koppel—45,000 substations. These are by definition soft

targets. They are in communities, they are in cities, they are in valleys, they are on mountains, they are in rural areas. So to try to protect everything from everything is a fool's errand.

What we need to do is continue to build that capacity to be responsive and redundant when things happen, and I will give you one quick example. You may be familiar with an attack that happened in Silicon Valley a couple of years back. One or more people, we still do not know, shot up a substation, rendering inoperable 17 of the 21 transformers there. It was a bad attack. But I will note that the lights did not even blink in San Francisco or Palo Alto. So it shows the enormous resilience of this grid.

Senator HEITKAMP. But a coordinated attack by somebody with a great deal of knowledge about how you create redundancy on the grid could create real problems——

Mr. AARONSON. We agree.

Senator HEITKAMP [continuing]. In a classic or traditional attack.

Mr. AARONSON. We agree completely, and your point about low-tech, Occam's razor, the simplest is the most likely. It is a lot easier for the hunter who had a bad day to go take potshots than it is for a well-coordinated, combined cyber physical attack. There is sort of an adversarial curve. I want to quote John Brennan, the Director of the CIA: "Those who can do this damage do not want to, and those who want to cannot."

Now, I will say that axiom is not static. There are certainly adversaries who are going to get more sophisticated.

Senator HEITKAMP. And we cannot afford the exception that proves the rule. That is the point.

Mr. AARONSON. And we have to stay more sophisticated. That is exactly right.

Senator HEITKAMP. I am concerned about what happens, Major Dunbar, in the event of a catastrophic power outage as it relates to first responders and the resiliency and redundancy for first responders to operate in a world where we do not have access to electricity. And I am wondering what planning you have done in the State of Wisconsin or other organizations—in North Dakota, we have an emergency management plan that is reviewed periodically with the National Guard. It has proven to be an invaluable resource when we look at the major floods where we did experience power outages or huge snowstorms with ice that takes down power lines.

What kind of system should we be looking at for first responders so that we can, in fact, keep the peace in the event of a catastrophic outage?

General DUNBAR. Thank you, Senator. In Wisconsin, like all States, we also have an emergency management plan that we update periodically. We have had experience with power outage, but not on the scale that we are talking about long-term and widespread. It is one thing if a small part of the community has power outage and the fire department and the police department have systems that they have right now to allow them to go into these areas and have generators and things like that and operate. The scale we are talking about, we do not have plans.

Senator HEITKAMP. Right.

General DUNBAR. We are trying to get our head around what that would look like, the very point that my colleagues on the panel are making in terms of how—it is one thing to have power outage for a couple of hours. I joke with my wife, if the power goes out for a couple of hours, it is almost romantic. You light a candle. It is not going to be romantic after a month. It is going to be a bad day, a bad week, a bad month in America. And then add to that if people start to leave their homes. A big concern of mine as Homeland Security Adviser in the State, if this happens in Milwaukee, our largest city in Wisconsin, or, God forbid, Chicago to our south and people start to leave their homes——

Senator HEITKAMP. I just think it is something that we need to have that communications network, we need to have the ability to continue to manage an emergency response network in the event of a catastrophic power outage, and, so prevention, hugely important, but also analyzing what we do with consequences.

Mr. Koppel, you mentioned food security. The World Food Program tests food all of the time. They have packets that they deliver or drop from the sky. They are just now transitioning to a high-protein, high-calorie product. Have you looked at all at what the World Food Program does to basically look at logistics in very difficult places and what they do with food security?

Mr. KOPPEL. No, ma'am, I have not. But I would point out to the Senator, we are not talking about delivery. I think if there is one thing that the United States absolutely surpasses any other country in the world at, it is delivery. I am talking about availability. In a State like New York, for example, you have 17 million people in the State. They have, let us say, 20 or 30 million MREs stored in New York State. Do the math. You are talking about 2 days' worth of food.

Senator HEITKAMP. You might be a little concerned about delivery if the power goes out and you cannot pump the gas.

Mr. KOPPEL. That is absolutely——

Senator HEITKAMP. I think you have to imagine, as Hollywood does all of the time, what an event like this looks like and what is the key components.

Mr. KOPPEL. You are absolutely right, Senator, and the other point I would make, which I was discussing with General Dunbar before this session, is that we have a diminished number of military in uniform. And the fact of the matter is if and when an event like this occurs, ultimately every State and the Federal Government is going to be dependent upon the Northern Command (NORTHCOM). We do not have enough troops to do what would be necessary in this kind of an event.

And if I may, your colleague Senator Ayotte asked if there is anything we are leaving out. I do not want this to be left out. The question of attribution, any other kind of attack that is launched against the United States, it is easy for our intelligence branches to discover instantaneously who did it, where the attack is coming from. In the event of a cyber attack, attribution becomes one of the biggest problems. You cannot respond if you do not know who did it. And it might take months before we actually determine, with any sense of certainty that would permit the President to respond,

who did it. That is a huge issue and one that needs to be examined more closely.

Senator HEITKAMP. Well, I think this is a great opportunity for us to have this conversation, to think about preparation, because 90 percent of making this work is actually being prepared and being able to imagine the what-ifs. And the what-ifs are not related always just to high-falutin' security attacks. There are some amazing things that can happen just conventionally with some very determined and bad people.

And so, General, thank you so much for your service. We need to continue to recruit into our National Guard. That is a challenge, I think, for all of the National Guard today. And talking about these issues publicly in terms of what importance it is for people to serve in uniform, especially in the National Guard.

Mr. Koppel, your book is a perfect example and a great recruiting tool to tell people what, in fact, the value of that service is. So thank you so much.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Heitkamp.

I just want to underscore what you said, Mr. Koppel, about availability. I come from a manufacturing background. I am not exactly sure when the concept was developed, but it has been decades: "Just in time." That is how we run our economy, just in time, so we do not have the availability. Senator Carper.

Senator CARPER. Thank you. Thank you, Mr. Chairman.

Mr. Koppel, you mentioned the number of people we have in uniform. I wore a uniform for about 5 years active, another 18 reserve, and so I am mindful of what you are saying. I also was commander in chief for 8 years with the Delaware National Guard as Governor of Delaware.

My last State of the State address that I gave came off pretty well and finished up, and we were having a reception later in Legislative Hall, and a woman came up to me, and she said, "Were you the Governor when we had the blizzard of the century?" And I said, "Yes, ma'am."

She said, "Were you the Governor when we had the ice storm of the century?" I said, "Yes, ma'am."

"Were you the Governor when we had the drought of the century?" I said, "Yes, ma'am."

And she said, "Were you the Governor when we had the flood of the century?" I said, "Yes, ma'am."

She said, "You know what I think?" I said, "No, ma'am." She said, "I think you are bad luck." [Laughter.]

Well, fortunately, the good luck was we had a great National Guard, and Frank Vavala, whom I know the general here knows well, is our adjutant general, and whenever there is a blizzard or an ice storm or a flood—they do not do so much on droughts, but we have Nor'easters, we have hurricanes on the East Coast, and the National Guard is always there. Air Guard, Army Guard, and we are grateful for all that they do.

Senator Heitkamp just said in her comments, I think she mentioned that when you go to pump gas in some kind of emergency, if you do not have electricity, you cannot pump gas, and what that sort of leads to. And what it leads me to is to say, a lot of busi-

nesses and a number of homes have diesel-powered generators that are there to provide electricity, maybe for a home or for a compound or for a business. They work. They also pollute a lot, and at a time when we are trying to reduce carbon emissions, they actually do not help out on that front.

I mentioned in my opening statement that there are some, I guess, 21st Century tools or methods to meet those needs that are now met by diesel generators across the country. And one of them was actually created at the old Moffett Field Naval Air Station where Navy P–3 squadrons were on the West Coast, and with a joint facility with NASA. And I am going to ask you for ideas on other similar technologies that you may be aware of that can help us when the electricity goes out and businesses need to be run and gas needs to be pumped. It could be a data center or a telecommunications company, it could be banking, it could be retail, it could be logistics—any number of things that depend on electricity. And when the power goes out, they are not able in many cases to deliver, to do their job, and the rest of us are in a bind.

The technology that came out of the efforts at the old NASA base near Mountain View, California, a company called Bloom Energy, and they used fuel cells and hydrogen in order to create electricity for some fairly small boxes—they call them "Bloom boxes." They are actually rather large ones that can meet greater needs. And they are installed across the country. Actually, the Department of the Navy uses them to some extent. I think other units of our military are interested in exploring those capabilities.

I think a couple of States—we manufacture some of those Bloom boxes in Delaware. I think both New Hampshire and Ohio not only use fuel cells like these, but they also contribute heavily to manufacturing fuel cells.

My question for our witnesses is: How can we change our policies and practices to further rely on innovative solutions like fuel cells to increase the security and resilience of our critical infrastructure? This is one thing that is being done. Go ahead, please, Mr. Koppel.

Mr. KOPPEL. If I may, Senator, two points.

One, I have a generator at home that runs on natural gas. The problem is the natural gas has to get pumped to my home, and the pump operates on the basis of electricity. So if we have a massive grid failure, I guess that natural gas is not going to make it to my house either.

The other point is I interviewed a retired lieutenant general from the Air Force who indeed is engaged in exactly the kind of work you are talking about. He and his partners have noted that the nuclear generators that fuel a number of our Navy ships have now had 50 years of successful operation without a single accident. The theory is if we could create a number of these nuclear power generators and put them on military bases around the country, they could not only serve those military bases, but they would be additional power to run critical infrastructure in neighboring communities.

I asked the general, if the President gave him the go-ahead tomorrow to develop that capability, how long would it take? His answer: Ten years.

Senator CARPER. Both my boys are Boy Scouts. I used to take our Scout troop, Troop 67 from Wilmington, Delaware, to the Norfolk Naval Station, every year for maybe 3 or 4 years, and spend the weekend, sleep in the barracks, eat in the galley, climb all over ships, submarines, and aircraft carriers. One Sunday we went to the Teddy Roosevelt, we got a tour of the Teddy Roosevelt. And we had about 25, 30 Scouts, maybe half a dozen adult supervisors. Anyway, we get to the bridge of the ship, and we were met by the commanding officer of the ship, a captain, a Navy captain. And he said to our group, he said, "Boys, when the Teddy Roosevelt goes to sea, it is 1,000 feet long." And the boys went, "Ooh." And he said, "Boys, when the Teddy Roosevelt goes to sea, it has 5,000 sailors on board." And the boys went, "Ooh." And he said, "Boys, when the Teddy Roosevelt goes to sea, it has 75 aircraft on board." And the boys went, "Ooh. And then he said, "Boys, when the Teddy Roosevelt goes to sea, it refuels once every 25 years." And the adults went, "Ooh."

The hearing we just had, the markup we just had that I was late for—I am the senior Democrat on the Subcommittee called "Nuclear Safety." We actually focused on just this thing, new generation, nuclear power, small modular. And, actually, with the technology, you can use spent fuel rods from other nuclear power plants and derive electricity from them. So there is some really exciting stuff going on. Maybe a lot smaller, easier to build, maintain, and so forth. And redundant with more resiliency, so thank you for that idea.

Any other ideas, please?

Mr. AARONSON. Yes, Senator Carper, I appreciate some of the things that Mr. Koppel said. I want to underscore one. He talked about how his generator relies on natural gas but the natural gas relies on electricity. I would go even further back. The electricity relies on natural gas. So there are profound interdependencies throughout, and I think that is something that this sector, which has always been held up as the most critical, really gets just as a matter of course and is working across those critically interdependent sectors.

With respect to technology as a solution to this, I would say, yes, technology, things like the Bloom boxes and other distributive resources, come with some added resilience and redundancy. It is a double-edged sword. They also come with, the phrase that has been used, "an added attack service."

I am from New Jersey originally, and if you look at what happened during Superstorm Sandy, several hundred circuits were destroyed and had to be fixed, and it took between 10 days and 2 weeks to get the power back on. Had there been distributive resources, maybe 30 million from all over the Greater New York Metropolitan Area, we would probably still be restoring. So I do not want to pretend that those devices in and of themselves equal security or redundancy. They are a component. They are a tool in the toolbox.

The last thing I would say is with respect to military installations and that sort of a partnership, yes, in fact, siting generation on military installations for their use and then for the community's use in the event of an incident is something that is happening and

certainly could be happening more. So I think there are a lot of interesting ways—I want to be very careful to say we are open to anything. I think anything that enhances the resilience and redundancy of the service we provide is something we all ought to be exploring, and it is the value of the Sector Coordinating Council and the CEO and senior government leadership which are setting that strategic course. As opposed to finding these little tactical things that we can be doing, let us learn from some of those experiences like Ukraine, like Metcalf, like Hurricanes Sandy and Katrina, like the wildfires in California, and like our experience putting things on military installations, and let us build on those and figure out—let us have an automated response to some of these incidents, and let us have a capacity to go back to the 1960s and be able to support civilization without automation.

Senator CARPER. All right. Thank you. My time has expired, but, Mr. Koppel, go ahead.

Mr. KOPPEL. If I could just add one footnote to what Mr. Aaronson just said, prior to the deregulation of the power industry, military bases in this country generated their own power. And the Pentagon came under great pressure from this particular geographic location on Capitol Hill to save money by using private industry to generate the power on the bases. So to a certain extent, we are talking about going back to the future.

Senator CARPER. All right. Good.

A quick side note, Mr. Chairman. Hurricane Sandy was about 3 or 4 years ago, but actually there were Bloom boxes that were deployed previously before Hurricane Sandy hit, and they were actually used, I think, to good effect. So that is, I think some encouraging news. Thank you so much for being here. It is a great hearing. Thank you so much. Good to see you all.

Chairman JOHNSON. Thank you, Senator Carper.

What I am going to do is kind of go down the line there and give everybody a chance to make a final comment. But I do want to quickly explore what I am assuming is the major, the primary weak link, and I think it really is transmission. First of all, is that correct? Yes, you can shut down a power station, but there will be other power stations that might survive. But let us say you do these things on military bases, and you can maybe distribute within the military base, but then going further and further out. Transmission is really sort of the weak link here, isn't it?

Mr. AARONSON. I mean, I will quibble with the word. I would not call it a "weak link." It is actually exceedingly secure because it is so redundant, but it is, I think, the primary focus of our attention for security.

Chairman JOHNSON. But, again, depending on maybe a very low probability of an EMP or a massive GMD, the weak link in that transmission system are these large power transformers, correct?

Mr. AARONSON. They are the lifeblood of the transmission system.

Chairman JOHNSON. OK. What determines the 200 to 700 critical transformers? Is that size? Is it location? Why are they critical, versus the tens of thousands of other ones that Mr. Koppel was talking about?

Mr. AARONSON. So, yes, it is size. It is what they serve. There is any number of criteria that each individual company would know as to why a particular transformer is critical, and I will just tell a quick anecdote. There is a company that had identified several of their transformers to be critical and disclosed them as so. And then that list changed, and somebody asked why. And the answer was they built another substation.

So there are certain substations that are taking electricity in very critical areas and transmitting it, and so as a result, those are your priority transformers. And let us put it this way: If you have 45,000 priorities, you have none. So we really do have to hone in on those that are the most critical to the system.

Chairman JOHNSON. So would you agree with me that—my concern has always been these large power transformers—those are the things we must protect, we must have redundancy for? There are other concerns, but that is coming from a manufacturing background, what is the root cause? Is that sort of the most critical thing that we should be turning our attention to, the protection of those?

Mr. AARONSON. There are a lot of critical things that we need to be doing, but I think I do agree with your statement, and the industry agrees with your statement, which is why we have developed so much excess capacity, and, again, working with folks like Mr. Farmer and the railroads, the ability to move these things around. I have heard too often this notion of if there was something really bad that happens, we would "reengineer the system." That is a hard thing for a non-engineer to fully appreciate.

What we have been doing recently is to explore what does "reengineer the system" mean and plan for that so we can do it more effectively and efficiently if and when something does happen.

Chairman JOHNSON. OK. Let me start with you, General Dunbar. Closing comments?

General DUNBAR. Well, Senator, thank you for the opportunity to be with you. I would foot-stomp I think four things at the end here.

One, just to reiterate the importance in my mind of trying to do what is possible from my level to State level. A lot of things we are talking about are beyond my level. If something happens long term, it is my intent to try and keep citizens in their homes, and that means making sure we have water and sewage systems so that they are not desiring to leave the city. A big problem if that happens.

If there is a long-term power outage, the industry talks about things like islanding and micro-gridding. I think there is great value in trying to think through how we do that as a country if we had to do that after an event.

The third thing I would mention—and, again, I am not an expert, but it is my understanding that our black start capability used to be largely based on coal. We are moving as a country away from coal for the reasons that we are doing it—I am not making a political statement, but from a public safety point of view, if we have issue with generating and transmitting natural gas and coal will allow a better black start, we ought to reserve some of that black start capability from a public safety point of view.

And the last thing I will mention is the information-sharing piece. The Federal Government is doing a lot of great work with utilities and with industry. Often the States are not part of that information sharing. I think we have a role to play, and we should be part of that information sharing.

Thank you.

Chairman JOHNSON. Thank you, General. Mr. Farmer.

Mr. FARMER. Thank you, sir, very much for the opportunity. Thank you, Senator Carper, as well.

I will open by referencing a point you asked about technology development, and really the key to advancing technological solutions is a combination of innovation and investment.

And to the point about coordination, what the Partnership for Critical Infrastructure Cross-Sector Council, and you can hear the term "council" and "coordinating committee" and think you have just seen another range of inside-the-Beltway groups. But they are not. In particular, this Cross-Sector Council that I am privileged to represent dates back 16 years now. That is a commitment by industry to working in concert, across sectors and with government, on matters relating to critical infrastructure protection. And there is a laboratory of ideas there. It is an ability to bring all that talent, that expertise together, in industry and government, to look at the sorts of problems we talked about today.

In some cases, we can look to near-term solutions that can help ameliorate some of the concerns, and then look through a technological development program to those longer-term innovative investments. DHS is starting this year and coordinated with our council in its development of a Resilience Challenge Program. The purpose of that is to do exactly what Senator Carper alluded to: Let us inspire some innovative ideas on how we can address some of these challenges.

And, again, we are looking at a two-phased approach. In some cases there are things we can do to mitigate problems now, and some are going to take a long time. But just because it takes a long time does not mean we should not be innovating and investing in that direction. Quite the contrary. If it is going to take a long time, let us get moving on it and let us use initiatives like a resilience challenge or some other similar investment program where we can combine public and private funds to advance these efforts.

As I said, this council has been in effect for 16 years. It is a tremendous forum to create a foundation for the sort of cooperation between industry and government that can make progress in these important areas. Think about this term "public-private partnership." This is a new way of government and industry working together, sharing experiences, expertise, information, ideas on a common goal. What can we do together to take the sorts of actions, near term and long term, to enhance how well our infrastructure is protected and how well it can withstand various types of threats. And we are taking innovations in this process that would have been inconceivable just a few years ago.

The day of the Paris attacks, we ratified an information-sharing approach that we had exercised just a few days earlier, that we had to put into effect within a matter of hours. We have built on that since then. And to the general's point about integrating State

and local government, we said to DHS there are going to be occasions when, whether it is a cyber threat or a physical threat or some broader concern—an electromagnetic pulse is one example—where you are going to want to share very quickly classified information, and you cannot wait days or weeks to get people in Washington, D.C., to do that. You have this tremendous infrastructure in the fusion centers that allows us to get on a secure video teleconference. Why aren't we using it to good effect to ensure that what formerly might have taken days or weeks can now be accomplished in a matter of hours?

On April 26 of this year, we exercised that capability. The participants did not have notice of precisely when this event was going to occur. They received an emergency notification that morning. It simply said, "Go to the fusion center where your clearance has been validated for a classified presentation by DHS." And we exercised it in six cities simultaneously, and it worked. We are going to exercise it again before our councils come together—Federal Government, industry, State and local—for a meeting in early July.

The point is the coordination that this process allows creates opportunities for a kind of interaction between government and industry that simply has not happened at this level before. And that is the strength of the perspective that I think this cross-sector route brings.

Some of these challenges are very daunting. Some of them are so daunting that inertia can set in and you kind of throw up your hands and say, "What to do about it?" But that is precisely what this group is designed to avoid. It is designed to bring together the right subject matter expertise, and through representatives like Scott and me to reach back for more. So I thank you for chance to talk about what we do.

Chairman JOHNSON. I appreciate that. You can have the most wonderful processes, but one of the things I have noticed about Washington, D.C., there is an affliction that affects this place, and it is called the "denial of reality." And in many respects, I think a lot of the discussion here is centered around the fact that we just deny this reality. The possibility of a low-probability event could be just catastrophic.

Now, Mr. Koppel, I appreciate the way you opened your book with a little scenario, that if people do not read the entire book, at least read that. OK? It will lay out what a potential reality would look like. If we lose power for more than 6 hours, it starts filtering into even days and then weeks and then months. So the first thing we have to do is recognize and admit this possibility, the reality, and start—because otherwise we will never take the first step in these processes, and it will take a very long time. Mr. Koppel.

Mr. KOPPEL. Thank you, Mr. Chairman, Mr. Ranking Member. I think the observation I want to make most of all is that the Chinese are already in our power grid; the Russians are already inside our power grid. They may lack the motivation because of the interrelationship that we have with both those governments to take action against our grid, but they can do it. We live in an age of cyber warfare. Cyber warfare is going on all of the time on every different stage of our lives.

The fact that the governments like North Korea, for example, which are desperately seeking the same kind of cyber sophistication that the Russians and the Chinese have, the fact that they do not yet have it should not be the source of any particular comfort to us. The fact that organizations like ISIS, which still probably have $1 to $2 billion in resources, have not yet used that money to buy the expertise to attempt perhaps a cruder kind of cyber attack on our power grid should not give us a great deal of confidence.

And I would like to add one other point that I suspect will be politically very controversial. I do not think the Department of Homeland Security is best equipped to deal with this issue. The National Security Agency is by far the most sophisticated body in the U.S. Government to deal with it, and I think leaving it up to a department that has one of the lowest rankings in Federal Government and allowing ourselves to be concerned more about privacy than about security clearly is the subject for a whole other hearing. But I did not want to let this one conclude without at least raising the issue.

Thank you, Mr. Chairman.

Chairman JOHNSON. I appreciate your comments, and, again, I appreciate your book. Mr. Aaronson.

Mr. AARONSON. Chairman Johnson, Senator Carper, it may surprise you to hear "thank you." I appreciate you all holding this hearing. And it also may surprise you that the industry agrees with a lot of what is being said. We do take this seriously. And we do understand the threats that exist out there.

I will tell you a quick anecdote. About 4 years ago now, several CEOs were in Colorado Springs for a board meeting, about 70 of them. We brought them over to NORTHCOM for a classified briefing, and the CEOs heard from the Intelligence Community, from the Department of Defense, from other agencies, some of the threats that were out there. And what came as a surprise, I think, to the government participants was the CEOs were not raising their hands saying, "Is there really a problem? We do not see this."

"Yes, there is a problem. What can we do about it?"

And from that one meeting has been born this incredibly effective relationship between CEOs and senior government officials. Now, I occasionally joke that CEOs do not do work. But they do provide accountability. They do provide a direction. They provide resources. And when the people in the corner office care about something, it is amazing how the rest of the enterprise does.

So what we are seeing is, up to and including the CEO level, security of the electric grid is a priority for this industry. In Mr. Koppel's book, there is a chapter titled "Guardians of the Grid." We are, and we take that very seriously.

The other thing I would leave you with is there are a lot of movie script scenarios out there that have been referred to. I had the opportunity to testify in a State capital and had to tell whether or not "Die Hard 4" was actually a plausible scenario. Let us not use movie scripts to dictate public policy. My problem is when I come into venues like this I am giving issues of popular mechanics and resilience and redundancy and all of the things that can and might happen, might not happen, and we are studying it. I get bored just

saying that. So I understand that we need to be informing public policy in a reasonable and rational way, understanding that these high-impact, low-probability events are something we absolutely have to put on the spectrum, but also understanding that there are a lot of things that happen day to day that require our attention as well. The Chinese, other sophisticated adversaries, that is where government and industry absolutely have to partner.

Now, I do not have an opinion on what Mr. Koppel said about whether or not DHS is the right place or the wrong place. We have had a wonderful experience working with the Department of Homeland Security and particularly NPPD. But I would suggest this is a whole-of-community issue. And by "whole of community," I do mean north-south, between the government and the industry, the industry and the government, and east-west across the critical sectors. And Tom talked about what we are doing with the railroads, but we are seeing very similar partnerships with communications, with financial services, with the water sector, with the gas sector.

So we are learning. We are looking at preparation. You build the roof when it is not raining, and that is what we are doing today. I think the industry has learned some great lessons from what has happened in Ukraine, from what has happened from the quite literally decades of natural disasters. And I want to leave you with the one parting thought that while there are 45,000 substations in the United States, it is the definition of a soft target. It is also exceedingly resilient and redundant. There is a lot of excess capacity, and we are working to grow that continually.

And then the last thing I would say is, as you all consider policies, let us not have a rush toward automation. Let us not have a rush toward the newest, shiniest object. Let us think about how policy decisions, just as we think about how investments decisions, will have an impact on the security, reliability, and resiliency of the grid.

So, again, I thank you for having me here today.

Chairman JOHNSON. I am the guy who is talking about manual breakers in Ukraine that kind of saved them. Senator Carper.

Senator CARPER. Thank you. I just want to come back to the question of the competency of the Department of Homeland Security. Mr. Koppel, I shared your views 4, 5, 6 years ago. The previous Chairs of this Committee—Susan Collins, Joe Lieberman, and me—and now Senator Johnson have worked long and hard to try to change that reality, and that was a reality half a dozen years ago, even 3 or 4 years ago. And I will not go through the entire list of things, but there was a time—we used to have the problem when I was Governor of Delaware—we hired people to work in information technology, hire them, train them, put them to work, and somebody would come along and hire them away. So we would hire some more. You guys know what I mean. We would hire some more people, train them, and they would go to work in IT, and somebody would hire them away.

As it turns out, the National Security Agency has the ability to hire people, pay them more money, retention bonuses and that sort of thing. The Department of Homeland Security never had that. So they would hire people, train them, and they would get hired away by NSA.

One of the things we have done is to make sure that Homeland Security has the ability to actually compete in a market that is really tough in terms of hiring—recruiting, hiring, and retaining cyber warriors.

I will not go through all of the other things that we have done, but we have worked long and hard for years, and I think—what is the old saying, the old tagline on Oldsmobile: "This is not your grandfather's Oldsmobile." This is not the Department of Homeland Security of even 4 or 5 years ago. And can they do better? Sure, they can do better. They can always do better.

The last thing I would say, the general here is wearing an Air Force uniform; I used to wear a Navy uniform. And there is a friendly inter-service rivalry, as you know, and I was with an Army guy the other day, and he was jagging me about being in the Navy. And I said, we wear different uniforms, but we are on the same team. We are on the same team. And the same is true with Homeland Security and NSA, and we need both of them to be really bringing their "A" game to the contest every day, because as you suggest, there is a real battle across the land.

The other thing I would say is I was in China about a month ago, and you may recall that President Xi, the Chinese President, was here last September. One of the things that our President confronted him about was cyber theft for stealing intellectual property for economic advantage. He basically said to him, "You have to stop this." The Chinese always say, "Oh, we do not do that." Well, they do. They have done it for years.

But you know what happened? The President said, our President said, in so many words, "You keep doing this, and the kind of sanctions we have imposed on Iran, we can do that with you. And we are your major trading partner."

So think about that. Since then, the incidence of cyber theft for intellectual property for economic advantage with respect to China has gone down. It is pretty interesting. A guy named Dave Dewalt who runs FireEye Mandiant, a big cybersecurity company, reported just last week or 2 weeks ago that we have seen a continued drop there.

The other thing, Iran for many years was going after our banks, trying to shut down our banks, going on their websites, started closing them down, and it is called "distributive denial of service." And one week after we entered into this joint agreement with Iran and five other nations, those attacks just stopped. They just stopped.

And so let us keep that in mind. There are things we can do and that we need to do to be resilient, but the Chairman and I believe—we are very much into root causes, and sometimes—now China has some intellectual property they want to protect, so they have a dog in the fight. And they also have the threat of if they keep up this stuff, they will pay the price for that.

The Iranians, they have been given a chance to be a good player. We will see how things continue if they keep their word. I think so far they have. And at least those attacks on our financial institutions have stopped.

Chairman JOHNSON. Thank you, Senator Carper.

Let me just close out the hearing reminding everybody that Dr. Richard Garwin—again, whom Enrico Fermi referred to as one of the few true geniuses he ever met—in testimony before this Committee reminded us of a solar event on the order of magnitude of the Carrington Effect happens once about every 100 years. In other words, we talk about low probability/high catastrophic, that is about a 10-percent chance every decade, every 10 years, of having a massive solar storm affect our electrical grid. So maybe not quite so low a probability.

Again, I want to thank all of the witnesses. I think this has been an extremely good hearing. It has certainly helped lay out a reality that hopefully we stop denying.

This hearing record will remain open for 15 days until June 2, 5 p.m., for the submission of statements and questions for the record. This hearing is adjourned.

[Whereupon, at 12:05 p.m., the Committee was adjourned.]

APPENDIX

Chairman Johnson Opening Statement
"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions"

Wednesday, May 18, 2016

As submitted for the record:

Good morning and welcome. Today's hearing seeks to identify key threats to critical infrastructure, available mitigation plans, and opportunities for the federal government to better assist stakeholders as they work to protect America's infrastructure.

Our nation's critical infrastructure sectors are not only lifelines in the integrated system, they are also crucial to our country's economic stability and national security. For these reasons, the safeguarding of critical infrastructure is a priority of this Committee.

During the past few years, the United States and countries around the world have experienced numerous attacks against vital infrastructure sectors. In April 2013, criminals shot at the Metcalf power substation outside of San Jose, California, putting 17 transformers out of service for 27 days and causing over $15 million in damage. This experience demonstrates that America's critical infrastructure is susceptible to criminal acts.

Additionally, since 2014, there have been more than a dozen instances of intentional cuts of fiber optic cables causing telephone and computer network disruptions in Northern California and several states on the east coast. These incidents represent a significant threat to the integrity of the system and to the efforts of first responders.

Although many of the previous attacks have been physical in nature, cyber-criminals are also employing highly-sophisticated tactics to infiltrate and manipulate control systems. In December 2015, a cyber-attack on the control system of a Ukrainian electric grid left over 230,000 consumers without power, in some cases for over six hours. The attack did not result in any physical damage to the grid, though it demonstrates how hackers could corrupt software-related assets.

In addition to man-made threats, there are natural hazards—earthquakes, hurricanes, tornados, and floods—that threaten critical infrastructure every day. According to experts, a major solar weather event causing widespread power outages is inevitable.

Protecting America's core infrastructure requires commitment and actions by all stakeholders. The government and the private sector play key roles, but neither can ensure critical infrastructure protection alone. The Department of Homeland Security (DHS) is the federal agency charged with working with state and local governments and private sector stakeholders to ensure all sectors have adequate information and protection. As we learn from the witnesses today, it is my hope that we will identify key areas in which DHS can better assist stakeholders in their work.

I want to thank our witnesses for joining us and I look forward to your testimony.

Statement of Ranking Member Tom Carper
"Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions"

Wednesday, May 18, 2016

As prepared for delivery:

Thank you, Mr. Chairman. Today, we are discussing a subject of immense importance to America – the security of our critical infrastructure. And when we talk about critical infrastructure, we're talking about the things we rely on every day: our supply of electricity, our drinking water, and even the financial system that supports our economy. Unfortunately, our electricity and water utilities, as well as our banks, are at risk every day in a number of ways. We've heard a lot lately about criminals and terrorists targeting them online, but these critical services are also at risk due to any number of other hazards such as violent storms, earthquakes, and even failure due to aging and under-investment.

Fortunately Congress, the Administration, and the private sector have been hard at work to address vulnerabilities in a number of these areas. We have passed several bills in recent years to help make our critical infrastructure more secure and resilient. In 2014, members of this committee worked for many months to enact legislation to reauthorize and enhance the Chemical Facilities Anti-Terrorism Standards (CFATS) program at the Department of Homeland Security. This program is our frontline defense against terrorist attacks against companies that store, manufacture, and process hazardous chemicals. Also in 2014, the President signed a bill to enhance the cybersecurity center at DHS that works with critical infrastructure owners to prevent and respond to cyber attacks. That same year we also gave DHS the authority to hire the best and brightest cyber talent. And just last year, the President signed the Cybersecurity Act of 2015, which our committee played a key role in drafting. This crucial new law makes collaboration between the federal government and companies grappling with cyber-attacks easier and faster.

This year, we are working hard to ensure proper implementation of these laws. We are also working to streamline and strengthen the office within DHS that helps protect critical infrastructure. That office is currently called the National Protection and Programs Directorate, or NPPD. This name is quite a mouthful and really doesn't tell the American people much about what the men and women who do there to better secure our critical infrastructure. As the Chairman knows, my staff and I have been working with DHS on legislation to streamline this office so that it can be a better partner with industry. We do this in part by elevating its cyber functions and making sure that physical and cyber threats to our critical infrastructure are assessed jointly, so the 'left hand' knows what the 'right hand' is doing.

We also want to rename the Directorate as the Agency for Cyber and Infrastructure Security. Doing so will make it clearer that, when there's a problem with a vulnerability in the electric grid or some other piece of critical infrastructure, there's no question about who in the federal government can help – and who can be held accountable when things go wrong and singled out for praise when things go right. And as we know, unfortunately, bad things oftentimes do happen. The important thing is to be prepared for when they do. So I credit the men and women of DHS, including in NPPD and elsewhere, for the hard work they do to ensure our critical

infrastructure is secure and resilient. As one example of this important work, DHS conducts on-site assessments and incident response for dozens of critical infrastructure companies every year.

When we talk about critical infrastructure – especially systems that we cannot afford to lose even for a few minutes – this means building resiliency into our policies and practices. Today's discussion about critical infrastructure reminds me of one very promising technology that is already helping to make our country more resilient to electric grid outages. A company called Bloom Energy manufactures fuel cells in Newark, Delaware. These stationary fuel cells do not require additional transmission capability to move electricity to the end user, meaning reliable electricity can be provided even when the electric grid goes down. Innovative solutions like these can help us be more prepared for a wide variety of threats.

With that, I would like to thank our witnesses for being here today and helping us learn more about critical infrastructure security. I look forward to learning more about what we can be doing better in this space.

Testimony to the Senate Homeland Security and Governmental Affairs Committee: Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions

Maj. Gen. Donald P. Dunbar, Adjutant General, State of Wisconsin
May 18, 2016

Good morning **Senator Johnson, Senator Carper,** and members of the Senate Committee on Homeland Security and Governmental Affairs, thank you for the opportunity to speak to you today. I am the Adjutant General for the State of Wisconsin and, although I appear before you today in uniform, I am speaking on behalf of the State of Wisconsin. I am not on active duty orders and no one in the Defense Department has seen, reviewed, or approved my remarks. As Wisconsin's Adjutant General, I command the nearly 10,000 Soldiers and Airmen who serve in Wisconsin's National Guard.

As you know, the National Guard has two primary roles - we are the primary combat reserve of the U.S. Army and U.S. Air Force and we are the first military responders in the homeland. I share this role with all Adjutants General across our nation.

In addition to my command role, I am responsible for Emergency Management, serve as Wisconsin's Homeland Security Advisor, chair the Homeland Security Council, and serve as the senior state official for cyber security matters.

Critical infrastructure is a shared responsibility. The federal government has a substantial role as does the industry leaders who generally own and operate the infrastructure. However, states have a role with state constitutions and Governor's authority under the law. I will touch briefly on our organization, our strategy, and our efforts at substantively addressing the threats to homeland security and critical infrastructure.

Every state is unique in its approach to homeland security. In Wisconsin, we did not create a separate agency to manage homeland security, choosing instead to rely on existing roles and responsibilities. Accordingly, the state relies on a Homeland Security Council to advise and coordinate on the preparation for and response to threats to Wisconsin's homeland security. The Council consists of representatives from major state agencies and first responders representing law enforcement, public works and fire fighters. In addition, our federal partners regularly attend these meetings.

The Wisconsin Homeland Security Council updates our homeland security strategy on a quadrennial basis following each gubernatorial election. This Strategy provides a framework to guide continuing efforts in preparation and protection of our communities and citizens. It also guides our investment of state and federal resources. The Strategy seeks to ensure that our first responders are trained and equipped, that our critical infrastructure is safe and secure, and that we continue to plan and prepare for emergencies and disasters that may impact our state.

This Strategy is Wisconsin's strategy and is our keystone document. It is informed by issues specific to Wisconsin as outlined in our Threat and Hazard Identification and Risk Assessment (THIRA) and our State Preparedness Report. From this keystone document, other plans are

updated and kept current; including our Wisconsin Emergency Response Plan, Continuity of Operations and Continuity of Government plans (COOP/COG), and our Cyber Disruption Response Strategy. It is informed by key federal documents including the National Preparedness Goal, the National Planning Frameworks, and the National Infrastructure Protection Plan.

Our Strategy has four key priorities: **Cyber Security; Asymmetric/Terrorist Threats; Catastrophic Incidents; and Capability Sustainment.** Each of our priorities has identified goals and objectives that are designed to be specific, measurable, achievable, relevant, and timely (SMART), with a specific state lead for each goal and objective. Each year, the Wisconsin Homeland Security Council issues an Annual Report to the Governor which provides an update on our progress. The following summarizes our priorities:

Cyber Security:

Wisconsin's state government has a clear responsibility to protect the state network and respond to cyber incidents. This priority is based on the leverage provided by cyber systems to accomplish essential state requirements and the importance of continuing these critical tasks in the event of a cyber-disruption. Wisconsin will provide support to local, tribal, and private agencies for cyber emergencies similar to other physical emergencies and will deploy capabilities in coordination with federal and regional partners.

The State of Wisconsin is highly dependent on technology. An incident involving the IT infrastructure could bring critical services to a halt. The State of Wisconsin alone receives 2 million cyber-attacks a day on the State system. In addition, the State receives 3.5 million incoming email messages per day with 94 percent of those messages filtered and blocked because they are malicious. In the last year, we have had several county and local government websites in Wisconsin that have been hacked and defaced.

While the U.S. Department of Homeland Security has identified 16 critical infrastructure sectors with vital assets or systems ranging from public health, transportation, and water systems -- most experts say the most critical is the energy sector. A cyber-attack on the energy sector could be devastating and affect homes, schools, businesses as well as all levels of government due to everyone's increased reliance on technology. We cannot operate in silos and MUST share resources and capabilities. That is why the time is now for the private sector and government to come together to prepare and respond to these threats.

The State of Wisconsin has taken a pro-active approach in working with businesses to protect the energy sector including:

- Hosting three Cyber Security Summits, bringing together business leaders, state and federal partners, and industry experts to discuss the State's role in cyber security.
- Co-hosting a Grid Outrage Retreat with the National Governors Association, bringing together public and private sector stakeholders to discuss the ramifications of a cyber or physical attack on an electrical grid; describe disaster response expectations; review existing emergency planning and response plans; and identify gaps aimed at helping the Governor and administration understand technical and policy issues involving planning and response efforts and increase communication with all players.

- Collaborating with FEMA Region V to create a regional power outage plan, including hosting a power outage workshop to bring stakeholders across all levels of government and the private sector together to develop a common operating picture and establish triggers and priorities for obtaining federal disaster assistance.
- Planning a series of water/wastewater system resiliency workshops to further identify challenges and potential solutions to restore or maintain services during a long-term power outage.
- Developing and training three State Cyber Response Teams in Milwaukee, Madison and Wausau that includes representation from local, state, tribal and territorial professionals. Currently, a fourth State Cyber Response Team is being formed to focus on the energy sector.
- Standing up a National Guard cyber protection team that will consist of 40 soldiers, co-located in Wisconsin and Illinois, and focused on training for the U.S. Army's mission protection priorities. In addition, the team will enhance the National Guard's existing computer network defense team and provide the State with a surge capacity to respond to cyber events. This team will be operational by the end of 2019 and, although trained to meet the U.S. Army's military requirements, it is fully available for state active duty at the Governor's discretion.
- Finalizing an agreement between the National Guard with several of our utility companies, who own critical infrastructure in the state of Wisconsin. Our agreement is aimed at information sharing and the potential for National Guard support. We initiated this relationship after learning of certain real world events, such as the attack in Metcalf.
- In order to meet this growing threat, the State will continue its commitment to developing state cyber response capabilities in coordination with local and federal partners, sharing information during an incident, raising awareness of cyber-security, and developing public/private partnerships to better protect critical infrastructure from cyber-threats. The State will also establish and improve processes to prepare for and respond to cyber-events.

Preventing and Protecting against Asymmetric or Terrorist Threats:

Our strategy for preventing terrorist threats centers on information sharing and, for this, we rely on two state fusion centers and our federal partners. Our two fusion centers - the Wisconsin Statewide Information Center (WSIC) and the Southeastern Wisconsin Threat Analysis Center (STAC) - are focused on collecting, analyzing, and sharing information.

The State also works with key partners in the public and private sectors to protect critical infrastructure from natural and intentional threats. Asymmetric threats include, but are not limited to, CBRNE (chemical, biological, radiological, nuclear, and explosive), infectious disease, and agricultural events. We have collaborated on the following exercises and/or processes:

- The National Guard Civil Support Team (Weapons of Mass Destruction) and the CEBRN Emergency Response Force (CERFP) are a key part of the layered protection for the state. These critical military resources provide enhanced capability as well as skills and training through outreach to our hazardous response community. They are also part of

the CBRNE Response Enterprise (CRE) providing a critical response capability wherever necessary across the nation.

- The Wisconsin Hazardous Materials Response Network (WHMRN) is based on a "risk benefit analyst" (RBA) model. The supporting data for this is a compilation of "fixed facility reporting data", transportation reporting data, demographic data, and historical response data. This analysis focuses on three primary areas: Threat, Vulnerability and Consequence Management so that WHMRN is predicated on "capability" rather than "capacity". Our hazardous materials response capabilities system is aligned with the National Incident Management System. We have a three-tiered system from local response to CBRNE capability. The state partners with 21 hazmat teams with different response capabilities. The goal is to have a hazmat team response at the incident site within 60 minutes of notification.
- The State has stockpiled firefighter foam that could be used during a crude oil fire. There is 1600 gallons of concentrate that could make 55,000 gallons of foam solution when mixed with water that is cached at Volk Field in Juneau County. An additional 1500 gallons of concentrate is stored at General Mitchell International Airport in Milwaukee and plans are to store a similar amount in the Fox Valley this fall.
- Wisconsin's state government has a clear responsibility to protect the state from infectious disease. This priority is based on the leverage provided by state agencies, such as the Wisconsin Department of Agriculture Trade and Consumer Protection, Wisconsin Department of Health Services, Wisconsin Emergency Management, and the Wisconsin National Guard. Through collaboration and information sharing and conducting exercises, we can accomplish essential state requirements and maintain preparedness in the event of an infectious disease outbreak.
    - Throughout the 2014-2015 Ebola outbreaks in West Africa and other affected countries, the Wisconsin Department of Health Services led the statewide response and provided updated information for public health professionals and the general public. Officials worked with the Wisconsin National Guard to establish a Rapid Response Team and developed a tiered hospital structure to ensure that, if needed, patients would be transported to a hospital that could provide the appropriate standard of care. These response capabilities have been incorporated into the State's ongoing planning for emerging infectious diseases. This 35 person team composed of doctors, physician assistants, nurses, liaison officers and decontamination specialists, conducted extensive training in order to respond and support our medical community in the event of an Ebola outbreak in Wisconsin.
    - The Highly Pathogenic Avian Influenza (HPAI) H5N2 was first detected in Wisconsin at a commercial chicken flock in Jefferson County on Monday, April 13, 2015. The State's response was led by the Wisconsin Department of Agriculture, Trade and Consumer Protection with support from Wisconsin Emergency Management, Wisconsin Department of Natural Resources, Wisconsin Department of Health Services and the Wisconsin National Guard. Ultimately, it spread to ten farms in four counties where 1,765,008 chickens and turkeys were depopulated over a five-week period. Quarantines were placed on the infected premises and individual premises in the 10km control zone to manage the spread of the HPAI. The Wisconsin National Guard provided the support in the form of a small team of decontamination specialists in order to provide

decontamination of vehicles entering and exiting the affected poultry facilities. Over the course of 28 days, the team decontaminated 95 vehicles and 70 pieces of equipment, thus helping to contain the outbreak at this location. On August 11, 2015, all HPAI affected premises were released from quarantine.

- Wisconsin' state, private, and public stakeholders fully understand the criticality to prepare for, manage, and respond to the finding of Foot and Mouth Disease (FMD) in a local dairy or other animal herd. The Wisconsin Department of Agriculture, Trade and Consumer Protection is storing a decontamination equipment unit at Volk Field that could be deployed during an animal health emergency. The primary goals are to ensure biosecurity is in place and to be able to conduct rapid depopulation during an outbreak. To that end, in November of 2015, 47 participants, from federal, state and local agencies, the Wisconsin National Guard and other entities, met to enhance preparedness, practice the FMD response plans, identify interdependencies amongst the animal-sector, public health, and the emergency services sector as well as coordination mechanisms. This exercise is but one part of Wisconsin's commitment to continued preparedness for an outbreak Foot and Mouth Disease.

- In 2012, Governor Walker joined officials with the U.S. Department of Homeland Security in the launch in Wisconsin of the "If You See Something, Say Something®" Campaign. The State has a dedicated website located at www.wiwatch.org and a toll-free number 877-WI-WATCH which is manned by both fusion centers. Following the Paris bombings in 2015, Governor Walker held a press conference with federal, state and local law enforcement encouraging citizens to be vigilant and report suspicious activity. Recently Governor Walker and State Superintendent of Schools Tony Evers participated in a video that will be shown at junior and high schools across the state encouraging youth that if they see something suspicious to report it to local law enforcement.

Catastrophic Incident Response and Recovery:

Consistent with state law and the Governor's vision, the state has a leading role in disaster response. Wisconsin's Emergency Management coordinates assistance in support of local agencies and, when required, coordinates with federal authorities for assistance.

In a catastrophic incident, local and state resources may be overwhelmed and there may be significant threats to life, safety, and property. It is important to plan for high-consequence, low-probability events in order to protect our communities and enable a speedy and full recovery following a disaster. Preparation for catastrophic events and exercising of complex processes will also ensure the best preparation and response for all emergencies. Our efforts include:

- Our Comprehensive Response Plan focuses on the priorities of need and the coordination necessary during the first 72 hours in the following areas: enable response; survivor needs; and starting restoration.
- The Wisconsin Emergency Support Team (WEST) provides an on-scene coordinated state unit to support local disaster response and recovery efforts. The team is comprised of representatives from designated state agencies. They will provide support to local field response and recovery activities; serve as the point of contact and communications

link for agency staff in the field; report agency information to the agency representative in the emergency operations center (EOC), if elevated, or otherwise to the agency designee; and provide a local--state conduit for resource requests and management.

- The State supports 50 local and regional exercises a year, including Miles Paratus which will be held June 5-9, 2016 at Volk Field and Fort McCoy. In addition, the State of Wisconsin Emergency Operations Center will be activated for three days to test our response capabilities. To ensure our responders can talk with each other, federal, state, county, tribal and volunteer agencies, and the military, communication assets are part of the annual State Interoperable Mobile Communications Exercise (SIMCOM) that is held every May. The goal is to develop relationships and understand the capabilities of other agencies before they are needed in a real emergency. Specific operations being tested this year include data sharing, radio frequency bridging and patching, and network failures. The State also continues to participate in exercises involving the Point Beach Nuclear Power Plant and the Prairie Island Nuclear Generating Plant.
- Wisconsin has established seven regional healthcare coalitions to coordinate how public health, healthcare institutions, and first responder agencies, such as police, fire and emergency medical services (EMS), will manage their efforts to enact a uniform and unified response to an emergency, including a mass casualty or other catastrophic event. The coalitions can help to close critical gaps in medical surge capacity, improve situational awareness, and provide support to health care system resource requests.
- We are creating a Business Emergency Operation Center (BEOC) that will serve as a conduit to share information between Wisconsin's State Emergency Operations Center (SEOC) and the private sector during an emergency. The BEOC will coordinate response and recovery efforts and improves communication and situational awareness between businesses impacted by a disaster and governments at all levels. This level of collaboration will speed and improve the response and recovery activities for impacted communities.
- The National Guard Reaction Force (NGRF) stands ready to provide assistance to civil authority for the protection of critical infrastructure and other state and/or national assets, and to conduct security operations. This 500 Soldier and Airmen force is fully trained and validated annually. The last validation of this force came in August 2015 in an exercise that included over 300 first responders and was conducted the community around Waukesha, WI. This force can provide site security and presence patrols, maintain roadblocks and checkpoints, and are capable of supporting law enforcement during civil disturbance events. In December 2014, the NGRF was deployed at the request of the Milwaukee County Sheriff as his office dealt with the District Attorney's announcement related to an officer-involved shooting of Mr. Dontre Hamilton.

Sustainment of Capabilities Built through Long-Term Investments:

The State has made significant investment to build and enhance homeland security capabilities. It is vital to sustain these capabilities in sufficient capacity through continued training and exercises, as well as equipment and technology recapitalization. Examples include:

- Wisconsin Emergency Management convenes a Funding Advisory Committee on an annual basis to seek the input of groups and agencies with a vested interest in the HSGP

allocations. Representation includes members of the emergency response community (police, fire, EMS), state agencies, and the Milwaukee Urban Area Security Initiative (UASI). All projects funded within the approximately eight overarching investments that make up the federal grant application are linked to the Wisconsin Homeland Security Strategy and are closing gaps identified in the State Preparedness Report. Most of the investments sustain capabilities such as our emergency regional response teams, the two fusion centers, and exercising and training for local responders.

- The State continues to provide training to more than 3,000 first responders per year in the National Incident Management System and several other emergency training courses.
- Wisconsin Emergency Management manages and maintains a Statewide Structural Collapse Taskforce that provides collapse rescue capabilities that can respond anywhere in the state within eight hours.
- Our Wisconsin National Guard works closely with Wisconsin Emergency Management in planning for and exercising our emergency plans. We are certainly not alone in this aspect, as the National Guard across the nation has unique relationships with law enforcement, fire fighters, federal agencies, and industry partners. Always focused on adding support for the incident commander and providing our nation's Governors with a surge force that is highly trained and relevant across the domestic response spectrum.
- WEM continues to implement the Wisconsin Credentialing and Asset Management System (WICAMS), which is a statewide system to rapidly identify, validate, and track incident response personnel and resources being deployed an incident. WICAMS enables incident commanders and emergency operations centers manage personnel and resources during large-scale responses, and helps prevent unauthorized access to impacted areas. Over 11,000 Wisconsin responders representing more than 1,600 agencies are credentialed in WICAMS, and the system is growing by more than 300 new responders each month. Wisconsin is working with utilities and other private sector entities to join the system.
- Following events or exercises, the State conducts an After Action Report (AAR). AAR's are required by FEMA and follow the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.

Homeland Security is important to the State of Wisconsin. As a home rule state, our first line of preparation and defense is our first responders. Our sheriffs and police chiefs lead professional and highly engaged law enforcement agencies. Our firefighters are highly skilled and have developed effective processes for coordination and collaboration.

When our first responders need assistance, the State provides regional and state-wide support. This includes all state agencies and the Wisconsin National Guard. The Wisconsin National Guard is a state military organization that provides robust capabilities when required in support of our first responders.

When state capabilities or capacity is exceeded, we rely on other states through the Emergency Management Assistance Compact (EMAC) for resources including the National Guard. Lastly, we work through FEMA for federal resources when needed.

The federal government has provided leadership and resources for homeland security. The grant programs and collaboration is greatly appreciated and largely effective in increasing capability and resilience. The FBI and USDHS are engaged with law enforcement and in our communities and they are professional and appreciated. FEMA is engaged regionally and they are appreciated.

Wisconsin is engaged as well. While we appreciate our federal partners and their support, we believe that we have a primary role for our citizens. We are committed to the National Response Framework and believe all disasters are local and, while we value our partnership with FEMA, we view them a resource and not as the responsible party.

There are matters before Congress that will add value to our shared concerns for critical infrastructure.

These matters include:

1. **Cybersecurity information** sharing must include sharing the information with state governments. Governors have a leadership role on behalf of their citizens. Fusion centers are strong state assets and the federal government must value them and their contribution. While grants do support fusion centers, the vast majority of funding is often state and local in terms of venue, equipment and personnel. Local and state collaboration is critical in our response to on-going terrorism concerns.

2. It would be beneficial if DHS could ensure that each **fusion center** had one intelligence and cyber analyst assigned to work full time in our cities and states.

3. We must **collaborate** on big issues that could cripple America. This includes long term power outage, whether caused by natural disaster, cyber events, or intentional acts of sabotage. A long term power outage could devastate our nation and we should seek areas to mitigate where possible. Issues such as sustainment of water and sewage systems during a power outage are examples of such mitigation planning.

4. Reviewing the cyber threat in its entirety and seeking to establish clear lanes of responsibility. Unlike most emergencies, where we can apply the **National Response Framework** and seek assistance above the local level when needed, cyber is pervasive in its value to our society and its threat.

5. **The Homeland Security Grant Program (HSGP)** could be improved if FEMA administered the Program with a focus on continuity in policy and consistent application and reporting requirements. The administrative burden for this grant is heavier than for other federal grants due to a lack of continuity and clear grant guidance.
States and UASIs have information that FEMA and Congress may want but the way in which the program is administered does not allow States and UASIs to share that information in suitable, useful formats. There are two examples:

One of the three online systems that are used to complete the federal grant application has severe character limitations for narrative information. Questions in the application ask for a significant amount of information but the space available to provide a thorough, detailed answer in context of a larger project plan, strategy, or identified gap is limited to the point where known information is often deleted in order to be able to submit the application. Wisconsin gathers more project information to share with our decision-making funding advisory body than we can possibly fit into the system. We actually delete crucial project information in order to be able to meet the limitations of the system.

The requirement for submitting a State Strategy for homeland security has been eliminated as a grant requirement. Over the years, states have built their homeland security programs to incorporate writing a strategy and then linking funding requests to that strategy. This has been true of numerous reports that have either been eliminated or drastically changed every few years. It becomes difficult to establish a baseline, track progress, and provide meaningful information to stakeholders, FEMA, and Congress if the program is starting over every few years in terms of strategy, plans, and gap and asset analysis.

6. Eliminate the 45-day pass-through requirement for the **Homeland Security Grant Program** and allow States to administer the program on the schedule that works for the sub-recipients and the State Administering Agency. HSGP is now an established program and most of the country is sustaining current projects as they receive a minimal amount of funding. The projects are on a set schedule that does not always match up with the need to get sub-grants out within 45-days. In order to achieve effective grants administration and provide excellent customer service to locals, states should be able to administer their program on a timeline that fits within the three-year performance period.

In closing, Wisconsin is committed to its citizens and is aware of our role in homeland security. By law, our Governor has substantial plenary authority under the State's Constitution and we seek to approach all hazards in a deliberative and collaborative method. We will continue to train, exercise, and learn from real world events, seeking to improve our collective posture and foster a culture of preparedness. While we can never be fully prepared for all emergencies, it is our intent to be as prepared as possible through engaged partnership and measurable planning. We look forward to continued federal partnerships and greatly appreciate the work of this committee.

TESTIMONY OF

THOMAS L. FARMER

CHAIR

CROSS-SECTOR COUNCIL

PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY

BEFORE THE

U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING ON ASSESSING THE SECURITY OF CRITICAL INFRASTRUCTURE: THREATS, VULNERABILITIES, AND SOLUTIONS

MAY 18, 2016

Good morning, Mr. Chairman and Members of the Senate Homeland Security and Government Affairs Committee. I am Tom Farmer, Assistant Vice President for Security for the Association of American Railroads.

Today, however, I am testifying in my capacity as the Chairman of the Cross-Sector Council of the Partnership for Critical Infrastructure Security (PCIS). The PCIS is a representative forum, established at the private sector's initiative, which facilitates consultations, information sharing, and coordinated effort across the critical infrastructure sectors and sub-sectors and with the federal government. We also work with the State, Local, Tribal, and Territorial Government Coordinating Council, the Regional Consortium Coordinating Council, and the National Council of Information Sharing and Analysis Centers.

PCIS dates from 1999, when it was established by the private sector to address priorities defined in Presidential Decision Directive 63 (*Critical Infrastructure Protection)* — most notably, to foster partnering with government for mitigation of security risks. While the representatives of the respective sectors and sub-sectors have changed over time, the commitment by members of the PCIS to cooperative efforts to enhance preparedness for all hazards and emergencies has not wavered.

The adaptive structure maintained by the private sector has enabled the PCIS Cross-Sector Council to meet the requisites of Presidential directives issued following the terrorist attacks of September 11, 2001, and of the National Infrastructure Protection Plan (NIPP), as first implemented in 2006 and in later updates. (The most recently updated is *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)*. Consistent with the organizing approach established under the NIPP, the Cross-Sector Council is comprised of the Chairs, Co-Chairs, Vice Chairs, and Designated Representatives of the Sector Coordinating Councils of each of the critical infrastructure sectors and sub-sectors.

Regular consultations occur between members of the PCIS Cross-Sector Council and federal officials, especially from the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence, and other federal agencies responsible for various critical infrastructure sectors. Some meetings occur regularly; others are driven by threats, incidents, or emergencies of interest to the sectors' representatives.

To afford the opportunity to engage with federal government officials for the purpose of achieving consensus on joint priorities and actions to advance critical infrastructure security, protection and resilience, some joint meetings between the PCIS Cross-Sector Council and representatives of federal departments and agencies are convened under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework.

The objectives, accomplishments, and continuing efforts of the PCIS Cross-Sector Council and its members are reflected in three categories: (1) unified priorities for action defined with DHS and its federal partners; (2) sector-based interaction with government components; and (3) cross-sector cooperation on interdependencies. I discuss each of these in turn below.

Unified Priorities for Action with Federal Partners

Four fundamental priorities drive the PCIS Cross-Sector Council's unified efforts with DHS and its federal government partners in the critical infrastructure protection and resilience mission:

(1) Timely Sharing of Actionable Intelligence:

The first priority is to ensure timely sharing of actionable intelligence and related security information on developing threats and concerns. In this vital area, PCIS members proposed a Joint Threat and Security Intelligence Engagement Group to leverage the existing cross-sector councils established by government and industry in the implementation of the National Infrastructure Protection Plan.

The objective is to ensure common, and sustained, awareness across sectors and sub-sectors – within industry, in supporting Information Sharing and Analysis Centers, and within governmental Sector Specific Agencies. Sharing practical and applicable threat intelligence and security information creates opportunities to narrow risk profiles through informed vigilance and, if warranted, heightened security measures.

The effectiveness of this engagement process was proven in a national communications exercise held November 10, 2015. Representatives of the government and industry cross-sector councils ratified the structure and procedures during a joint meeting on November 13. Within a matter of hours, the horrific terrorist attacks in Paris necessitated activation of the engagement group for its intended purpose – timely sharing of accurate information on developments and the threat and security implications for the United States.

Recognizing that at times the relevant intelligence and security information may be classified, the PCIS Cross-Sector Council proposed two significant enhancements to government procedures.

First, we leveraged the existing video-teleconferencing capabilities in state fusion centers[1] and field offices of federal agencies to enable secure sharing of classified information. This proposal sought to eliminate the inordinate delays and excessive costs that resulted from the recurring practice of calling private sector representatives to Washington, DC, for classified briefings and discussions on potential security threat or the implications of physical or cyber-attacks. There is substantial progress to report.

On April 26, 2016, DHS's Offices of Infrastructure Protection and Intelligence and Analysis partnered with a group of PCIS Cross-Sector Council representatives and officials at state fusion centers to hold a classified briefing via secure video teleconference. Participating fusion centers included Colorado, Kentucky, New York, and Wisconsin (Madison and

[1] State fusion centers are locally owned and operated facilities that serve as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between government, tribal, and private sector partners. DHS considers them to be the primary conduit between frontline personnel, state and local leadership, and the rest of the homeland security enterprise.

Milwaukee). DHS hosted the conference from its offices in Arlington, Virginia. This initial test proved the concept.

A second similar exercise will be held by early July 2016, with the aim of reaching representatives of each of the critical infrastructure sectors and sub-sectors nationwide. With this capability, what had formerly taken weeks to accomplish in multi-lateral sharing of classified information can now occur within just a few hours, ensuring awareness and enabling more timely actions to narrow risk profiles.

The second significant enhancement to government procedures we proposed is the concurrent development of an unclassified "tear line" during production of a classified assessment or analysis to enable participants to bring actionable information to their respective sectors. In the absence of appropriate security clearances and need-to-know, the classified information received cannot be shared. But to ensure the objectives in holding the classified meeting are met, an unclassified version enables participants to bring information to their sectors that can be applied to inform vigilance and, as warranted, proactive protective or preparatory measures.

(2) Draw and Apply Lessons Learned

The second priority is to draw lessons learned from the numerous exercises and regional risk and resiliency assessments conducted or sponsored by DHS. A wealth of information and experience has been gained from the conduct of National Level Exercises (NLEs), Cyber Storm exercises[2], and applications of the Regional Resiliency Assessment Program. Too often, however, the conduct of the exercise or the assessment itself is the performance measure rather than an analysis of results and lessons learned to identify any recurring deficiencies in capabilities, coordination, or performance. The identified concerns could then inform joint priorities for action by the government and industry cross-sector councils. We are working with government partners to achieve this outcome.

(3) Enhance Risk Management

The third priority is to enhance cyber threat analysis and its effectiveness as a risk management tool. DHS and FBI have gained extensive experience and insights as they've responded to cyber breaches and threats and disseminated indicators of concern. This wealth of information on cyber tactics employed and on gaps in preparedness allows recurring analysis of this information to inform cybersecurity risk mitigation by highlighting:

- Tactics that are most commonly employed to gain illicit access to networks and systems;
- Vulnerabilities in targeted systems and networks most frequently exploited;
- Indicators of these illicit activities most often noted in post-incident analyses that were missed or disregarded; and

[2] Cyber Storm refers to biennial DHS exercises designed to strengthen cyber preparedness in the public and private sectors. The most recent exercise took place March 8-10, 2016.

- Protective measures most often found lacking or absent that could have made a difference.

As a comparative reference, Australia's equivalent to the United States Computer Emergency Readiness Team (US-CERT) conducted such an analysis and found, "at least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following" four mitigation strategies. This determination, shared publicly via the ASD's website, informs effective cyber risk management decision-making for private sector entities in Australia.

Applying information that is already available can enable collective improvement, across the sectors, in defeating the most common tactics and redressing frequently exploited vulnerabilities and gaps. Significantly, DHS has commissioned a pilot program focused on these analytical priorities for the Transportation Sector, with the goal of applying lessons learned in products for sharing across sectors.

(4) Outreach – Early and Often

The fourth priority is early and regular outreach and coordination on proposed homeland security and preparedness strategies and programs, on preparedness initiatives, and on defining objectives to enhance practices and procedures.

At times, private sector input has been sought after many months of effort within government when, practically, the opportunity to shape or influence the finished product is substantially diminished. Yet, the strategies, programs, and initiatives often entail some level of action by private sector entities. More effective and sustainable outcomes are achieved when there is, from the outset, a common understanding of purposes and goals and opportunities for industries to provide relevant information and context based on their knowledge of and experience in their respective sectors.

Sector-Specific Interaction with Federal Partners

The second main category of activity by PCIS members is in their sector-specific interaction with government components. Frequently, these interactions have produced outcomes beneficial across the critical infrastructure community. For example:

- For enhanced cybersecurity, the Defense Industrial Base Sector partnered with the Department of Defense and DHS in an innovative program to share classified indicators of potential threats with private corporations. The success of this initiative prompted expansion to other sectors through a program managed by DHS. The productive outcome has enhanced awareness and opportunities to implement effective protective measures.
- Engagement by DHS officials with representatives of the Commercial Facilities and Retail Sectors in the aftermath of the terrorist attack at Westgate Mall in Nairobi, Kenya, in September 2013, produced a regionally applied training initiative that focused on indicators of concern, protective measures, and immediate response actions

for potential active shooter threats at malls, hotels, and other retail venues. This cooperative effort led to quarterly consultations on classified reporting on security threats and incidents by DHS and Commercial Facilities Sector representatives. This initiative has now been expanded to encompass representatives of other industry sectors. The collective group of government and industry representatives review information classified at up to the Top Secret level for broader cross-sector relevance and application and for opportunities to reduce classifications and produce unclassified advisories.

- In view of the persistent threat posed by active shooter incidents, representatives of multiple industries partnered with the DHS and FBI to develop a comprehensive training program on prevention and mitigation. The prevention element leverages insights gained from investigations of these types of incidents to highlight recurring behavioral indicators that have preceded a mass shooting attack. The mitigation component focuses on immediate actions that people at a targeted facility or area should take to protect themselves and others and to facilitate an effective law enforcement response. The application of this program in Washington, DC, in April 2016 drew wide participation by area law enforcement departments and security leads for educational institutions, corporations, trade associations, and other private sector entities.

Cross-sector Cooperation

Finally, the third main category of activity facilitated by PCIS is cross-sector cooperation. The regular interaction of industry representatives through meetings, consultations, coordination, and information sharing within the PCIS Cross-Sector Council fosters connections that yield benefits in expanded and enhanced cooperative efforts to address priorities and concerns defined in each of the sectors. As representative examples:

- PCIS coordinated a thorough assessment to identify interdependencies among critical infrastructure industries.
- The National Council of Information Sharing and Analysis Centers has engaged with PCIS sector representatives to conduct cross-sector exercises, using realistic physical and cyber threat scenarios that seek to enhance information sharing and coordinated efforts.
- The Electricity Sector has proactively engaged colleagues in the Communications, Information Technology, and Transportation Sectors in cooperative efforts to enhance the resilience of electrical power generation and transmission in the face of natural and man-made threats. Cross-sector exercises have tested plans and procedures for cooperative responses to mitigate effects of disruptions to availability of electrical power and facilitate more timely and efficient restoration actions.
- The Commercial Facilities Sector has provided cross-sector partners access to facilities designed for greater resilience in areas affected by emergencies.

- Entities within the Transportation Sector, notably the Rail and Highway and Motor Carrier sub-sectors, have assisted entities within the Communications Sector following major storms and other natural hazards in gaining access to infrastructure for response and recovery actions.

Again, the activities outlined above are representative examples. The full scope of effort is substantially broader, reflecting a fundamental strength of the critical infrastructure protection and resilience mission. Corporations, companies, and associations across industries are dedicating staff, resources, and investment to cooperative efforts across sectors and with government in a shared commitment to critical infrastructure protection and resilience. The sustained emphasis is on identifying opportunities to improve and proposing the solutions to transform the opportunities into productive and sustainable outcomes.

On behalf of the colleagues across sectors for whom I am privileged to serve as a representative and spokesperson, thank you for this opportunity to address their level of commitment and the scope and effectiveness of their efforts.

Statement of Ted Koppel

"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions"

May 18, 2016

Mr. Chairman, Mr. Ranking Member, Members of the Committee.

Your late colleague, the distinguished Senator from New York, Daniel Patrick Moynihan, liked to say that each of us is entitled to his own opinion, we are not, however, entitled to our own facts. That observation, which once seemed both sensible and self-evident, can no longer be taken for granted. In a political climate where even the President's status as a natural born American citizen remains the object of doubt for more than a quarter of our population as he nears the end of his second term in office, in that climate it will be difficult to settle the far more complex issue before the committee this morning: Is the nation at risk of a crippling cyber attack against elements of our infrastructure in general and against one or more of our electric power grids in particular? After more than a year of research into the question, I believe the answer to be "yes."

Simply stated, the electric power industry is made up of 3200 separate companies linked in a network that both generates and distributes electricity. For the system to function, a perfect balance has to be maintained between the amount of electricity being generated and the amount being distributed. Only the Internet is capable of maintaining that exquisite balance at all times. The Internet was never designed to be defended. The Internet remains vulnerable to cyber attack. Evidence of that vulnerability is accumulating every single day in private industry, government agencies and in breaches of our personal data. General Keith Alexander, the former head of the National Security Agency, likes to say that there are only two kinds of companies – those that have been hacked and those that don't yet know it. Members of this committee are certainly familiar with the conclusion of our intelligence agencies that the Chinese and the Russians have already mapped and penetrated the systems that control our electric power grids. Iran is not far behind. Nations like North Korea and Syria are enhancing their cyber warfare capabilities. It is surely only a matter of time before a terrorist group, unrestrained by any geopolitical interests, acquires the capability to attack one of our power grids.

The problem, as Tom Ridge, our first Secretary of Homeland Security, noted is that ours is a reactive, not a pre-emptive society. In the wake of the attacks on 9/11/2001, the United States embarked on actions and expenditures that would have been inconceivable only a week earlier.

My message to this committee this morning is simple: The nation cannot wait for a cyber attack on the grid before making preparations for its consequences. It is my belief (and again, this committee has access to more information on this subject than I) – I believe that while the Department of Homeland Security has plans for dealing with the consequences of hurricanes, blizzards, floods and earthquakes, it has no discreet plan for dealing with the aftermath of a cyber attack on one of the nation's power grids. The Department's recommendations for each disaster are essentially the same: a two to three-day supply of food and water for each

person, a plan for families to meet at a pre-arranged point, a supply of essential medicines, flashlights and a battery-powered radio. A cyber attack against one of our electric power grids could deprive tens of millions of Americans of electricity for a period of weeks or even months. I asked Homeland Security Secretary Jeh Johnson what, exactly, he would be telling Americans on their battery powered radios after an attack that he was unwilling or unable to share now. He gestured toward a shelf carrying several white binders: "I'm sure there's a plan up there somewhere," he told me. I don't share the Secretary's confidence.

We have neither the adequate food supplies to take care of those millions who decide to shelter in place, nor the collaborative plans with state governments to house and feed what could amount to millions of internal refugees. If we began tomorrow, Mr. Chairman, implementing such plans would still take a couple of years.

I thank the Committee for its attention to this critical issue.

STATEMENT OF SCOTT I. AARONSON
MANAGING DIRECTOR, CYBER AND INFRASTRUCTURE SECURITY
EDISON ELECTRIC INSTITUTE

BEFORE THE U.S. SENATE HOMELAND SECURITY
AND GOVERNMENT AFFAIRS COMMITTEE

"ASSESSING THE SECURITY OF CRITICAL INFRASTRUCTURE:
THREATS, VULNERABILITIES, AND SOLUTIONS"

MAY 18, 2016

Introduction

Chairman Johnson, Ranking Member Carper, and members of the Committee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Managing Director for Cyber and Infrastructure Security at the Edison Electric Institute (EEI).

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly and indirectly support more than 1 million American jobs. EEI has 70 international electric companies as Affiliate Members, and 270 industry suppliers and related organizations as Associate Members. For EEI's member companies, securing the power grid is a top priority; I appreciate your invitation to discuss this important topic on their behalf.

In addition to my role at EEI, I also serve as Secretary for the Electricity Subsector Coordinating Council (ESCC). The ESCC is comprised of the chief executive officers of 21 electric companies and 9 major industry trade associations. This group—which includes all segments of the industry, representing the full scope of electric generation, transmission, and distribution in the United States and Canada—serves as the principal liaison between the federal government and

the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC has been held up by the National Infrastructure Advisory Council as a model for how critical infrastructure sectors can more effectively partner with government. In fact, the ESCC has been a catalyst for major initiatives that are improving the security posture of the industry and, by extension, the nation.

My testimony focuses on the value of the government-industry partnership in the face of threats to the electric sector, as well as the public policy considerations and strategic initiatives that can enhance the security of the nation's most critical infrastructure.

Managing Risk: An Overview of Threats to Critical Electric Infrastructure

Electric companies understand that reliable electricity is essential to the nation's security and our way of life. Providing reliable service is a responsibility the industry takes extremely seriously. Importantly, the industry also understands that it cannot protect all assets from all threats, and instead must manage risk. Rather than trying to achieve the impossible task of protecting every asset from every conceivable threat, the electric sector follows a multi-layered risk management approach to grid protection.

The key to this strategy involves setting priorities to protect the most critical power grid components against the most likely threats. If we frame risk as a function of likelihood and consequence, then we can allocate resources more effectively.

With threats that are less likely to occur, but could have potentially severe impacts to grid reliability, an important partnership has developed between government and industry to ensure the sector and our nation are secure. It is the man-made events—such as coordinated cyber and physical attacks or an electromagnetic pulse (EMP)—or the natural phenomena, like solar flares, major earthquakes, or weather events on the scale of Superstorm Sandy, that require coordination between government and industry, as well as across the critical infrastructure sectors.

Grid operators prioritize risk in order to enhance protection around critical assets, engineer redundancy to avoid single points of failure, stockpile spare equipment for hard-to-replace components, and develop other contingencies to minimize impact regardless of the nature of the incident.

By exercising and applying lessons from actual events, electric companies are able to enhance grid protection, resiliency, and restoration efforts. Invaluable insights have been gained from events such as Hurricane Katrina, Superstorm Sandy, the April 2013 Metcalf Substation attack in California, and recent events in Ukraine where industry experts accompanied a DOE after-action assessment team.

It is this flexibility and adaptability in the face of an always-evolving threat environment that are positioning the industry to be truly prepared to manage risk and respond to all hazards.

Defense-in-Depth: Standards, Partnerships, and Response

The electric power sector takes what is known as a "defense-in-depth" approach to protecting grid assets. This includes several tools that, when taken together, provide a more comprehensive approach to the industry's security posture. Specifically, the industry is subject to rigorous, mandatory, and enforceable reliability regulations; closely coordinates with industry and government partners at all levels; and has efforts in place to prepare, respond, and recover should power grid operations be impacted.

Security standards and regulations are important to the industry's security posture.

Under the Federal Power Act and Federal Energy Regulatory Commission oversight, the electric power sector is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties of up to $1 million per violation per day.

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

In addition to implementing Versions 5 and 6 of the cybersecurity requirements, prompted in part by lessons learned from the aforementioned Metcalf attack, the industry is implementing new mandatory requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry also is using voluntary standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as the Department of Energy's Cybersecurity Capability Maturity Model (C2M2). Electric companies throughout the industry are assessing their cybersecurity capabilities against this framework and capability maturity model and, based on results, prioritizing their investments to strengthen cybersecurity.

While regulations and standards provide a solid foundation for strengthening the industry's security posture, they alone are insufficient. As the threat environment evolves, so must the industry's security efforts.

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

As has been noted throughout this testimony, protection of critical infrastructure is a shared responsibility between the government and industry. The ESCC was formed to help coordinate these efforts and to ensure we are appropriately deploying each other's expertise, capabilities, and assets. The ESCC consists of electric company CEOs and trade association leaders who represent all segments of the electric sector and actively partner with government executives to prepare for, and respond to, national-level incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work very closely and very quickly, senior executives on both sides also help to ensure unity of effort and unity of message among their organizations. During an incident, the ESCC's role—while not operational—is to provide situational awareness, align messaging, and coordinate with government on response and recovery efforts.

The industry and government leaders are focusing on four main areas that improve the security posture of the industry and the nation. They are:

1. Tools & Technology: Deploying government technologies that improve situational awareness and enable machine-to-machine information sharing;

2. Information Flow: Making sure actionable intelligence and threat indicators are communicated to the right people at the right time;

3. Incident Response: Planning and exercising to coordinate responses to an incident;

4. Cross-Sector Coordination: Working closely with other interdependent infrastructure sectors to ensure all are prepared for, and can respond to, national-level incidents.

Within these areas of focus there are three specific ESCC initiatives I would like to highlight:

Cyber Mutual Assistance

The electric power industry has a culture of mutual assistance; when a weather event or natural disaster impacts a region, crews and lineworkers from all over North America descend on the affected region to restore power. Through storm preparation and mutual assistance networks, the electric power sector has decades of experience working together in response to major incidents.

For example, the sector's response to Superstorm Sandy had companies from as far away as California, Texas, and Canada sending equipment and crews into the affected regions to restore

power. More than 80 companies and tens of thousands of mutual assistance crews responded. Similar responses were seen following Hurricanes Katrina and Rita. In short, mutual assistance is not just a program, it is in our DNA.

As cyber risks proliferate, the industry is organizing itself to pool resources in the face of incidents that exceed the capacity of individual companies to respond. In its early stages now, a framework is being developed to identify and share resources during incidents. Over the long-term, this project—with the backing and leadership of senior industry executives—will evolve based on the cyber incident response needs of the industry. In addition, electric companies work to maintain and strengthen their ties to state agencies, state and local law enforcement, and state Fusion Centers that receive, analyze, gather, and share threat information.

Cybersecurity Risk Information Sharing Program (CRISP)

The electric power sector has deployed CRISP to bolster its situational awareness and information sharing. CRISP developed as a partnership among five pilot electric companies, the Department of Energy (DOE), the Electricity Information Sharing & Analysis Center (E-ISAC), and the Pacific Northwest and Argonne National Laboratories. CRISP enables near real-time sharing of cyber threat data among government and industry stakeholders, while supporting machine-to-machine threat mitigation.

Cyber threat information shared through CRISP is helping to inform important security decisions not just among participating companies, but to all E-ISAC members throughout the electric sector, as information gleaned by the technology is then shared anonymously through the E-ISAC portal. By the end of this year, more than 75 percent of all electricity customers will be covered by an electric company that will have deployed CRISP, but the entire industry continues to benefit.

Electromagnetic Pulse (EMP) Mitigation

The ESCC works closely with the government to better understand the threat posed to electric infrastructure from a man-made EMP, either from a high-altitude nuclear blast or a so-called "directed energy" weapon. Based on these discussions, and building on research done by the

National Labs and Department of Defense, the Electric Power Research Institute (EPRI) is undertaking a major collaborative research effort with DOE. This project is designed to enhance our understanding of system impact should such an attack occur and to explore the effectiveness of mitigation strategies (including hardening and recovery). The project will allow grid-specific research to inform the application of technologies that will increase grid resilience and accelerate recovery.

A recent Government Accountability Office (GAO) report recommended enhanced federal agency coordination with industry to identify and prioritize risk-management activities, such as research and development efforts, to address EMP risks to the grid. The recently initiated EPRI project is just such an effort.

Protecting and defending electric infrastructure are not enough; we also must plan to respond and recover should an incident impact operations.

Owners and operators of critical infrastructure strive for a 100-percent success rate in their protection efforts, but the adversary only needs to be right once. Given these odds, a comprehensive approach to security must include contingency plans to respond and recover as quickly as possible in the event something occurs.

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

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

Support Guide to expedite the deployment of equipment and services that would be needed to move these critical assets rapidly in an emergency.

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

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

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

With exercises and real-world events serving as catalyst for new initiatives, from developing a cyber mutual assistance regime to looking at extraordinary measures the sector can take to mitigate damage from incidents, the electric sector is constantly improving its security posture and approach to preparedness.

Conclusion

Security cannot be static; threats evolve and so must we. The electric sector embraces this fact as demonstrated by the ongoing development of regulatory standards, the high-level partnerships

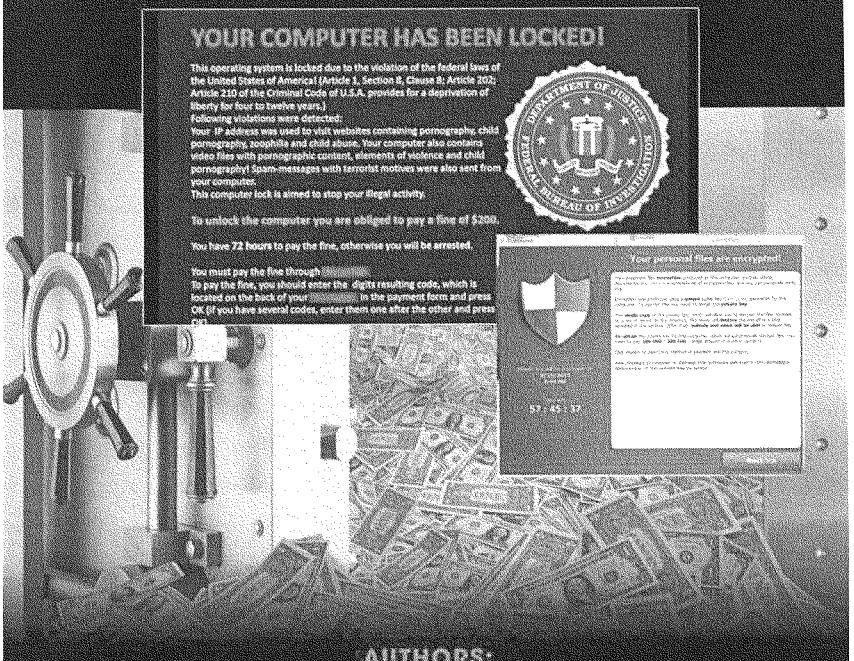
developed under the ESCC that are enabling us to accomplish more in less time, and the focus on constantly improving preparedness by applying lessons learned from exercises and real-world events. As industry and government leadership improves our ability to protect critical infrastructure from all types of threats, we look forward to working with Congress on this important mission.

On behalf of owners and operators of critical electric infrastructure, I appreciate the Committee holding this hearing to learn more about threats facing the industry. It is my hope that this testimony provides insight into what the electric sector is doing to address these threats, while also making clear that there is no such thing as risk elimination, only risk management.

As we work to manage risks facing the sector and the nation, I am proud to say the electric sector and the government are working closely in innovative ways to protect critical infrastructure from attacks and to limit the consequences of an attack should one occur.

THE ICIT RANSOMWARE REPORT

2016 WILL BE THE YEAR RANSOMWARE HOLDS AMERICA HOSTAGE



AUTHORS:

JAMES SCOTT (ICIT SENIOR FELLOW – INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY)

DREW SPANIEL (ICIT VISITING SCHOLAR, CARNEGIE MELLON UNIVERSITY)

COPYRIGHT © 2016 INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY – ALL RIGHTS RESERVED

ICIT Institute for Critical Infrastructure Technology

Expert research contributed by the following ICIT Fellows:

- Danyetta Magana (ICIT Fellow – President, Covenant Security Solutions)
- Igor Baikolov (ICIT Fellow – Chief Scientist, Securonix)
- Brian Contos (ICIT Fellow – Vice President & Chief Security Strategist, Securonix)
- John Menkhart (ICIT Fellow – Vice President, Federal, Securonix)
- George Kamis, (ICIT Fellow – CTO, Forcepoint Federal)
- Stacey Winn (ICIT Fellow - Senior Product Marketing Manager, Public Sector, Forcepoint)
- Thomas Boyden (ICIT Fellow – Managing Director, GRA Quantum)
- Kevin Chalker (ICIT Fellow – Founder & CEO, GRA Quantum)
- John Sabin (ICIT Fellow – Director of Network Security & Architecture, GRA Quantum)

Contents

Introduction:

2016 is the year ransomware will wreak havoc on America's critical infrastructure community. New attacks will become common while unattended vulnerabilities that were silently exploited in 2015 will enable invisible adversaries to capitalize upon positions that they have previously laid claim. "To Pay or Not to Pay", will be the question fueling heated debate in boardrooms across the Nation and abroad. Ransomware is less about technological sophistication and more about exploitation of the human element. Simply, it is a digital spin on a centuries old criminal tactic.

Early in the evolution of structured path systems, the most direct roadways that connected civilization were predominantly used by more privileged members of society and armies. Eventually those who could afford horses or carriages used the roads to travel and merchants used the roads to transfer their wares. Both parties had the money of their birth or labors. Consequently, the roadways became prey to travelling footpads referred to as highwaymen. Modern stories have romanticized these figures into gentlemen thieves who shouted slogans such as "your money or your life" prior to robbing their prey. The culprits were ransoming their prisoners with a choice. Either pay a "travelers fee" or suffer the consequences imposed by a masked adversary. Provided that the thief was honorable enough to allow his victims to live, authorities had a difficult time investigating the crimes and apprehending suspects because the adversaries were mobile. Consequently, culture had to adapt in response to the threat in order for any meaningful change to occur. Carriages began employing guards. People began travelling in groups and travelling at reasonable hours. As roadways became more traversed, highway crime decreased because the risk of getting caught began to outweigh the reward.

The internet is not unlike the aforementioned roadways. Initially, only a privileged few such as security researchers, the military, and a rich few, had access. Attackers could have made money from exploiting the sparse number of victims, but it was not until a greater influx of unwary victims began moving about that real profit could be realized. Ransomware threat actors adopt the highwayman mentality by threatening the lifeblood of their victims – information – and boldly offering an ultimatum. Despite recognition of the threat, the adversaries remain a numerous and nebulous bunch. Law enforcement has neither the time nor the resources to track down the culprits. Only a societal cybersecurity reformation in user awareness and training will deter the attackers.

Security firms like Kaspersky, Covenant Security Solutions, Forcepoint, GRA Quantum, Trend Micro and Securonix predict a dominant resurgence of ransomware attacks in 2016. Already, healthcare organizations, who were previously off-limits targets among ransomware threat actors, have been brutally and relentlessly targeted with inbound attacks intent on leveraging patient lives against the organization's checkbook. This shift may be largely backed by the more sophisticated Advanced Persistent Group Threat actors who are entering the stage because ransomware attacks are under-combated and highly profitable. According to Brian Contos, ICIT Fellow and VP & Chief Security Strategist at Securonix, attackers are pivoting to ransomware because "[It] is a volume business. It's simple, relatively anonymous and fast. Some people will pay, some will not pay, so what. With a wide enough set of targets there is enough upside for these types of attacks to generate a steady revenue stream." Ransomware has been

around since 1989 but its popularity decreased in favor of other malware because the number of internet enabled victim devices was not exceptionally beneficial to the adversary's profit margin. Now, with prevalence of mobile devices and the looming shadow of the internet of things, the potential threat landscape available to ransomware threat actors is too tantalizing a target to ignore. Danyetta Fleming Magana, ICIT Fellow and President and Founder of Covenant Security Solutions elaborates that "The world is a living and breathing digital planet, and over the past decade is has accelerated into a gorgeous global information field. The internet remains the single most common vehicle for billions of communications and business transactions on a daily basis. As new technology becomes available, more and more people and businesses will be connected to the internet in a variety of ways, making most of them prime candidates for a cyber-attack." Society now relies on constant access to the vast stores of data gathered from constant communication of people, devices, and sensors. Information security specialists and the technical controls that they implement must become adaptable, responsive, and resilient to combat emerging threats.

Ransomware cyber-criminals occupy a unique niche in the attack surface. Unlike hackers who attempt to exfiltrate or manipulate data where it is stored, processed, or in transmission, ransomware criminals only attempt to prevent access to the data. Aside from Advanced Persistent Threat groups, hackers, in general, worry about what they can steal. Ransomware criminals concern themselves with what they can disrupt. As harsh as it sounds, businesses can easily continue operations after a data breach. Customers and end users tend to be the long-term victims. The same cannot be said for an active ransomware attack. Business operations grind to a halt until the system is restored or replaced. Moreover, unlike traditional malware actors, ransomware criminals can achieve some profit from targeting any system: mobile devices, personal computers, industrial control systems, refrigerators, portable hard drives, etc. The majority of these devices are not secured in the slightest against a ransomware threat.

One reason that ransomware is so effective is that the cybersecurity field is not entirely prepared for its resurgence. Attacks are more successful when effective countermeasures are not in place. Information security systems exist to detect and mitigate threats, to prevent data modification, to question unusual behavior, etc. After it is on a system, ransomware bypasses many of these controls because it effectively acts as a security application. It denies access to data or encrypts the data. The only difference is that the owner of the system does not own the control. That is not to say that ransomware goes unchecked. Many security applications detect ransomware based on its activity or the signature of the variant. Security firms are consistently developing and releasing anti-ransomware applications and decryption tools in response to the threat. However, solutions do not always exist because some encryption is too difficult to break without the decryption key. For variants of ransomware that rely on types of strong asymmetric encryption that remain relatively unbreakable without the decryption key, victim response is sharply limited to pay the ransom or lose the data. No security vendor or law enforcement authority can help victims recover from these attacks.

As with any cyber-crime, law enforcement's response to ransomware is limited by their constraints (training, personnel, budget, etc.). The FBI leads the effort to prevent the spread of ransomware and respond to incidents. Their Internet Complaint Center allows victims to report ransomware attacks for investigation. In some cases, such as with Cryptolocker, the FBI has partnered with foreign law enforcement to neutralize a threat. Similarly, the Department of

Homeland Security (DHS) devotes resources to analyzing and responding to ransomware threats through U.S. CERT. Whenever an attack is reported to law enforcement, more information is gathered about the ransomware and the attacker's tools, tactics, and procedures. The information is aggregated and used in operations, such as Operation Tovar, to dismantle ransomware operations at the source and recover decryption keys from the captured servers. These large efforts are scarce because most ransomware attacks come from a distributed number of script kiddies and second-hand adversaries who purchased the malware. These more numerous attackers are one of the main differences between ransomware campaigns and APT attacks. There is no central command or primary adversary to focus countermeasures upon.

The other reason that anti-ransomware efforts are stunted is that the opposition is not unified in a response procedure. Most security vendors advise the public (who are not yet victims) to never pay the ransom and to focus on mitigation efforts instead. Mitigation is excellent so long as one negligent employee does not mistakenly compromise the entire system by opening an email. Afterwards, reality sets in. Victims have to make a very difficult decision. Either pay the ransom without knowledge of who receives that money and what further harm is done with it or to lose all of their data behind a layer of encryption. Larger agencies, such as the FBI and DHS have the resources and technical expertise to respond to cyber-attacks in a responsible and rational manner. Smaller law enforcement organizations, such as local police forces, might lack the resources necessary to respond appropriately. Consequently, on a few occasions, police forces have paid the ransom demand to free their systems and resume critical operations. Now, law organizations would only have paid the ransom after exhausting all other options. However, the decisions invoke a feeling that law enforcement bodies may not be the singular solution to the threat. Brian Contos remarks, "If they can't protect themselves adequately we shouldn't expect them to solve all our problems for us." Further, ransomware attacks, especially those against individual users, only demand a few hundred dollars at most from the victim. In comparison to the APT threats and other forms of cyber-crime costing millions of dollars per incident, it seems unlikely that agencies will devote significant resources to investigating individual attacks. From law enforcement's perspective, a home burglary results in greater loss than a singular ransomware attack. Executives at Forcepoint contends that, "The FBI, one of the leading law enforcement agencies tasked with pursuing cybercrimes, has stated that they will assist victims with traditional hacks. In cases of ransomware; however, they are working out the best response approach for victims of these types of attacks." In point of fact, in October 2015, Joseph Bonavolonta, the Boston-based head of the FBI's CYBER and Counterintelligence Program, said, "To be honest, we often advise people just to pay the ransom." In response to pressure from Senator Ron Wyden, the FBI clarified that its position was only to pay the ransom if mitigation steps failed and the only other option was to lose the files. More or less, victims' response amounts to reporting the incident to the FBI and hope that the threat actor is eventually caught. The victim will never recover their ransom (if they paid). Despite increased ransom demands, the response for businesses is not exceptionally better. According to Symantec, "Information security researchers, however, suggest that some cybercriminal extortionists have found $10,000 to be the sweet spot between what organizations are willing to pay and what law enforcements are reluctant to investigate." Again, this response may be justified in that the FBI and DHS also must handle significantly larger incidents. As the internet has no borders, in many cases these agencies do not even have the authority or capability to respond even if the attacker was a known entity.

Cyber-crime is a shared problem that the public and private sector need to collectively address. Ransomware, as a fraction of cyber-crime, is no different. Collaboration and collective cybersecurity improvement is the best strategy for mitigating the ransomware threat and reducing the impact of successful attacks. As initiatives to increase societal cybersecurity training and awareness improve, the attack surface and profitability of ransomware and other malware campaigns will decrease. Imagine how few malware attacks would succeed if no one opened their email! At the same time, public and private sector solutions to malware attacks will improve through shared information to address these problems at their source.

Origins of Ransomware:

The first ransomware, the AIDS trojan, was originally developed by biologist Joseph Popp. Popp passed 20,000 infected floppy disks out at the 1989 World Health Organization's AIDS conference. An accompanying leaflet warned that the software on the disk would "Adversely affect other program applications" and that "you will owe compensation and possible damages to PC Cyborg Corporation and your microcomputer will stop functioning normally." Nevertheless, users booted the disks and infected their own machines. To their credit, malware was relatively scarce at that time because significantly fewer users had access to computers. Similar to some modern ransomware, the AIDS trojan displayed a pretentious display message, chastising the mistakes of the user and eventually informing them to send $189 to PC Cyborg Corporation's P.O. box in Panama in order to free their system. The AIDS trojan counted the number of times that the computer was booted. When the counter reached 90, the malware would hide the directories and either encrypt or lock the files on the C drive. The AIDS trojan ultimately failed because it had a limited number of targets and because a decryption process was quickly developed. Strikingly, the two derivative ransomware variants, crypto ransomware and locker ransomware, follow the same tactics as Popp's 1989 campaign. Even more surprising is that the ransom has not significantly increased for the average user. Instead, global economics, the advent of the internet, and the reliance of technology has expanded the threat surface to include international organizations that are better resourced than the average user. Modern malware evolved to target people and organizations in economically developed nations because their reliance on technology allows it to succeed and to spread. Throughout the nineties, malware was predominantly used for pranks, vandalism, or to gain notoriety. Then, in the early millennium, the threat landscape shifted and attackers began to develop and deploy sophisticated malware to steal secret information, to inflict physical harm on remote systems, or to financially profit. Advanced Persistent Threats (APTs) usually developed for the former two categories while ransomware evolved under the latter motivation.

Ransomware reappeared around 2005 in the form of fraudulent applications, fake spyware removal tools (SpySheriff, etc.), and malicious "performance optimizer" applications (PerformanceOptimizer, RegistryCare, etc). These campaigns targeted Windows and Mac personal computers. Warnings of corrupt files and unused registry entries were used to panic home users into paying $30-90 for a license to a tool that often did nothing for the system. Also in 2006, a forerunner to modern crypto ransomware surfaced as the Trojan.Gpcoder family of malware. Gpcoder used weak symmetric encryption algorithms and was easily decrypted.

Nevertheless, by 2006, other attackers saw the potential of emulating Gpcoder. Trojan.Cryzip and Trojan.Archiveus appeared in 2006. According to Symantec, "Cryzip copied data files into individual password-protected archive files and then deleted the originals." Cryzip was disarmed when researchers discovered that the passcode was embedded in the trojan's code. Archiveus emulated Cryzip except that it asked victims to purchase medication from specific online pharmacies and submit the order identification number instead of asking for a cash transfer. Researchers believe that the developers of Archiveus earned commission from the online pharmacies to which victims were directed. After 2006, the attack surface shifted and caused malicious adversaries to develop ransomware in different ways.

In 2008, users began to recognize the threat landscape and the necessity of fundamental information security applications such as firewall and anti-virus applications. In response, attackers began to develop and deploy fake anti-virus programs, which mirrored the form and function of legitimate applications. The fraudulent programs performed illusory scans and claimed to have found a significant number of threats to the system. Victims were then prompted to either pay for a license or subscription or to pay a flat fee ($40-100) to "fix the problems." As awareness of the scams increased, users began to ignore the applications (both when prompted to download or after the fact) or to remove the applications altogether. The underlying problem in the attack vector was that it relied on user attention to initiate the download or respond to the advert and it depended on user panic and response to receive payment. After developing and deploying the application, the adversaries had no further leverage to entice users to pay.

By late 2008, Trojan.Ransom.C, the first locker ransomware emerged. Locker ransomware locks the user interface of the host machine, thereby disabling the victim's access to their system, often by disabling control of the mouse, some of the keyboard, and other system components. Locker ransomware spread like malware, often through malicious emails and driveby downloads. Ransom.C spoofed a Windows Security Center message, locked the host, and prompted victims to call a premium-rate phone number to reactivate a license for security software. Victims could not ignore locker ransomware. If they wanted to regain access to their system, then they had to either enter a payment voucher number or they had to wait for a vendor solution and learn to deploy it. Keep in mind, that mobile devices were not as capable or as prevalent in 2008 as they are now. Many victims did not have another system on which they could access the internet to search for a vendor solution, let alone have the know-how to decrypt their own systems. Consequently, attackers increased the ransom accompanying locker ransomware by 200-300% to $150-200 per infection.

By 2012, locker ransomware surpassed fake applications because it did not require conscious user action to infect a system. Locker ransomware campaigns became more blunt, telling users about the infection and about their inability to use the system unless a ransom was paid in the desired digital currency. Attackers optimized their social engineering endeavors and the display prompt to incite the most panic in victims in order to minimize victim's ability to react rationally. Attackers posed as law enforcement, claiming on the realistic prompt displayed on the locked screen that the system was locked because the users had pirated music, movies, or software or because the user had accessed illicit content such as child pornography, human trafficking sites, etc. Naïve victims believed that they were paying a fine instead of paying the licensing for a fake service or a ransom. The success and profitability of locker ransomware campaigns declined between 2012 and 2014 because calls to law enforcement and efforts of

security researchers increased the awareness of the scams and the availability of vendor solutions. Further, the prevalence of APT activity has resulted in an increased awareness of social engineering tactics. Rather than adopt more sophisticated tactics, ransomware groups began to shift their development to crypto ransomware.

Since 2013, attackers have been migrating back to crypto ransomware, similar to Popp's AIDS trojan and Ransomware.C, except with stronger encryption algorithms. Crypto ransomware evolution has accelerated over the few years since is reemergence because cyber-criminals have copied each other and adapted upon successful and failed strategies. Successful attackers typically rely on industry standards of encryption, such as RSA, triple Data Encryption Standard (3-DES), or the Advanced Encryption Standard (AES). Crypto ransomware is even more blunt than locker ransomware; often, presenting the intention of the malware and the demand for payment without pretense. Because the malware is more expensive to develop, more sophisticated, and more difficult to remove, attackers increased the average ransom to about $300 per infected host; however, targeted attacks against businesses and critical systems have led to significantly higher ransom demands. As of 2016, ransomware is mutating again to be more vicious and less predictable than in the past. This transition may be the result of adoption by more knowledgeable and ruthless adversaries, such as Advanced Persistent Threat groups.

Overview of Ransomware:

If you wanted to secure the valuables in a room, you could adopt one of two basic approaches. You could lock the valuables in container (a safe, a chest, etc.) so that only those with the key could access them or you could lock the door so that no one could access the room. Analogously, there are two types of ransomware, crypto ransomware and locker ransomware. Crypto ransomware encrypts personal data and files so that the victim cannot access those particular resources unless they pay the ransom. Locker ransomware prevents the victim from using the system at all by locking components or all of the system. Generally, ransomware is profitable because it leveraged society's digital lifestyle against itself. Ransomware locks the devices and data that some value more than their real world interactions. Ransomware depends on the majority of users reacting out of ignorance, fear, or frustration. The most internet dependent nations, United States, Japan, United Kingdom, Italy, Germany, and Russia, are also the most targeted by ransomware. The average ransom for either ransomware is around $300, as of 2015. One might notice that $300 might be significant for an individual; however, the average includes attacks on commercial businesses. In some cases, users might be charged less. In any case, $300 is less than half the price of a new laptop or mobile device; which is critical to the nature of the attack. Adversaries must keep the ransom proportional to the value of the infected host and the ability of the victim to pay. Cybercriminals choose which type of ransomware to deploy based on their skill set, the specifications of the target system, and their prediction of how each type might affect the target victim. In the former analogy, you might have decided that the best approach was to secure the valuables in a safe and then to lock the door. Luckily, a hybrid ransomware has not yet been popularized; however, with more sophisticated adversaries entering the arena, the development of more sophisticated or hybrid ransomware is only a matter of time.

Types of Ransomware:

Locker Ransomware:

Locker ransomware is typically spread through social engineering, phishing campaigns, and watering-hole sites. According to Symantec, about 36% of binary-based ransomware detected in 2014-2015 was locker ransomware. Computer lockers restrict user access to infected systems by either denying access to the user interface or by restricting the availability of computing resources. Certain capabilities, such as numeric keyboard functionality, might remain unlocked while the rest of the keys and the mouse are locked. This design increases user frustration while restricting user action to following the attacker's instructions. This type of ransomware is akin to the locked door in the earlier analogy. Locker ransomware usually leaves underlying files and systems unaffected; instead, it only restricts access to the interface. This design also means that locker ransomware can often be removed easily by restoring the system to a restore point or by deploying a commercial removal tool. In the previous analogy, this is akin to removing the door to access the contents of the room.

The contents of a room tend to remain unharmed if a door is either knocked down, unlocked, or if it is gingerly removed at the hinges. Because the computer locker can be removed without harm to the valuable data, locker campaigns depend on inciting panicked irrational thought in victims. In unsophisticated campaigns, a display page or a banner tells the user that the system will be unlocked if a fine (~$200) is payed, usually through payment vouchers. Victims can purchase vouchers from local stores, credit shops, or "loan outlets." Locker ransomware relies on vouchers because the victim cannot access a cryptocurrency market to purchase Bitcoins because the user interface is disabled.

More sophisticated schemes strongly incorporate social engineering into the scam to pressure the user into paying the fee. The tactic exploits the victim's trust in law enforcement, the need to obey the law, and the fear of the consequences, by invoking imagery and wording reminiscent of law enforcement. For example, a display page might claim that the FBI has locked the computer in suspicion of downloading child pornography or pirating movies. The page will offer to unlock the system if a fee is paid by inputting a numeric code (usually an account number or voucher) into the page or by calling a listed phone number. Any rational user would realize, at the very least that:

A. (Hopefully) The user was not engaging in the alleged illegal activity.
B. It makes no logical sense for the FBI to remotely lock down a computer instead of just showing up and arresting a suspect.
C. The FBI (or whomever) would not accept a "fee" to ignore due process.

Nevertheless, locker ransomware has proven a profitable attack vector, likely because of the victim demographics of its infection vectors. How many senior citizens, who have flawlessly obeyed the law for their entire lives, will input their credit card or financial information into a page telling them that a law enforcement organization will arrest them if they do not immediately pay the fine? Even if they understand that the ransomware is malware, how many sheepish teenagers would use their parent's credit cards to pay the fine to not have to explain that they how they infected their computer on an adult web site?

If the victim was actually engaged in the illicit activity described on the ransom demand, then they might be more likely to pay it, even if they suspect that it is a scam. For instance, many young people visit adult websites and digital piracy websites, through which locker ransomware is known to be distributed. Because the victim already feels guilty or ashamed, they are less likely to think rationally or to seek outside help. Here, the threat actors are leveraging human nature against the victim to achieve their desired outcome. As knowledge of locker ransomware increased, the pool of victims and the profitability diminished.

Attackers abandoned locker ransomware in favor of its more robust counterpart, crypto ransomware. Locker variants are still developed, but they are less numerous than crypto ransomware families. However, 2016 may be the year that locker ransomware reemerges because locker ransomware can infect emerging technology such as mobile phones, wearable devices, and systems connected to the "internet of things". Unlike personal computers, these alternative devices might lack system restore capabilities. User options might be limited to: pay the ransom, pay for a vendor tool to remove the ransomware and then figure out how to deploy and operate the tool, or to restore the device to factory default (if the option remains unlocked). Even in large campaigns, adversaries tend to scale the ransom to the victim demographics' ability to pay. What if the ransom to unlock an IPhone or smart watch is significantly less than cost of the vendor solution? What if the ransom is low enough (say $0.99) that users are willing to pay the ransom because it is more convenient than finding a software solution and then learning how to deploy it on the locked device. Those readers with social media may be familiar with the Facebook scams (offering cheap sunglasses, life-hacks, etc.) that appear when a profile is compromised. The victim's profile propogated the malicious attachment or url to their contacts by either posting on their page or by privately messaging their friends. Now, imagine if locker ransomware spread in the same fashion, texting a malicious link to every device in the victim's contact book. Even a low ransom (less than $0.99) could be extremely profitable if the ransomware is propagated from every infected device.

Crypto Ransomware:

Instead of restricting user action by denying access to the user interface, Crypto ransomware targets the data and filesystems on the device. The critical system files and functionality tend to remain unaffected. The victim can use the computer to do anything except access the encrypted files. Crypto ransomware often includes a time limit, after which the decryption key may or may not actually be permanently deleted if the victim does not pay the ransom on time. People do not think rationally under time limits; as before, the cyber-criminals are compensating for a lack of technical sophistication by leveraging human behavior against the victim. The victim is subject to the anxiety of the ticking clock, the fear of the consequences of making the wrong decision, and the fear of regret if the data is lost forever.

In 2014-2015, crypto ransomware accounted for 64% of the binary based samples of ransomware detected by Symantec. Attackers usually ask for ~$300 USD in bitcoins to unlock the encrypted files. Unlike locker ransomware, crypto ransomware still allows users to access the internet to purchase cryptocurrencies. Some variants of crypto ransomware even provide users with a site to purchase Bitcoins and articles explaining the currency. Interestingly, as Law

Enforcement Agencies and security researchers buy out digital currencies, such as Bitcoins, average users have to pay the price of inflation of the decreased commodity.

Crypto ransomware did not popularize until 2013 because attackers failed to realize that successful crypto ransomware attacks rely on current strong encryption algorithms and proper management of the accompanying cryptographic key. Prior to that, variants failed to be more profitable than locker ransomware because attackers stored the key on the host or within the malware. For some variants, the key was even the same across all samples, which means that once one person had unlocked their system, they could just post the key for any other victim to use to unlock their system.

According to information security researchers at Symantec, the current crypto ransomware threat landscape is still fragmented into new entrants into the market and mature criminal groups. Both types of attackers try to employ industry-standard encryption algorithms, such as RSA, Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) with a suitably large key in their ransomware; however, entrants tend to lack technical skills and the operational tactics, techniques, and procedures associated with mature groups. Entrants often store encryption keys in the ransomware or they fail to fully disable a system to prevent user action. In contrast, mature cyber criminals generate a unique asymmetric key for each infected system and they wipe the session key from memory when they are finished with it. These dominant cybercriminals combine strong public/private encryption with their established operational procedures to limit victim response to paying the ransom or losing their data. Entrants operate to make a profit from naïve victims, while mature cyber criminals operate to hold hostage systems belonging to users and businesses, and to not be identified by law enforcement. To this end, the community relies on Tor, proxies, and crypto-currencies, such as bitcoins to remain anonymous.

In this digital age, the vast majority of personnel and people digitally store data vital to their profession and personal life. Only a small percent of users regularly backup all of their essential data or all of their essential systems. Crypto ransomware is often spread through Tor, botnets, or other malware. Crypto ransomware is as simple as weaponizing strong encryption against victims to deny them access to those files. After the initial infection, the malware silently identifies and encrypts valuable files. Only after access to target files has been restricted does the ransomware ask the user for a fee to access their files. Without the decryption key held by the attackers, or in some cases, a vendor decryption solution, the user loses access to the encrypted files. Even if the user regularly backs up their data, the crypto ransomware might still be effective if the user does not have the time to revert to the backup or if the user has not backed up their data frequently enough. For example, a medical organization might be a target if they need real time access to their data while a college student might be a target if they have not backed up the term paper that they are rushing to finish for the following morning. Crypto ransomware incites panic in users, but it relies more on their desperation. Because different user worry about different things (documents, photos, servers, etc.) and because cryptographic algorithms are numerous, a plethora of crypto ransom variants target the attack surface. Nevertheless, due to a lack of personal sophistication, the majority of threat actors rely upon or adapt a few successful variants.

Active Examples of Crypto ransomware:

Locky:

On February 5, 2016, medical systems belonging to Hollywood Presbyterian Medical Center were infected with the Locky ransomware. Healthcare data remained unaffected but, computers essential to laboratory work, CT scans, emergency room systems, and pharmacy operations were infected. The email system was taken down, but it remains unclear whether the system was infected or if the system was taken down to preserve indicators of compromise or to prevent further phishing emails. While media outlets reported that the adversary demanded a ransom of 9000 Bitcoins ($3.6 million), President and CEO of HPMC Allen Stefanek said that the accounts were inaccurate. After almost two weeks, the hospital paid a ransom of 40 Bitcoins ($17,000) to unlock their machines, despite ample assistance from the FBI and LAPD, because paying the ransom was the quickest and most efficient way to restore their systems. Stefanek does not believe that the hospital was specifically targeted. He argues that the attack was the result of a random malicious email. In contrast to this assertion, the attackers did not demand the typical user ransom of $210-420.

The novel Locky ransomware is not any more sophisticated than other ransomware applications, but it is rapidly spreading to victim systems. Forbes claims that the Locky ransomware is infecting approximately 90,000 systems per day and that it typically asks users for 0.5-1 Bitcoin (~$420) to unlock their systems. Locky encrypts files with RSA-2048 and AES-128 ciphers. Victims are presented with links to payment landing pages and instructions to install Tor. Security firm Proofpoint asserts that Locky was developed and deployed by the Dridex criminal organization. The Dridex criminal group is the most prominent operating banking malware. Locky is disseminated through spam emails containing Microsoft Word attachments. Each binary of Locky ransomware is reportedly uniquely hashed; consequently, signature based detection is nigh impossible. After infection, the malware deletes backup shadow copies of the operating system. Encrypted files are renamed with the .locky extension and the victim is presented with the ransom demand. Palo Alto Networks, who also connected Locky to Dridex, believes that the group has already raised several hundred thousand dollars from Locky ransoms.

TeslaCrypt/ EccKrypt:

TeslaCrypt infects systems through the Angler exploit kit, which leverages vulnerabilities in Adobe Flash (such as CVE-2015-0311). Silverlight and Internet Explorer may be exploited in absence of Adobe Flash. Angler is injected from an iframe on a compromised website. The victim is redirected to a landing page, where anti-virtual machine checks, antivirus assessments, and host analysis tools are systematically run. If all the checks succeed, then the Flash exploit is used to download the ransomware payload into the victim's temp folder. The Xtea algorithm is used to decode the payload and the ransomware is written to disk.

The TeslaCrypt binary is compiled in Visual C++. The ransomware code is encoded within the binary. After the code is decrypted into memory, TeslaCrypt overwrites the MZ binary

onto itself. The malware copies itself to %appdata%, where it also stores a SHA-256 key (key.dat) and a log file listing the files found through directory enumeration and encrypted. Encypted files feature the additional extension names of .encrypted, .ecc, .ezz, .exx, and recently, .mp3. The malware runs a few threads: a file encryption thread, a thread to monitor and terminate .exe, .msconfig, .regedit, .procexp, and .taskmgr processes, a thread to delete backup shadow files using vssadmin.exe, and a thread to contact the command and control server to communicate the sha-256 value of the key generated from key.dat, the Bitcoin address, the number of files encrypted, and the victim IP address. Although it resembles Crytolocker in design and appearance, they do not share source code. After infection, victims are presented with a pop-up window informing them that the files have been encrypted and directing them to the TeslaCrypt website, directly or through a Tor2Web proxy.

Initially, TeslaCrypt used symmetric encryption; however, after researchers from Cisco's Talos Group released a decryption tool (the Talos TeslaCrypt Decryption tool), the authors reconfigured TeslaCrypt to use asymmetric AES encryption. By late 2015, Kaspersky labs had released another decryption tool, the TeslaCrypt Decryptor. By January 2016, the threat actor had remedied the flaw in their malware and released a third version that appends the .mp3 extension to encrypted files.

TeslaCrypt originally targeted 185 file types related to 40 computer games (Call of Duty, Skyrim, Minecraft, etc.) on Windows systems. The malware capitalizes on how much victims' value the time spent in artificial realities and the intangible assets collected there. Newer variants also encrypt Word, PDF, and JPEG files. Overall, the ransomware is particularly devastating to college aged young adults. Victims are prompted to pay a ransom of ~$500 (in Bitcoins, PaySafeCard, or Ukash). Victims may decrypt a single file for free as a show of good faith.

Cryptolocker:

Cryptolocker is a crypto ransomware trojan that began infecting Windows systems in September 2013 through the Gameover ZeuS botnet, and encrypting the host data with RSA public-key encryption. The private key needed to decrypt the data was stored in the malware's command and control servers. The ransomware also spread as a malicious email attachment (a .ZIP file containing an executable with a PDF icon). Cryptolocker installs in the user profile folder and adds a key to the system registry so that it runs at startup. Next, it connects to one of its C2 servers and generates a 2048-bit RSA key pair, stores the private key on the server, and sends the public key back to the victim machine. The trojan encrypts document, picture, and CAD files on the local hard-drives and mapped network drives with the public key and logs each encrypted file as a registry key.

The vast majority of victim systems were located in the United States and Great Britain. Victims were presented with the demand that unless a 0.3-2 Bitcoin or cash voucher payment was made within 72-100 hours, the private key would be deleted and the data would be forever encrypted. Sometimes, if payment was not received by the deadline, the attackers would offer a new deadline at a higher price, marketing it as an online removal service. In November 2013, this after-the-fact service was offered as a stand-alone website. The site claimed that the private

key would be sent to the victim within 24 hours of a 10 Bitcoin payment. Even if the ransom was paid, some attackers did not decrypt the files. Cryptolocker can be removed from infected systems, but files still cannot be decrypted without the private key.

Cryptolocker and the ZeuS botnet that it relied upon were taken down in the May 2014 Operation Tovar. Afterward, the private keys saved on the servers were converted into an online file recovery tool. Overall, in its 6-month operation, attackers used Cryptolocker to extort over $3 million from victims. Security researchers estimates that only 1.3-3% of victims chose to pay. As a result of its success, numerous rebranded variants appeared on the market.

Cryptowall/ CryptoDefense/CryptorBit:

The Cryptowall family of ransomware first appeared in early 2014 and became popular after Operation Torvar dismantled the Cryptolocker network. Cryptolocker is spread through various exploit kits, spam emails (with attached RAR files that contain CHM files), and malvertising pages. When the malware is delivered, the binary copies itself to the %temp% folder. It then launches a new instance of the explorer.exe process, injects the unpacked Cryptowall binary, and executes the injected code. The malware uses the vssadmin.exe tool to delete shadow copies of files. Afterwards, it launches the svchost.exe process with user privilege and injects and executes its code in the process. Next, It tries to connect to the I2P proxies to find a live command and control server using a hash value that is created by taking a randomly generated number followed by a unique identification value. This is generated using system-specific information such as computer name, OS version, processor type, volume serial number, and other identifiers. The server replies with a unique public key and delivers ransom notes in the language based on geolocation of the machine IP address. Notes are placed in all directories where victim files are encrypted and then Internet Explorer is launched with a display page of the ransom note.

Current variants of the malware (such as Cryptowall 3.0) use I2P network proxies to communicate with their C2 infrastructure and they use the Tor network to collect Bitcoin payments from victims. Initial variants encrypted victim files with RSA public-key encryption; however, the malware has now (Cryptowall 3.0) evolved to use the AES 256 algorithm. Further, the AES decryption key is stored on the C2 server and encrypted with a unique public key. The malware includes a service to decrypt a few randomly selected files as a demonstration that the rest of the files will be decrypted if the 1 Bitcoin ransom is paid. Unlike Cryptolocker, the Cryptowall malware targets Windows systems globally; though, the United States (13%), Great Britain (7%), the Netherlands (7%), and Germany (6%) were the most affected.

CTB-Locker:

The "Curve-Tor-Bitcoin-Locker" (CTB-Locker) is a PHP based trojan that was publicly analyzed by security researcher Kafeine in mid-2014. CTB Locker is essentially a ransomware as a service (RaaS), where the attackers outsource the spread of the malware to a number of script kiddies and botnet operators (often referred to as affiliates) for a share of the paid ransoms. This RaaS model was proven and popularized by fake antivirus, click fraud schemes, and other types of malware. Though CTB-Locker remains the most abundant RaaS, other ransomware has begun to adopt the distribution channel. In CTB-Locker's model, affiliates pay the operators a monthly fee to use the malware. In other models, the originator receives a small percentage of each ransom.

Due to the affiliate model, CTB-Locker uses every infection vector imaginable. Mostly, attackers rely on exploit kits (Rig, Nuclear, etc.) and malicious email campaigns. The latter campaigns often use the Dalexis or Elenoocka downloader to deliver the malware. Dalexis is an auto-executable attached to emails as a cab file. Elenoocka and other downloaders are auto-executables hidden in ZIP or RAR archives. CTB-Locker is also available in English, French, German, Spanish, Latvian, Dutch, and Italian to accommodate affiliates and targets from most American and European countries.

The downloader drops CTB-Locker into the temp directory and it creates a scheduled task to enable reboot persistence. The file system is iterated and files that match CTB-Locker's extension list are enumerated for encryption. The background image of the system is changed and the ransom message and a clickable interface overlay the center of the screen. Victims are told that they have 96 hours to pay the ransom (variably determined by the affiliate) and that any attempt to remove the malware will result in destruction of the decryption key.

CTB-Locker uses a combination of symmetric and asymmetric encryption to restrict victims' access to their files. Rather than use RSA, which is based on prime number factorization, like most ransomware, files targeted by CTB-Locker are encrypted with AES and with Elliptic Curve Cryptography (ECC). ECC is a form of public key cryptography based on elliptic curves over finite fields and the strength of the algorithm derives from the elliptic curve discrete algorithm problem. ECC can achieve similar security levels to RSA with a much smaller key. For instance, a 256-bit ECC key provides equivalent security to a 3072-bit RSA key. The malware uses AES to encrypt the files, and then the means to decrypt the files is encrypted with an ECC public key. Consequently, only the attackers, who possess the ECC private key, can decrypt the files.

CTB-Locker is unique among ransomware in that it does not require internet access or contact with its C2 infrastructure to begin encrypting files. Network connection is not necessary until the victim attempts to decrypt their files. Payment communication is carried out over Tor and proxy sites that relay Tor traffic. After the ransom is paid, a decryption block is sent from the C2 server to the victim host.

In February 2016, attackers began to use the CTB-Locker to encrypt websites hosted by Wordpress. This variant of CTB-Locker is referred to as Critroni. The attackers hack an insecure website and replace its index.php file or index.html file with different files that encrypt the site's data with AES-256 encryption. Afterwards, a ransom message is displayed on the homepage. The prompt provides instructions for how to purchase Bitcoins and typically demands 0.4 Bitcoins. In the first week of the attack, around a hundred sites were infected; though no major domains were infected. The victims tended towards those who relied on outdated versions or vulnerable plugins. Even though the ransomware did not infect major sites, the mutation of the malware should be heeded as an indication that the overall ransomware threat is ramping up. Critroni may have just been an experiment or an innovative script kiddie. At the moment, users who navigate to the victim site see the same ransom instructions as the administrator. Consider the implications if the attackers figured out a way to spread the ransomware onto each visitors' machine. The impact of the malware and its profitability would increase significantly.

Hybrid Ransomware:

One of the prevalent malware mitigation strategies is a layered depth. It stands to reason that in accordance with the concept of mutual escalation, attackers will begin to "attack in layers." This behavior already occurs in APT campaigns and in some ransomware attacks, where for instance, the adversary launches a DDoS attack alongside a more concerning attack. In terms of ransomware, it will be interesting to see if locker ransomware resurges with crypto-ransomware running behind the scenes. Layering the types seems unnecessary now, because victims often pay and because neither security researchers nor law enforcement can break the strong encryption used; however, if either of those cultures change, then locker ransomware, which prevents most user action, may return with controls borrowed from crypto ransomware.

Delivery Channels:

Ransomware follows the same distribution and infection vectors as traditional malware. The primary difference is that ransomware threat actors often lack the sophistication to breach modern networks. These criminals either rely on more experienced members or they pay for a malware installation service, which charges by the number of installations.

Traffic distribution system (TDS):

Traffic distribution services redirect web traffic to a site hosting an exploit kit. Often, traffic is pulled from sites hosting adult content, video streaming services, or media piracy sites. Some ransomware groups, especially criminals who purchase their malware instead of developing it themselves, may hire a TDS to spread their ransomware. If the host is vulnerable to

the exploit kit on the landing page, then the malware is downloaded onto the system as a drive-by-download.

Malvertisement:

As with a TDS, a malicious advertisement can redirect users from an innocuous site to a malicious landing page. Malvertisements may appear legitimate and can even appear on trusted sites if the administrator is fooled into accepting the ad provider or if the site is compromised. Malicious threat actors can purchase traffic from malvertisement services. Redirected victims can be purchased according to geographic location, time of day, visited site, and a number of other factors.

Phishing Emails:

As with most malware campaigns, phishing emails and spam email are the primary delivery method of malicious content into a network because users are culturally trained to open emails and to click on attachments and links. Even with training and awareness programs, most organization find it difficult to reduce successful spear phishing attempts to less than 15 percent of personnel. Attackers only need a single user within an organization to click on the malicious link or attachment in order to compromise the network. The larger the organization, the greater the risk of infection through malicious email.

Botnets are used to send spam emails or tailored phishing emails at random or to personnel within an organization. These botnets and email services are a criminal enterprise unto themselves. Botnets and spam clients are comparatively cheap. It is reasonable to assume that many who purchase their ransomware may also purchase botnets and email spammers. According to Symantec, ransomware emails tend to masquerade as mail delivery notifications, as energy bills, as resumes, as notifications from law enforcement and as tax returns.

Downloaders:

Malware is delivered onto systems through stages of downloaders to minimize the likelihood of signature based detection. Ransomware criminals pay other threat actors to install their ransomware onto already infected machines. The other threat actor offers the service because the infected machine may have been an accidental infection, may be a stepping stone infection, or may no longer contain valuable data. If the ransomware threat actor actually decrypts the system, then the ransomware infection could draw attention to the other compromise; however, it could just as easily mask the other malware by focusing the user's attention on certain infected systems. Users may not suspect that there is a deeper infection after they remove the ransomware. Moreover, the ransomware infection provides the initial threat actor an easy revenue stream, even if the system was not valuable. Botnet operators are

especially fond of offering these services to ransomware and malware authors as a means of drawing quick revenue from the easily constructed botnet. Malware groups who conduct widespread phishing campaigns and watering-hole attacks may be equally willing to sell access to the systems that they compromised by accident.

Social Engineering:

Popp's AIDS trojan relied on social engineering, and human ignorance, to generate profit. The only systems infected belonged to users who ignored the plainly worded warning pamphlet. These victims were either brash or curious. In 1989, a decent percent of the 20,000 victims probably had no choice but to pay the ransom. Older ransomware relied on social engineering and illusory pressure to entice users into infecting their own machines. Fake anti-virus applications told users that their computer was at risk of numerous debilitating viruses while performance optimizers persuaded users that their system could achieve better results. Even locker ransomware that appears as a malvertisement on other sites depends on users clicking on the prompt to initiate installation.

Self-Propagation:

Select ransomware variants contain the functionality to self-propagate through a network in a fashion similar to other malware. The majority of these samples are crypto ransomware because locker ransomware is not exceptionally popular at the moment; however, Android variants of crypto ransomware and locker ransomware have appeared in the wild. These mobile applications are either downloaded from an app store or they spread through an initial victim's contact book via SMS messages to other systems. One such variant targeting Windows is the Ransomlock (W32.Ransomlock.AO) screen locker. With the emergence of the internet of things, self-propagating ransomware is likely how the malware will evolve in the future because the greatest number of interconnected devices can be infected for the minimal amount of applied effort. However, this evolution is not without its own problems. As Symantec observes, ransomware that is continuously spreading throughout the network deters victims from paying the ransom because the system will just be infected again. Criminals will have to develop a mechanism to check whether or not a system has already been infected (such as a certificate) and a mechanism to decrypt all systems belonging to a victim who has paid the ransom; otherwise, the entire business model will be upended. This could be accomplished by either simultaneously removing or deactivating the ransomware from all of the victim's systems.

Ransomware as a Service (RaaS):

When malware attacks succeed, less technical criminals try to capitalize on the threat landscape. Sophisticated threat actors can gain notoriety and additional revenue by outsourcing their malware to these script kiddies. These opportunities are also attractive to botnet operators

who do not know how to exploit their zombies. Ransomware is starting to follow the trend of other malware, in the form of ransomware as a service, through which script kiddies can use the ransomware developed by experienced criminals to exploit victims. The applications are designed to be deployed by practically anyone. The script kiddie downloads the client for free or a nominal fee, sets the ransom and payment deadline, and then attempts to trick victims to infect their own systems through phishing emails or watering-hole sites. If the victim pays the ransom, then the original creator receives a fee (5-20%) and the script kiddie receives the rest.

The Reveton ransomware may have been the progenitor of the ransomware as a service model. In 2012, the Reveton actors paid sites to spread the malware. The first free tool was the Tox ransomware, which allowed users to keep 95% of the ransom. The tool, created by a teen hacker by the same name, infected over 1500 systems and demanded a ransom of $50-200. Fearing law enforcement attention, Tox sold his service, the source code, the web domain, a database of infected systems, and the decryption keys, to an unnamed buyer for $5000. RaaS may not always be profitable. In interviews with Business Insider and Motherboard, attacker Jeiphoos admitted that his November 2015 Encyptor RaaS, had made no money, despite infecting around 300 devices. Brian Krebs comments that "Many [RaaS authors] will try but few will profit reliably (and much at that) for any period of time," he continues that those that succeed will be the ones that offer good "customer service" to script kiddies and victims alike.

In theory, it is a mutually beneficial relationship between the actual threat actor and the script kiddie because both parties generate a profit with minimal additional effort. The script kiddies can utilize a tool that they could not have created and the threat actor can focus their time on developing new variants. However, in practice, the threat actor can suffer if the script kiddie does not decrypt the systems of victims who pay the ransom because news will spread and less victims will pay in the future. If the malware becomes too ubiquitous, then security researchers will develop a decryption tool faster and the ransomware will be rendered prematurely obsolete.

Targets for Ransomware:

Unlike APT campaigns, financially motivated cyber threats, like ransomware campaigns, do not care about the individual target. Instead, they target the subset of society believed to be most likely to pay the ransom demand. Ransomware is often spread in mass in the hopes that a portion of the users will pay. Ransomware, whether purchased or developed, is relatively cheap in comparison to APT malware. Delivery is virtually free. Further, if the attacker does not intend to unlock the user system after the ransom is paid, then there is virtually no need to continuously dedicate resources to an individual attack. A small team can easily infect and ransom millions of systems. The attackers only need a few users per million of targets to pay the ransom for the campaign to be successful.

Financially motivated adversaries tend to target the lowest hanging fruit. Because different threat actors have different perceptions of the market and because the willingness to pay ransoms decreases as victim markets become over-saturated and desensitized, the targets of ransomware change according to victim awareness and willingness to pay. Some adversaries

may even widen their delivery vector to encompass multiple demographics to account for market shifts.

The Average User:

In cybersecurity, people are considered the weakest link. They are also both the most abundant resource and the most susceptible target. Individual users who are easily pressured or who are not fluent in technical solutions to ransomware are the most viable targets. As previously mentioned, this tends to include the elderly and teenagers; however, any age group is a viable target if the attacker effectively incites enough panic or fear into the victim to influence them into the illogical decision to pay the ransom. Attackers can increase this pressure by including a timer, after which the user cannot pay to recover their system or data. Even if the user knows that there is a freely available solution, such as the Tesla decoder (which deciphers the TeslaCrypt crypto ransomware), the user may not understand how to employ the solution and may opt to pay the ransom out of frustration and perceived helplessness.

Individual users are targeted because in the digital era, much of our knowledge, work, and personally valuable objects (photos, music, etc.) are stored on whatever internet enabled device we rely on. The majority of users do not consistently backup their data or follow basic cyber hygiene thoroughly enough to mitigate the impact of a ransomware attack. Symantec claims "twenty-five percent of home users did not do any backups at all. Fifty-five percent backed up some files. In terms of backup frequency, only 25 percent of users backed up files once a week. The rest only made backups once a month or even less frequently than that." Ransomware attackers depend on hitting users between backups. Even if the interval is only one day, the work from that day of labor might be worth a few hundred dollars. Further, some of the more complex variants of ransomware delete local backups, remove system restore points, and spread to any connected device (such as a backup drive). Since crypto ransomware in particular remains in the background until target files are already encrypted, external backups might be compromised before the ransom demands are even made.

Businesses:

The American economy is literally built upon intangible goods and services such as information and knowledge. Businesses large and small rely on their systems and the information contained within in order to conduct their day-to-day operations. Very small businesses, such as a mom-and-pop coffee shop might be able to process transactions without access to their POS system, but Starbucks certainly cannot. Businesses are the prime targets of ransomware because their systems are the most likely to house valuable databases, containing sensitive data, important documents, and other information; meanwhile, their systems are the least likely to be adequately secured. Businesses have the greatest access to liquid capital. Further, for many organizations, system downtime equates to loss of income and reputation. Consequently, they are the most likely to pay the ransom in order to resume operations.

The private sector is a prime target because the number of businesses to target is only less numerous than the number of personnel at each business who can be individually targeted with phishing emails and watering-hole attacks. Many organizations have redundancy systems and backup servers in case an attack succeeds; however, an equal or greater number of businesses have neither. It is unrealistic to expect a small to medium size business to have the same infrastructure as a larger business. Sometimes, extra systems such as backup and redundancy servers are simply outside of their budget. Even if the victim organization has the necessary systems, crypto ransomware has evolved specifically to account for complex victim networks. Modern crypto ransomware maps networks, enumerates drives, and spreads onto as many systems as it can before it activates. As a result, numerous systems, including the backup and redundancy systems, may be infected. Not even a large organization can ignore half their systems going offline. The organization will have to react through remediation, surrender, or allowing the loss of the data. Many organizations cannot survive the loss of essential data for an extended period. Without adequate backups, business continuity may be impossible and customers or end users may be affected. Even with a backup server and business continuity plan, a business may be susceptible to attack. Crypto ransomware can target the corporate network or individual user systems and then spread throughout the network. Sophisticated variants, (PHP.ransomware, Tesla Crypt, etc.) may remain silent on the network while they encrypt databases or files before or during backup operations. Further, many organizations have never conducted live testing of their business continuity or disaster recovery plans. What if the reversion time is unacceptable? What if a backup system is no longer operational due to a system flaw? Attackers know of these operational weaknesses. Attackers systematically target these vulnerabilities in the actual business when they make their ransom demands.

Law Enforcement and Government Agencies:

Law Enforcement and Federal Agencies are often targeted with malware attacks in response to their efforts to investigate and apprehend cyber criminals. While large organizations such as the FBI, DHS, and other federal agencies have resources which increase their resiliency, smaller organizations, such as numerous police stations and state/local government offices, have been the victims of ransomware attacks in recent years. Typically, such as the February 2016 ransomware attacks against the police of the city of Durham North Carolina, the authorities ignore this advice, ignore the demand, and revert their system to a recent backup. This decision can have consequences. In late January 2016, 300 systems belonging to the Lincolnshire County Council were infected with ransomware and had to be taken offline in response. The systems are returning to operation in March 2016. Similarly, on March 4, 2016, 6000 files belonging to the North Dorset District Council had been encrypted by ransomware. The infection had been limited by security systems in place and the council has declined to pay the 1 Bitcoin ransom. Still, in other instances, the authorities have paid the ransom in order to resume critical operations. On February 25, 2016 the systems belonging to the Melrose Police Department of Massachusetts were infected with ransomware from a malicious email that was sent to the entire department. The malware encrypted a software tool called TriTech, which police officers use for computer aided dispatch and as a record management system during patrol. The program also enables law enforcement officers to log incident reports. The department paid the 1 Bitcoin ransom on February 27, 2016.

Emergency Services:

DHS and the Multi-State Information Sharing and Analysis Center warn that cyber-attacks against law enforcement, fire departments, and other emergency services are increasing in frequency. Targets such as these, for whom lost access to systems could cost lives, are juicy targets for ransomware threat actors.

Healthcare Organizations:

The healthcare sector was not a traditional target for ransomware attacks. One theory is that attackers did not target systems that jeopardized lives. Recently, that mentality has changed for at least the group operating the Locky ransomware. Around February 5, 2016, systems belonging to the Hollywood Presbyterian Hospital Medical Center was infected with the Locky ransomware. After ten days, the administration paid attackers 40 Bitcoins ($17,000) to release the systems. Later that week, five computers belonging to the Los Angeles County health department were infected with a ransomware variant. The health department refuses to pay the ransom and will restore its systems from backups. Similarly, two hospitals in Germany were infected with ransomware at roughly the same time as Hollywood Presbyterian Medical Center. Both are restoring their systems from backup systems.

Educational Institutions:

Ransomware threat actors may target administrative systems at lower and higher education institutions. General education systems are more likely to be disrupted by a ransomware attack; though, colleges and universities are more likely to have funds sufficient to pay a sizable ransom. In February 2016, at least 2 primary school districts were targeted with crypto ransomware. Horry County school district in South Carolina paid $8500 to decrypt their 25 servers after an FBI investigation yielded no alternative action. The Oxford County school district in Oxford Mississippi was also infected around the same time. Oxford systems are operational again at the time of this writing, though it remains undisclosed whether the situation was resolved by paying the ransom or by reverting the system from backup servers.

Religious Organizations:

Religious organizations' networks are often infected with malware because their personnel are not trained to ignore phishing emails and they are unaware of cyber-threats. In late February 2016, two Churches were targeted with ransomware attacks: the Community of Christ Church in Hillsboro Oregon and St.Paul's Lutheran Church in Sioux City, Iowa. The former was

infected with the Locky variant of crypto ransomware that recently infected the Hollywood Presbyterian Hospital. The Community of Christ Church paid $570 to free their system. Information about the latter incident is more scarce, except that the church declined to pay the ransom.

Financial Institutions:

The banking and finance sector is the frequent target of botnet schemes such as the Dyre, Dridex, and Ramnit botnets. Ransomware often spreads through established bonnets. Further, the Locky ransomware is believed to have been developed or deployed by the Dridex group. Consequently, financial institutions are likely the next major sector to be targeted by ransomware, if their systems have not been infected already.

On February 17, 2016, attackers behind the TeslaCrypt ransomware issued spam emails masquerading as Visa Total Rewards emails. A malicious attachment, claiming to be a white paper containing more information about rewards and benefits, was used to deploy a JavaScript downloader that delivered the TeslaCrypt malware onto victim hosts. Ransoms of 1.2 Bitcoins within 160 hours were demanded of victims. If victims do not pay within the time frame, then the ransom doubles. The United Kingdom (40%) and the United States (36%) were the most targeted.

Target Systems:

Any system valuable to a user is a valuable target for ransomware because the profitability of the attack vector derives from inconveniencing the victim. As technology becomes more ubiquitous and society's dependence on constant access to information becomes more ingrained, the threat landscape of ransomware increases. According to Symantec, the most frequent targets of ransomware are personal computers, mobile devices, and servers and databases. Additionally, IoT devices, and critical systems (PoS terminals, medical devices, etc) are tantalizing targets.

Personal computers:

Personal computers are the current primary target of ransomware campaigns because they are numerous and easily compromised. Users tend to have poor cyber-hygiene and many users can be coerced into infecting their own systems through social engineering. Ransomware actors make less per victim than in attacks on organizations, but average users are more numerous and in general, they are more likely to pay the ransom out of frustration or lack of viable options. Ransomware variants are designed to target specific operating systems because it must leverage system API hooks to restrict victim access to the system. Additionally, some variants utilize native encryption libraries and APIs to perform the encryption and decryption of user data. Most

target Windows, but variants that target Linux, Mac, and Android are also developed. Symantec comments that like malware, most variants target Windows operating systems because Windows systems account for "around 89 percent of the OS share for desktop computers, with Mac OS X and Linux making up the rest." At least one system agnostic variant, the Browlock Trojan (Trojan.Ransomlock.AG), exists. Browlock executes as Javasccript from a web browser. Its goal is to target the segment of the victim pool not saturated with other attackers.

Mobile devices:

We live in the age of constant access to information. When you hear stories of information restriction out of places like North Korea, you probably have some knee-jerk thoughts in reaction to how a people can exist without open access to the internet. According to the PEW Research Center, as of 2016, 72 percent of American adults owned a smart phone. The global median, as of spring 2015, is about 43 percent. Those figures are further increased if one includes tablet devices, mobile game consoles, and other internet-enabled devices. For the most part, sensitive data is not stored on mobile devices. The value is the device themselves and the inconvenience suggested to most users should they choose not to pay. Since many mobile devices now automatically back data up into the cloud, mobile ransomware must heavily rely on social engineering panic in victims; otherwise, the user can just reset their device to factory default and download some or all of their data from the cloud network.

Mobile devices are almost all operated on Android or iOS. Android supports approximately 80 percent of the devices on the market, but iOS devices tend to be more expensive. There are ransomware variants that exploit both flavors of mobile device. Apple restricts the installation of application from outside of the Apple store, so ransomware may be more difficult to migrate onto a non-jailbroken iPhone. According to Symantec, "A ransomware developer who wishes to explore this route would first have to obtain an enterprise developer certificate from Apple, build their app, sign it with the enterprise certificate, distribute it to potential victims, and convince them to install it. The problem for the cybercriminals in this scenario is that their room to maneuver could be highly restricted and Apple could easily shut down their operation simply by revoking the certificate. This makes ransomware development activity for iOS very risky with little prospect of payback." Android devices are more numerous and more susceptible to attack, so the majority of mobile ransomware targets Android devices.

Ransomware targeting Android devices already exists. In June 2013, Android.Fakedefender infected devices by posing as an antivirus program and then locking the system after a fake scam found "critical threats." Victims were then coerced to pay for a fake software license. Other entrants, such as Android.Lockerdroid.E imitated an adult website application. After installation, the victim was threatened with a traditional law enforcement warning message and told to pay a fine to ($500) unlock their device.

Android.Simplocker, a mobile crypto ransomware also appeared in 2014. Since the Android operating system prevents applications from accessing data in other applications, Simplocker encrypted and ransomed external SD card data (which was not protected by the operating system at the time). Additional variants, such as the 2015 "Porn Droid" change the

user's PIN code. The ransomware does this by obtaining administrative privileges by hiding the escalation button under a fake confirmation message.

Servers:

An organization's servers and databases store all of their critical information. Within a server are an organization's documents, databases, intellectual property, personnel files, client list, and other intangible resources. The compromise of one essential server can hobble an organization. Despite their value, organizations regularly fail to secure, update, and patch the systems. This makes servers susceptible to lateral movement and attack. When a server is compromised, the organization goes into a panic. Even if the attack is a ransomware attack, there is concern for reputational harm due to the perception of lost customer data. Even if the organization has a business continuity plan or disaster recovery plan, the amount of time necessary to revert to a redundancy system may be unacceptable. Symantec reports that ransomware forces this opinion by combining attacks on servers with distributed denial of service (DDoS) attacks against the organization's system. The latter attack stresses the network to the extent that the former attack succeeds in pressuring the victim to pay a ransom. Another avenue of attack is to target the server and the redundancy system prior to revelation that the organization is under attack. Since many servers are perpetually connected to backup systems for real-time redundancy, lateral movement across systems is easy. One way or another, once the attacker has removed the safeguards surrounding the servers, they present the organization with a ransom 10-50 times greater than that demanded of individual users. In numerous cases, organizations tend to pay because, for them, every minute of downtime directly equates to lost revenue.

IoT Devices:

Ransomware is effective because it restricts access to information from a society that feels entitled to constant access to information. Many users pay the ransom without exploring alternative options simply because accepting the lost revenue is easier than applying effort. As more devices are connected to the threat landscape referred to as the internet of things, ransomware will have greater power over victims. Imagine the potential impact of a ransomware that infects a digital home temperature system. Given last year's proof of concept of wirelessly hacking a car, how successful do you suspect a ransomware capable of immobilizing a vehicle might be? In either case, and many others, the attacker would need to employ an alternative means of presenting the challenge for ransom and for collecting the payment. Nevertheless, ransomware is better suited for IoT attacks if only because the code is significantly smaller. Sure, some encryption operations will not work on certain devices and some target devices may not have the storage space necessary to encrypt and decrypt large amounts of data; however, that might just mean that attackers become even less likely to return data back to normal after manipulation.

Critical Systems:

Recall the 2013 Target breach in which point of sale (PoS) terminals were infected with malware. Even conservative estimates assess that the breach cost Target well over a billion dollars. A ransomware attack along the same vein would not compromise customer data in the same manner, but it would result in significant loss of sales. Transactions would become nigh impossible if customers had to use cash only or if the resulting delay per transaction caused lines to reach halfway across the store. Since security researchers speculate that the new Locky ransomware hails from the Russian Dridex criminal group (known for targeting banking and financial organization), it is not too farfetched to foresee this evolution of malware. Consider in the healthcare sector, Locky infected critical systems belonging to Hollywood Presbyterian Hospital and made conducting tests and basic procedures impossible without paying the ransom. Organizations backup critical assets such as databases, but they often neglect to do anything to ensure redundancy of critical systems such as payroll, email servers, or the aforementioned devices. Locky indicates how ransomware will evolve when guided by advanced malware threat actors instead of simpler financially motivated criminals.

The Economy of Ransomware:

Ransomware is unique among cyber-crime because in order for the attack to succeed, it requires the victim to become a willing accomplice after the fact. APT campaigns and less sophisticated financial cyber-crime prefer to remain undetected on the victim system because they profit from the data silently exfiltrated from the victim network. In order for ransomware criminals to profit, they again must rely on exploiting human nature rather than technical sophistication. Humans, like electricity, prefer the path of least resistance. If paying a small fee alleviates our workload or suspends our reality, we pay it. This is why home movers and media outlets are profitable enterprises. Even if the user knows that what they are paying for is illusory and will not alter their situation, such as a gym membership, a credit monitoring service, or the lottery, humans tend to pay into it for the peace of mind that they receive. Therefore, the adversary's goal is to convince victims that paying a ransom will relieve them of their current predicament, without drawing attention to the detail that the attacker is the direct force behind the situation. This approach is similar to 1500s Robin Hood-esque bandits along the road or 1920s mobsters. Victims are paying to regain what already belonged to them from an antagonist who offers to go away or in some cases, offers protection from future harm.

The game of ransomware attacks is discovering the right price for the threat landscape and the target economy. The cyber criminals utilize first-degree price discrimination to locate the highest amount that victims will pay without resorting to alternative solutions. Sources are not entirely clear as to why the AIDS trojan charged $189, an oddly specific number, as its ransom; but, the cost has not significantly increased in the 27 years since. According to Symantec, taking into account inflation, the $189 in 1989 was equivalent to roughly $368 in 2015, which is higher than the average of $300. In reality, the cost to users (as of 2015) fluctuated between $21-700 depending on variant, criminal, infected device, and victim demographic. The wide range shows

that some criminals prefer to make a small profit from a large number of victims while other prefer the inverse.

Ultimately, if the campaign is going to succeed, the ransom must be tailored to the victim population and the victim currency. Most variants require payment in the form of bitcoins or credit vouchers in USD; however, victims might be located across the globe. Even though the United States and India are both developed countries with bustling economies, the ability of the individual to pay will differ according to the national economy and the willingness to pay a given price will differ based on culture. Even in the United States, a victim will be more willing to pay $100 to unlock an infected iPhone than they would to unlock a $25 GoPhone. In response, many groups dynamically tailor their ransoms according to geography and infected system. For example, Cryptowall (Trojan.Cryptodefense) alters the ransom amount according to the victim's geographic location. The ransomware does this by matching the IP address to geographic IP lookup table internally or within the command and control infrastructure.

Cyber-criminals also must discriminate based on the type of victim. Individual users have a low ability to pay and cannot be charged more than the cost of the infected system. Businesses on the other hand value their data more than the system that contains it. Especially in the intangible goods market of the United States, data is the basis for modern business. Attackers who target organizations must be more sophisticated in their operation and their ransomware. Consequently, they assume greater risk, expend greater resources in preparation for the attack, and demand greater ransoms. Whether data is related to financial services, healthcare, or other critical systems, it has an associated value. While ransomware actors do not sell the data for its market price, as an APT might, the value of data does reflect in the ransoms demanded of businesses. For comparison, in 2013, polling company the Ponemon Institute claims that each minute of unexpected data center downtime resulted in a loss of $7900. Similarly, Arbor Networks surveyed organizations to estimate that a DDoS attack costs an average $500 per minute. Now unless a ransomware actor is very thorough, their attack will not halt business operations altogether the way a total network outage would. Further, many of their primary targets (financial institutions, Universities, etc.) can resort to paper forms in the interim. Nevertheless, ransomware attacks do have a financial impact because business operations are slowed while critical systems are restored. In some cases, such as healthcare, lives are jeopardized as the timer ticks forward.

Ransomware criminal groups understand and specifically engineer the pressures that victims feel. Attackers set the timer to restrict the ability of incident response teams to respond. Most adversaries set the timer for a few days but, in the future, others might set the timer to be less than the amount of time it takes to get ahold of a vendor and implement a solution. Symantec predicts that the average ransom paid by businesses is about $10,000. Organizations that pay the ransom do not tend to publically report the amount. Estimations can be made from the few empirical examples available. On February 5, 2016, attackers encrypted the email system and patient records of Hollywood Presbyterian Hospital and demanded a ransom of $17,000 in Bitcoins. After almost two weeks, the hospital paid. Healthcare organizations were not a primary target for ransomware attacks prior to 2016; but, the success of the Hollywood Presbyterian attack and the media coverage will ensure that attackers focus on the healthcare sector in the future. For comparison, after U.S. CERT and DHS released a bulletin about the Cryptolocker ransomware on November 5, 2015, police station systems were targeted with ransom demands of

$750. For comparison, the November 2015 Linux.encoder attacks against Linux based websites demanded a ransom of $420. The evidence suggests that the threat landscape is shifting towards more profitable sectors.

Payment Mediums:

The payment method has evolved with ransomware since the AIDS trojan in 1989. Actors no longer ask for checks or account numbers because those transactions take time, and can be easily traced by law enforcement. Instead, some variants, such as the 2009 Trojan.Ransomlock, ask for wire transfers and premium rate text messages while others demand that the ransom be paid with a digital voucher (CashU, MoneXy, MoneyPak, etc.) or in cryptocurrencies. Cryptocurrencies are typically purchased through the dark net accessed through Tor; though, law enforcement, security researchers, and computer enthusiasts also hold part of the market. Bitcoins (BTC) are the reigning pseudo-anonymous decentralized cryptocurrency. Because Bitcoins are steadily becoming more difficult to purchase on the dark net and because the currency is more volatile than it was in the past, some ransomware variants accept Litecoins (LTC) and Dogecoins (DOGE). Cryptocurrencies are mostly anonymous, though a few security researchers are working on models to track transactions. Cyber-criminals likely exchange the cryptocurrencies for their native currency as soon as they can because the volatile nature of the former could result in a loss of the latter.

Threat actors launder payment vouchers through online services such as casinos and betting sites that are hosted in various geographical and legal jurisdictions so that law enforcement cannot track the culprits. The money is then transferred to prepaid debit cards and the funds are withdrawn from ATM machines using human proxies. These proxies, sometimes referred to as "money mules," withdraw money for criminal organizations for a predetermined percentage. Bitcoins allegedly do not need to be laundered; however, recent efforts to trace Bitcoins have resulted in Bitcoin laundering services. These services essentially toss legitimate and illicit bitcoins into a bag, shake it, and redistribute the coins for a fee. Alternately, Bitcoins can be routed through block transaction wallets or Bitcoin anonymizers to obfuscate the identity of the owner. As previously stated, cryptocurrencies can be subject to volatile market fluctuations. As a result cyber-criminals do not necessarily have the time to fully obliterate their trail. Conveniently (for them), the criminals who receive Bitcoins do not need to entirely hide their trail from law enforcement efforts to remain at large. Instead, they just need to move coins around enough to provide plausible doubt that they were the culprits involved in the ransomware attack. In most cases, obfuscation methods need only disrupt law enforcement efforts long enough for the adversary to convert their ransom into tangible currency.

How Profitable is Ransomware?:

According to Kaspersky, creating a phishing page and setting up a mass spam email costs about $150. A trendy crypto ransomware sells for about $2000 on dark net forums. Locker ransomware probably costs less. This means that an attacker only needs to ransom eight everyday users (at the average $300) to generate a profit. Symantec estimated that in 2009, 2.9 percent of the victims paid the ransom. In 2014, CTU researchers estimated that about 1.1 percent of the Cryptowall ransomware victims paid the ransom (at an average of $500). Despite this seemingly low response rate, the FBI reported that from the 992 related complaints, Cryptowall reportedly netted over $18 million from victims between 2014-2015. Who knows how many infections were not reported? The lesson is that ransomware, while less sophisticated than APT groups and other cyber criminals, is still significantly profitable, even when only a miniscule number of user fall for its scheme.

Mitigation:

As with any cyber threat, preventing infection is preferred over remediation efforts. The first step to mitigating a ransomware threat is to implement a comprehensive cybersecurity strategy. Any organization that marginalizes cybersecurity to the bottom of the budget or that relies on a "silver bullet" technical solution is going to be breached by cyber criminals and advanced persistent threats alike. Software and hardware solutions are necessary, but they are not the only necessity. First and foremost, information security training and awareness must improve. Afterward, organizations can rely on the layered defenses that they have invested in to secure their network.

Have a Dedicated Information Security Team:

An information security team is essential to every organization. The team is not the same as the information technology team, but the two collaborate. The information security team conducts risk assessment on the organization's cyber security posture against its risk appetite to define incident response procedures, business continuity plans, and disaster recovery plans. The information security team teaches cyber security best practices to personnel and monitors adherence to policy and practices. The team ensures that key assets are protected according to their value to the organization. The information security team deploys and configures the security of all devices on the network. In the case of ransomware, it would be the responsibility of the information security team to ensure that all systems were updated and patched (especially browsers and Adobe, Java, Microsoft, and Linux applications) so that threats do not exploit open vulnerabilities, and to ensure that all critical systems were backed up in the event of a successful attack. ActiveX content in Microsoft Office applications should be disabled so that executables

do not run from malicious attachments. Similarly, blocking the execution of binaries from %APPDATA% and %TEMP% paths will prevent some ransomware from executing. It is also the responsibility of the team to map the network and to allow or deny new devices from joining the network. The team must know who and what devices are connecting to the network and for what reason those devices are connecting. Likewise, remote desktop connections to the network should be disabled. Information is key and only known entities should have access to the network.

Cyber threats evolve according to the value of data and the susceptibility of organizations to attack. Personnel on the information security team should remain up to date on sector relevant threats to the organization's cyber security. This means monitoring and profiling advanced persistent threat groups, criminal groups, hacktavists, ransomware criminals, and other threats to the organization. Information about these threats can be found in industry whitepapers, security intelligence bulletins, and on security research blogs.

Training and Awareness:

Personnel need to be trained to recognize and report threats to the organization. Information Security researchers often chime that "humans are the weakest link" in organizational cybersecurity; but, humans are simultaneously the strongest link because your organization is only as aware as your worst employee. The vast majority of breaches and cyber security incidents are directly correlated to the innocuous or malicious actions of personnel. Malicious emails are the favored attack vector of ransomware and other malware alike. Employees should be trained to recognize a malicious link or attachment. There is no justifiable reason that most organizations cannot reduce their personnel's malicious link click rate below 15 percent. A single employee is all it takes for the entire network to be compromised. Teach employees to not click on any links in any emails. It takes barely any more time to type a link into Google as it does to click the link. Personnel should only open attachments from personnel that they trust and only if they are expecting the file. Ultimately, personnel are the strongest and the weakest link in organizational security. If they make a mistake, then the organization has made a mistake. If they fail, the organization has failed.

Layered Defenses:

Organizations should protect their network as if it was a castle under siege. The goal is not necessarily to prevent an attack. Rather, network defense is about slowing the adversary and detecting their presence in time to react to the intrusion. At the very least, an organization should have as many fundamental systems as possible. No single product should be relied upon because there is no single product that provides comprehensive security. White-list firewalls permit only trusted traffic. Explicitly denying all traffic from Tor and I2P can prevent some variants of ransomware from contacting its C2 infrastructure. Intrusion detection and intrusion prevention systems warn the information security team of threats that get past the firewall. Anti-virus, anti-

malware, and anti-ransomware applications protect the network with systematic scans. User Behavioral Analytic (UBA) systems monitor baseline user behavior and notify the information security team of suspicious activity on the network. An endpoint solution incorporates signature based, heuristic based, behavioral based, and reputational based protections into one product. Change management systems prevent unwanted modification or loss of data. When possible, data should at least be encrypted while at rest and in transit. Segmenting and subnetting the network restricts the access of successful attackers. User accounts should follow a least privileged model. Finally, especially with ransomware attacks, it is paramount to have backup and redundancy systems to ensure data confidentiality, integrity, and availability as well as business continuity.

Policies and Procedures:

After personnel are trained and technical controls are configured, administrative policies can help to prevent incidents. Users should know what activities are allowed on the network. They should know how to recognize suspicious activity and to whom it should be reported. It may be beneficial to negotiate a cyber insurance policy that covers ransomware attacks as well as data breaches. Cyber insurance policies insulate the organization from the unpredictability of the cyber-threat landscape. If nothing else, the policy vendors issue minimum qualification guidelines that can help benchmark what the organization's minimum cybersecurity posture should be. These insurance policies help to quantify risk by applying an actuarial value to digital assets. An appraisal may inform the organization of what they should be protecting as well as what others in their sector are protecting. The rate of the policy will inform the organization where it sits relative to the cybersecurity posture of its competitors. Ultimately, though, the cyber insurance policy is valuable because it removes some of the panic surrounding an incident, allowing more rational responses to inevitable incidents.

When Compromises Occur:

Despite even the best information security program, exceptional operational security, and adherence to the most stringent of mitigation procedures, attacks will occur and some will succeed. Responding to ransomware is situational. When mitigation fails, it is important for organizations and individuals to consider all of the possible responses to a ransomware demand. Disengage from communicating with the attacker until the situation is thoroughly assessed and a course of action decided. Since attackers often give victims a time limit, organized response is essential to ensuring rational decision making. The proper response will depend on the risk appetite of the organization, the potential impact of the hostage data, the impact on business continuity, whether a redundant system is available, and the sectorial regulatory requirements.

Option1: Engage the Incident Response Team:

The response to ransomware attacks follows the same form as the response to APT attacks. Incidents response begins when the organization's information security team is informed of the ongoing attack. Incident response should not be spontaneous. The information security team should have planned out a procedure to follow in the event of a ransomware attack, during their risk assessment. Organizations who cannot afford an internal dedicated information security team should consult with vendor organization prior to an event. Any organization that believes that they can get by without an information security team is doomed to exploitation. Their only response will be to pay the ransom and wait to be exploited again by the same criminals, different criminals, or an advanced persistent threat group.

The incident response team should begin by notifying the authorities and applicable regulatory bodies. Ransomware attacks are, after all, a crime. As with traditional breaches, C-level management may be reluctant to report an incident out of fear of reputational harm. However, this mindset fails to consider that a breached system or, in this case, a system permanently held hostage will inevitably result in much greater harm to the organization. A properly trained information security team should have a plan of action in the event of a ransomware attack. They should also have a disaster recovery plan that identifies the organization's recovery time objective (RTO), and recovery point objective (RPO) for data breaches. RTO, RPO, and the risk appetite of the organization (identified in the risk assessment) will better inform the best course of action.

In the event that a backup exists, then cyber-forensic evidence of the incident should be preserved and documented for/ by law enforcement. Afterward, affected systems can be reverted to backup copies. In the event that there are no redundancy systems or if the secondary systems are compromised, then the information security team can find and implement a vendor solution or decryption tool.

Option 2: Try to Implement a Solution without an Information Security Team:

If a victim organization does not have an information security team, then a respondent will have to assume those roles and responsibilities. Knowledgeable users can implement some vendor solutions and decryption tools; however, without training in information security or computer systems, the victim might not be able to remove the ransomware. In many cases, files may be partially corrupted or incompletely decrypted. Even if the vendor solution is a simple executable, the victim may not be able to assure that their system is not still compromised by inactive ransomware, backdoors, or other malware. The initial infection occurred as the result of a human error (clicking on a malicious email) or a pe-existing infection. Without training and awareness or more comprehensive system management, there is reasonable likelihood that the system will be compromised again.

Option 3: Attempt to Recover the Data:

System backup and recovery are the only certain solution to ransomware. If you have a backup system, then recovery is a simple matter of restoring the system to a save point. Otherwise, you could attempt to recover data through shadow copies or through a file recovery software tool; however, many ransomware variants delete shadow copies and some even detect file recovery software. Since many variants infect the registry, system restore from a save point may not be possible even if the recovery point remains unaffected.

Option 4: Do Nothing:

In lieu of an information security team or vendor solution, options are limited to paying the ransom or accepting the loss of the system or data. If the system is backed up, and the backup remains reliable, then the victim can ignore the ransom demand and restore the system according to the backup. If there is no backup, but the ransom outweighs the cost of the system, then the victim may have to purchase a new device and dispose of the infected system with extreme prejudice.

Option 5: Pay the Ransom:

If the culprit actually provides the decryption key, then paying the ransom may alleviate the immediate pressure on the organization. Some attackers may release the system after receiving payment because doing otherwise would reduce the likelihood that other victims will pay. Ransomware is rampant. If paying the ransom is legitimately being debated, then perform a quick internet search on the type of ransomware holding your system. Whether or not criminals who use that ransomware are likely to release data after receiving payment is likely to show up online. As executives at GRA Quantum point out, "It is always a gamble to pay the ransomware as there is no guarantee that the attacker will relinquish the data (i.e. provide the private key to unlock the files) upon payment." Some attackers recognize this dichotomy of trust. They recognize that if files are never unlocked then no victim will ever pay a ransom. As a result, variants such as CTBLocker (Trojan.Cryptolocker.G) have an option to decrypt a few random files as a gesture of good faith.

GRA Quantum advises that "paying ransoms once also does nothing to prevent future attacks on the same system." Recognize that you are interacting with criminals. Cyber-criminals do not tend towards honest interactions. If you pay the ransom once, then the threat actor's logical response after releasing the system would be to strengthen their foothold in hopes that you will pay the ransom again in the future. If the culprit does not decrypt the data, then there

may not be hope of recovering the system without a vendor solution because some variants, such as cryptolocker, employ strong encryption algorithms such as 2048-bit RSA.

Conversely, the industry claim of "never pay the ransom" is unrealistic. Sometimes, no other options exist. If the backup is compromised or if the system is time critical and restoring the system would significantly impact operations, then it might make sense to pay the ransom. For example, if a critical hospital system is compromised and lives are at risk for every minute that the system remains down, then it might make sense to pay the ransom, even if the system could be restored over a longer period of time. The decision makes sense in consideration of the healthcare organization's primary concern: minimizing loss of life at any cost. If the ransom must be paid, then the organization should pay in bitcoins or some tangible asset. Victims should never pay with their credit cards or financial account information. Even when paying for bitcoins or currency vouchers, the organization should not pay with their credit cards or financial account information. If no alternative exists, then the card or account used to pay should be frozen or closed immediately after the transaction to prevent cascading breaches.

Option 6: A Hybrid Solution:

If the ransom is low, say $300 for a multimillion-dollar organization, then it might make sense to adopt a hybrid approach. This could include simultaneous efforts to pay the ransom, to triage the system, and to attempt to restore from a backup server. Organizations devout the effort and resources to a hybrid approach when system downtime is more dire than the consequences of the ransom. A hybrid approach ensures that the system will be operational in some amount of time, no matter what. This option is essential for critical systems, such as medical devices or police databases. To minimize the expended resources and the impact to the organization, hybrid solutions should only be attempted by a trained and prepared information security team.

Conclusion:

The simple and turnkey application of ransomware enables script kiddies the ability to now play in the hacker big leagues. The number of ransomware attack variations is limited only by the imagination and motivation of the attackers. A vigilant cybersecurity centric corporate culture that cultivates an environment of awareness is the most effective means to minimize the attack surface populated by the human element. The enlistment of an information security team whose sole purpose is proactive corporate infosec management is the first step in a companywide security strategy. The InfoSec team's activity should, at a minimum cover: an immediate companywide vulnerability analysis, a crisis management strategy that takes into consideration all know threats, continuous device and application patching, auditing of third party vendors and agreements, organizational penetration testing and security centric technological upgrades. Together, these actions can profoundly minimize a company's attack surface.

Sources:

Ars Technica:

http://arstechnica.com/security/2016/02/mysterious-spike-in-wordpress-hacks-silently-delivers-ransomware-to-visitors/

The Atlantic:

http://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/

Bit Defender:

https://labs.bitdefender.com/2016/02/ransomware-and-sms-sending-trojans-top-threats-in-bitdefender-android-h2-2015-report/

Business Insider:

http://www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12

CryptoCoins News:

https://www.cryptocoinsnews.com/melrose-police-pay-1-bitcoin-to-get-rid-of-ransomware/

Dark Reading:

http://www.darkreading.com/endpoint/ransomware-5-threats-to-watch/d/d-id/1297317

Data Center Knowledge:

http://www.datacenterknowledge.com/archives/2013/12/03/study-cost-data-center-downtime-rising/

Digital Trends:

http://www.digitaltrends.com/computing/ctb-locker-ransomware-encrypts-wordpress-sites/

Forbes:

http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#1d401fe475b0

Forcepoint:

https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains?cmpid=pr

The Hacker News:

https://thehackernews.com/2015/02/cryptoware-ramsomware-bitcoin.html

Healthcare IT News:
http://www.healthcareitnews.com/news/data-center-outages-come-monster-pricetag

HIPAA Journal:

http://www.hipaajournal.com/cyberattackers-demand-3-6m-ransom-from-hollywood-hospital-8313/

Information Management:

http://www.information-management.com/news/security/data-security-threats-growing-putting-projects-and-innovation-at-risk-10028336-1.html

Information Security Buzz:

http://www.informationsecuritybuzz.com/hacker-news/the-rise-of-android-ransomware/

Invincea:

https://www.invincea.com/2016/02/dridex-crew-bets-on-ransomware/

Kaspersky Lab:

https://noransom.kaspersky.com/

https://business.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/2930/

Know Be 4:
https://www.knowbe4.com/aids-trojan

Krebs on Security:

http://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/

KTVN:

http://www.ktvn.com/story/31274059/hollywood-hospital-victimized-by-ransomware-locky-spreading-fast

LA Times:

http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-storay.html

Lavasoft:

http://lavasoft.com/mylavasoft/company/blog/ddos-report-downtime-cost-companies-over-500minute

PC Magazine:

http://www.pcmag.com/article2/0,2817,2499822,00.asp

PC Risk:

https://www.pcrisk.com/removal-guides/8120-your-personal-files-are-encrypted-virus

PC World:

http://www.pcworld.com/article/2983138/security/android-ransomware-changes-a-devices-pin-code.html

http://www.pcworld.com/article/2600543/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html

PR News Wire:

http://www.prnewswire.com/news-releases/cyber-threat-alliance-cracks-the-code-on-cryptowall-crimeware-associated-with-325-million-in-payments-300168593.html

The Register:

http://www.theregister.co.uk/2015/11/02/kaspersky_announces_death_of_coinvault_bitcryptor_ransomware/

http://www.theregister.co.uk/2016/03/04/north_dorset_council_ransomware_refusal_pay_out/

http://www.theregister.co.uk/2016/01/28/lincolnshire_council/

Security Ledger:

https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/

Security Madein:

https://securitymadein.lu/ransomware-campaigns-behind-the-scenes/

Sophos:

https://blogs.sophos.com/2016/01/06/the-current-state-of-ransomware-teslacrypt/

https://blogs.sophos.com/2015/12/31/the-current-state-of-ransomware-ctb-locker/

https://blogs.sophos.com/2015/12/17/the-current-state-of-ransomware-cryptowall/

Symantec:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf.

http://www.symantec.com/connect/blogs/ransomcrypt-thriving-menace

http://www.symantec.com/connect/blogs/spam-offering-fake-visa-benefits-rewards-leads-teslacrypt-ransomware

Tech First Post:

http://tech.firstpost.com/news-analysis/mobile-malware-tripled-in-2015-ransomware-at-the-helm-kaspersky-301687.html

Top Tech News:

http://www.toptechnews.com/article/index.php?story_id=113001Z7BMY2

Trend Micro:

http://www.trendmicro.com/vinfo/us/security/definition/Ransomware#Known_Ransomware_Families

USA Today:

http://www.usatoday.com/story/news/nation/2014/05/14/ransom-ware-computer-dark-web-criminal/8843633/

Wired:

http://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

ZD Net:

http://www.zdnet.com/article/ransomware-springboards-from-wordpress-to-joomla-domains/

Appendix A: Ransomware File Extension and Identifiable Notes

File extensions appended to files:

.ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .LeChiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .HA3, .toxcrypt, .magic, .SUPERCRYPT, .CTBL, .CTB2, .locky, .MP3, or 6-7 length extension consisting of random characters.

Known ransom note files:

HELP*DECRYPT.TXT, HELP_YOUR_FILES.TXT, HELP_TO_DECRYPT_YOUR_FILES.txt, RECOVERY_KEY.txt HELP_RESTORE_FILES.txt, HELP_RECOVER_FILES.txt, HELP_TO_SAVE_FILES.txt, DecryptAllFiles.txt DECRYPT_INSTRUCTIONS.TXT, INSTRUCCIONES_DESCIFRADO.TXT, How_To_Recover_Files.txt YOUR_FILES.HTML, YOUR_FILES.url, encryptor_raas_readme_liesmich.txt, Help_Decrypt.txt DECRYPT_INSTRUCTION.TXT, HOW_TO_DECRYPT_FILES.TXT, ReadDecryptFilesHere.txt, Coin.Locker.txt _secret_code.txt, About_Files.txt, Read.txt, ReadMe.txt, DECRYPT_ReadMe.TXT, DecryptAllFiles*.txt FILESAREGONE.TXT, IAMREADYTOPAY.TXT, HELLOTHERE.TXT, READTHISNOW!!!.TXT, SECRETIDHERE.KEY IHAVEYOURSECRET.KEY, SECRET.KEY, HELP*DECYPRT_YOUR_FILES.HTML, help_decrypt_your_files.html HELP_TO_SAVE_FILES.txt, RECOVERY_FILES.txt, RECOVERY_FILE.TXT, RECOVERY_FILE*[random].txt Howto*RESTORE_FILES*.txt, Howto*Restore_FILES.txt, howto_recover_file*.txt, restore*files*.txt, how*recover+[random].txt, _how_recover*.txt, recovery*file*[random].txt, recover*file*[random].txt recovery*file*[random].txt, Howto_Restore_FILES.TXT, help_recover_instructions+[random].txt, _Locky_recover_instructions.txt

Appendix B: Locky Domains For February 2016 through March 2016:

ICIT fellow Forcepoint traced the C2 infrastructure of the Locky ransomware and has published the following list of domains that distribute the Locky ransomware. Network administrators and home users can use this information to block access to these domains.

24/25 Feb 2016:

bkadufmdyf[.pm]
kpvoxwgf[.pm]
fysck[.fr]
hsasjielgfkneh[.ru]
qquvjijtvatj[.in]
edmgbqygn[.de]
nbavfpb[.uk]
wyusb[.yt]

26/27 Feb 2016:

yuljfxdf[.pm]
bvtavc[.nl]
ktovxeteqtwtcsh[.yt]
xyfnvvbuovcd[.be]
hwsdymcytd[.yt]
cgwlamg[.pw]
ehfjt[.pm]
nfacehihugohhi[.nl]

28/29 Feb 2016:

cproso[.pm]
lnjrmdjyidprrse[.de]
nortkbiqhtdgd[.de]
ixwllqpbog[.in]
rvkgvjbp[.it]
ficpn[.fr]
ogworigxknalsd[.eu]
qaekmjxgrtcs[.de]

1 March 2016:

prydlvlxw[.be]
rsimigt[.us]
bqvcl[.in]
ovmspedrbkxlj[.ru]
xthppvomcxu[.be]
aupgcrvfm[.us]
uemtsb[.uk]
echmfrnyuwrlmas[.uk]

2/3 March 2016:

jaliqnp[.yt]
ejpmaxavyptyqnc[.pw]
nhkpknfyjnoqp[.ru]
iqountnrqs[.ru]
krpphdlu[.yt]
tpkmyc[.ru]
hubvdqgfcoierc[.pw]
qsaifcyuopyv[.de]

4/5 March 2016:

bxlrnw[.pw]
vhpurxfuohbqso[.fr]
ffkseaisuicb[.eu]
hgspblbnex[.yt]
cppvgch[.in]
lnkva[.pw]
ysbfaksqohpmf[.in]
iqvcaeogjeg[.it]

6/7 March 2016:

spxst[.us]
nycbuwfisadao[.be]
wwpyvxnihcm[.fr]
yxxpmghmx[.uk]
thcfqk[.it]
dfwqdyjrtyiuaij[.pm]
qrokkqdsmtxa[.us]
apgodprqgy[.eu]

8/9 March 2016:

djcbwpykgnsdikb[.pm]
fkkdmvsjnnptv[.yt]
athfaulmew[.pw]
cupggwpf[.pm]
lsotcg[.in]
gcsxwslqsvbhpr[.pw]
ivtlxgqfkiyj[.it]
dfxvcvxfa[.be]

10/11 March 2016:

kfifrxqke[.in]
fogyrq[.uk]
ombqnwvepxjeufs[.tf]
qnjoimqcqkokt[.yt]
lpmxewicfk[.us]
uubnggrp[.in]
woiwpu[.fr]
rxmbadyblcuoat[.in]

12/13 March 2016:

dlhhgett[.us]
mqvubo[.de]
haageiedrybojk[.tf]
jtlqoqfaykdj[.uk]
edpglqefm[.it]
nbdwqkj[.fr]
pcmfx[.de]
klqqvsewphwko[.it]

14/15 March 2016:

vqmkfujpobvu[.us]
xkxapdrojh[.nl]
stckmju[.yt]
uulhq[.fr]
esyjyjiklwnbhd[.tf]
ycdntrbxkuw[.de]
bdlpmukcp[.eu]
vmpthc[.it]

16/17 March 2016:

ddutcdmfvmbaaba[.be]
mbikamdjklmce[.de]
hkmaebphml[.yt]
jetxtfwv[.pw]
enxme[.us]
nllwyhyrvsdodo[.fr]
pmttrjeukjnl[.yt]
kvxcsnink[.yt]

18/19 March 2016:

vopbboe[.tf]
fmktk[.pw]
avppvitupmdtm[.tf]
cwxghlngfxo[.nl]
wguofdum[.it]
yhdrnk[.ru]
ifxjoqrmcmajhjf[.ru]
docniprmgcxm[.be]

20/21 March 2016:

adrefp[.ru]
jinpjwfrsjpmjgu[.us]
ekqmsioexowp[.uk]
glrbxuhejj[.de]
buvpbsq[.pw]
dvehl[.pw]
mtygfrrwfppuvv[.us]
hdvmubmbyxs[.nl]

22/23 March 2016:

radqq[.tf]
bfyilphwkctxdf[.us]
vhcrhadppxa[.it]
xidmofnsc[.ru]
srlkgw[.pw]
ustmanuqnxxhlmj[.pm]
eqplamxxqghrd[.tf]
yamyqrhatl[.de]

24/25 March 2016:

jxeepaassngeetq[.in]
sdsyswxogrhjf[.tf]
nfvdvistdi[.nl]
pgeeucpt[.uk]
yercwd[.nl]
mqjlvimienyxwr[.fr]
voebnwfybwkg[.pw]
qximfakki[.fr]

26/27 March 2016:

xjneysaum[.us]
hhbrghm[.eu]
jijps[.in]
ernthxdqkbuoi[.tf]
npixhjhhmpm[.uk]
burfvaac[.pm]
ksmbxx[.in]
mtuamviphwoapcq[.uk]

28/29 March 2016:

jjrlgvdlqurpa[.pm]
shmcsgbpypg[.fr]
uivmeislw[.eu]
prsobv[.pm]
ypnlcncyegxteub[.in]
bqvjrrodkfhjg[.it]
vaaytyxqyl[.eu]
fxnitwaq[.fr]

30/31 March 2016:

pvmyilqakqqkl[.in]
kfqoruddyo[.nl]
myxmilto[.it]
hicqd[.us]
qnqlfdthdyidbw[.be]
shxppmfnhjao[.pm]
nqcxfhycl[.in]
wowkllj[.it]

Contact Information

Legislative Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies, Executive Branch and Fellow Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

 https://twitter.com/ICITorg

 https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

 https://www.facebook.com/ICITorg

Joint Statement for the Record by the

AMERICAN PUBLIC POWER ASSOCIATION (APPA) and the

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA)

Submitted to the

SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE

For the May 18, 2016, Hearing on

"Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions"

The American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) appreciate the opportunity to submit a statement for the record for the Senate Homeland Security & Government Affairs Committee (HSGAC) hearing on "Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions." APPA and NRECA support and agree with the testimony of Mr. Scott Aaronson with the Edison Electric Institute.

The electric power grid is a complex, interconnected network of generating plants, transmission lines, and distribution facilities. The electric power industry continuously monitors the bulk electric system and responds every day to events large and small. Consumers are rarely aware of these events primarily because of the sector's system operation expertise, planning, coordination, response and resiliency activities. Protecting the nation's electric power grid and ensuring a supply of safe, reliable, and affordable electricity is a top priority for the electric power industry.

The electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to a wide variety of hazards to electric grid operations, including natural events, such as severe weather or geomagnetic disturbances (GMDs) caused by solar storms, as well as malicious events such as physical or cyber attacks directed at the grid, and primarily response and recovery for electromagnetic pulses (EMPs) caused by an attack on the homeland via the high-altitude detonation of a nuclear weapon. We expect that the federal government will be responsible for the prevention aspect of an EMP event.

The goal of every utility and the industry as a whole is to manage risk prudently. Still, there are tens of thousands of diverse, often remote, facilities throughout the U.S. and Canada that cannot be protected 100 percent from all threats, requiring utilities to prioritize facilities that, if damaged, would have the most severe impacts on their ability to "keep the lights on." These facilities would then receive increased attention and investment in critical infrastructure protection.

The electricity sector continuously strives to improve on its history of protecting its assets from security threats, including longstanding programs and protocols designed to protect utility systems. Key to reliability efforts are the crisis management and site-specific security plans developed by electric utilities to ensure that operations and infrastructure systems are properly supported; in addition, a number of redundancies are built into the system, in many cases allowing utilities to re-route power around damaged facilities. Utilities also partner with federal, state/ provincial, and local government and law enforcement agencies in both the United States and Canada to ensure that they can respond effectively to any event that may impact their operations.

To maintain and improve upon the high level of reliability consumers expect, electric cooperatives, public power utilities, and investor-owned utilities all work with each other and the North American Electric Reliability Corporation (NERC), the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) on matters of critical infrastructure protection – including sharing needed information about potential threats and vulnerabilities related to the bulk electric system.

In 2013 the electric utility industry reorganized the Electricity Subsector Coordinating Council (ESCC) to ensure high level engagement. The new ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

The electric sector and its subject matter experts will continue to partner with government agencies like DHS, DOE, and FERC on matters of critical infrastructure protection to improve physical and cyber security for its assets. It is important to note, however, that to help maintain operational security, the industry is careful not to publicize clearly sensitive information about critical infrastructure that might provoke new threats or endanger the safety and well-being of the North American public or the integrity of the electric power grid.

State of Wisconsin / DEPARTMENT OF MILITARY AFFAIRS

P.O. BOX 8111
MADISON 53708-8111

TELEPHONE 608 242-3000
DSN 724-3000

OFFICE OF THE ADJUTANT GENERAL

July 19, 2016

Via Email (laura_kilbride@hsgac.senate.gov)

The Honorable Ron Johnson
United States Senate
328 Hart Senate Office Building
Washington, DC 20510-4905

Subject: Homeland Security Committee Post-Hearing Response

Dear Senator Johnson:

Thank you for inviting me to testify at the May 18, 2016, Homeland Security and Governmental Affairs Committee Hearing: "Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions". Below are our responses to the post-hearing questions from Senators Ayotte and Portman. Please let me know if you have any other questions. I appreciate the committee's attention to this critical area of concern.

Post-Hearing Questions Submitted by Senator Kelly Ayotte

Q1. During a recent hearing of the U.S. House Transportation and Infrastructure Committee, industry witnesses disclosed that a cyber-attack could cause a grid blackout lasting two weeks. Does the National Guard in the State of Wisconsin plan for a blackout lasting two weeks?

In Wisconsin, the Adjutant General is the Secretary equivalent for the Department of Military Affairs (DMA). In this capacity, I command the National Guard and am responsible for Emergency Management and serve as the Homeland Security Advisor. DMA consists of the Wisconsin National Guard and Wisconsin Emergency Management (WEM).

We have a Homeland Security Strategy and a comprehensive Emergency Response Plan, both of which contemplate catastrophic events such as a long term power outage. Our plan is based on the fifteen emergency support functions and a series of annexes, such as catastrophic incident, severe weather, and cyber. Our plan is updated on a quadrennial basis consistent with the gubernatorial election cycle. The primary focus and foundation of our plan is based on meeting projected requirements for the 13 most likely threats as defined in our state Threat and Hazard Identification and Risk Assessment (THIRA).

The National Guard is embedded in this plan, along with state agencies and volunteer organization partners, to guide state response to natural and man-made events. Our National Guard operates under a Joint Force Headquarters and also occupies a position in the Emergency Operations Center, when activated for an event. For exercising and operational planning, we focus on the first 72 hours of a catastrophic event.

Specifically for black outs lasting two weeks, We have partnered with power companies, utilities, as well as other critical infrastructure facilities in the state to analyze needs and resources. We have refined our military concepts which will allow the deployment of forces based on core capabilities of transportation, signal, aviation, logistics, security, engineering, medical, and maintenance and have exercised these with civilian first responders. These resources meet a wide range of requirements anticipated during a long-term power outage.

Lastly, we recently completed a two-day intensive review of the power gird reliability within Wisconsin and are partnering with our Public Service Commission to work even closer with utilities, water systems and sewage treatment facilities. This includes a review of diesel fuel requirements for sustained power outage.

Q2. Does the National Guard in your state have plans to protect personnel and backup diesel fuel supplies for critical electric grid facilities, including control centers and "black start" generation plants, in event of a long-term grid outage persisting days or weeks?

We continue to develop our plans and procedures for long-term events which would require National Guard support, and then exercise them to refine and validate our tactics, techniques, and procedures. Any blackout, whether several days or longer, is a concern for maintaining Critical Infrastructure (CI). WEM has coordinated with state agencies for the availability of fuel at their locations around Wisconsin, along with the petroleum marketers. This year WEM is reaching out to water and sewage facilities along with electric utilities through Regional Workshops across the state. The kick off session is on August 9th, where WEM is hosting the FEMA Region V Long Term Power Outage workshop. Additionally, Long Term Power Outage exercises have been conducted regionally across the state which focused on electric utilities and assisted living facilities. We continue to build upon the lessons learned. The Wisconsin National Guard has established relationships with private utilities across Wisconsin. We have ongoing efforts with electric, water and sewage entities which has led to a much better understanding of the CI architecture in the state and the detailed requirements to support short-term and long-term power disruption across the state. These efforts include potential missions to protect key resources and diesel fuel assurance for back-up generators.

The resiliency of our public sector systems is driving decisions and planning by our civilian leadership and refined planning to support projected requirements. The National Guard has been identified as a critical resource provider within the state's emergency response plans, and stands ready to provide support as planned or will adapt to provide resources as determined necessary by the state's emergency management community during a crisis.

Q3. Does the National Guard in your state have plans to assure supplies of backup diesel fuel for the sites of National Guard cyber defense teams?

Yes. The Wisconsin National Guard cyber defense capabilities are collocated in the Joint Force Headquarters and within the same facility as the State Emergency Operations Center (SEOC). That facility has backup power generation to support the first 24 hours of an event

with National Guard diesel storage infrastructure near-by with sufficient haul capability to continue resupply for a long-term power outage.

In addition, we have back up capacity at our alternate locations for Continuity of Operations and Continuity of Government (COOP/COG) plans.

Q4. The United States has not yet experienced a wide-area outage of the Bulk Power System (interstate high-voltage transmission system) lasting more than one day. Electric utilities rely on commercial telecommunications carriers that normally use grid power; these carriers typically have diesel fuel for backup generators lasting only 1 to 3 days. Given this interdependency, does the National Guard in your state have a contingency plan to provide radio communication for electric utilities to facilitate electric grid restoration?

No, we do not have a specific contingency plan to provide radio communications to facilitate electric grid restoration.

However, the State's Wisconsin Statewide Communications (WISCOM) is a statewide platform to enhance responder communications capabilities. WEM is exploring communications requirements with the electric utilities to determine their needs for additional communications beyond their corporate redundant systems. As a result of a growing National Guard and local utilities relationship, we have a greater understanding of utility communications capabilities and redundancies necessary to support grid restoration.

The Wisconsin National Guard and other state agencies have capacity to provide supplemental support at prioritized locations, based on long-term recovery needs. WEM, in collaboration with the emergency management community, will prioritize resources for deployment, if not previously identified through planning efforts. Ongoing collaborative efforts are producing results to help identify gaps and allow for preplanned resource management and the resources to proactively fill gaps. Wisconsin does have an established communications network, WISCOM, this along with the anticipated national deployment of FirstNet are key elements that support our emergency communications needs statewide.

Post-Hearing Questions Submitted by Senator Rob Portman

Q1. The Wisconsin and Minnesota ports on Lake Superior ship the vast majority of iron ore required by Indiana, Michigan, Ohio and Pennsylvania integrated steel mills. To get to those steel mills, the ships carrying this vital ingredient must pass through the Army Corps of Engineers' Soo Locks complex in northern Michigan. Last year, the Department of Homeland Security estimated that if the largest of these locks, which is nearly 50 years old, became inoperable for six months, the Great Lakes region and the nation would experience a massive economic upheaval because steel and automobile manufacturing would halt due to a lack of supplies. Doesn't it make sense to ensure there is additional lock capacity to protect against such an economic catastrophe?

The Soo Locks are a critical resource for our nation's economy. The locks are a Federal Facility, operated by the Army Corps of Engineers (ACOE) on the Michigan side of the U.S./Canada border. Intuitively, it makes sense to increase capacity and ensure security,

which I am confident that the Department of Homeland Security (DHS) has and will continue to contemplate.

The DHS and ACOE have been conducting ongoing assessments related to the Soo Locks for both security and facility maintenance or replacement. Recently, DHS published the findings of a study related to the impacts and long-term needs that provide valuable insight on the issues of resiliency, security and maintenance.

Critical Infrastructure, such as the Soo Locks Complex, present the potential for national impacts and must continue to receive congressional attention to ensure no single point of failure can hold our economy as a hostage. The DHS study demonstrates and advocates a need for resilience. Specifically, the report suggests a second twin lock and long overdue maintenance of the current lock. I would defer to the DHS National Protection and Programs Directorate and the report's authors for specifics and any discussion.

Q2. I also understand that during World War II, the Army stationed thousands of troops around the Soo Locks to ensure that U.S. steel production that was so vital to the war effort was not disrupted. What kind of physical protection should this type of critical infrastructure have now?

As a national resource the Soo Locks Complex is a resource that must have an appropriate level of physical security in order to meet the potential threat. It is the purview of DHS to determine what is appropriate to ensure the physical protection of the facility is assured. Should the Secretary determine that additional support is needed, the National Guard could assist under state or federal direction.

If you have any questions, please contact Ms. Jackie Guthrie, Director of Government Affairs. She can be reached at 608-242-3026 or email jackiea.guthrie@wisconsin.gov.

DONALD P. DUNBAR
Maj Gen, Wisconsin National Guard
The Adjutant General

Post-Hearing Questions for the Record
Submitted to Mr. Tom Farmer
From Senator Rob Portman

"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities and Solutions"
May 18, 2016

I understand your background is in the rail industry. Last year, the Department of Homeland Security determined that if the Army Corps of Engineers' Soo Locks in northern Michigan unexpectedly went down for an extended period of time, the railroad industry would be unable to provide the capacity to move the 40-50 million tons of iron ore currently carried by vessels annually through those locks to integrated steel mills in Indiana, Michigan, Ohio and Pennsylvania. I understand that in 2014, the railroad industry told the Corps that building a rail infrastructure back-up system to the Soo locks would cost $5 billion and was not economically justifiable for that industry. Building the Congressionally-authorized second large lock at the Soo complex at an estimated cost of $600 million appears to make more sense.

1. Isn't back-up capability for choke points such as this an important aspect of transportation security?

To follow up on our discussion from the hearing, I have some additional questions regarding ransomware.

2. How would you design a reporting and enforcement scheme to ensure all ransomware intrusions are investigated and, if possible, prosecuted by law enforcement?
3. What regulatory and legislative restrictions need to be eliminated in order to assist organizations in responding to and recovering from ransomware intrusions?

You mentioned in your testimony at the hearing that the United States is not doing a good job of researching the intrusion mechanisms used by these cyber criminals.

4. What are some emerging and current trends among the intrusion mechanisms being utilized by cyber criminals?

Depending on size, economic sector, and information holdings, entities require differing levels of cyber security.

5. What basic steps should entities take to reduce their attack surface?

Witness responses to questions submitted for the record were not received by time of printing.

Post-Hearing Questions for the Record
Submitted to Mr. Tom Farmer
From Senator Claire McCaskill

"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities and Solutions"
May 18, 2016

In February 2013, President Obama issued Presidential Policy Directive-21 (PPD-21), calling for a "national unity of effort" in critical infrastructure protection centered on a common strategy. Out of that came the National Infrastructure Protection Plan of 2013 (NIPP), which seeks to fulfill the President's requirement. The NIPP then created three types of councils to improve communication, planning, program implementation and response and recovery.
These councils facilitate engagement between the private sector and federal officials to come up with a consensus on joint priorities and actions to improve security of our critical infrastructure. It is my understanding, however, that implementation of these actions is not required, although presumably many companies are implementing the security improvements these councils are coming up with.

1) Who is responsible for oversight of implementation of the action items that these councils come up with?

2) Is there any data on how many private sector companies have taken action on all of the recommended security steps?

For example, you noted in your testimony that, after the mall attack in Nairobi, representatives of multiple industries partnered with the DHS and FBI to develop a comprehensive training program on prevention and mitigation. Your testimony also stated that application of this program drew "wide participation."

3) Do you know what percentage of malls in this country applied the training program and are prepared for such an attack?

Witness responses to questions submitted for the record were not received by time of printing.

Post-Hearing Questions for the Record
Submitted to Mr. Ted P. Koppel
From Senator Rob Portman

"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions"
May 18, 2016

1. Much has been said about protecting the U.S. electrical grid from direct attack. Even if the grid is protected, however, if the supply of power plant fuel is significantly degraded on a regional basis, wouldn't that also have negative impacts? To ensure electrical power supply security, shouldn't we ensure there also is power generation fuel supply chain security, including the transportation of coal and natural gas?

Response:

I have done no research on the subject and regret that I have nothing of value to offer.

Post-Hearing Questions for the Record
Submitted to Mr. Ted Koppel
From Senator Kelly Ayotte

"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions"
May 18, 2016

(1) Based on your conversations with senior government officials, does the U.S. Government effectively plan for electric grid outages persisting beyond three days?

Response:

No. The Department of Homeland Security's website, does not even include the likelihood of a cyber attack on the power grid among its list of likely catastrophes. In my conversation with the Secretary of Homeland Security, it is clear that he is unaware of any plan specifically designed to deal with an outage of more than a few days. The two senior officials at FEMA differ as to how a major city should respond. The second in command would recommend evacuation, his boss dismisses evacuation as a viable option.

(2) In your opinion, what percent of the local population would die if all of the New York metropolitan area had no electric power for three days? And also for two weeks?

Response:

NY State has adequate MRE's to avoid food shortages during a three-day power outage. It would, however, run out of food thereafter. How many deaths would result from lack of essential medicines, inability of law enforcement to maintain order, lack of food and water and the inability to dispose of human waste and the resulting illnesses, depends in large measure on how wide the affected area is. If we were "only" talking about New York City, supplies could fairly easily be brought in from outlying areas. The Eastern Interconnect (one of three power grids in the United States) covers almost the entire eastern half of the United States. If a cyber attack took out the entire grid, the resulting deaths after only two weeks would be catastrophic.

(3) Based on your interviews with the Secretary of Homeland Security, who indicated evacuation from urban regions would be necessary, and the Director of the Federal Emergency Management Agency who indicated that urban evacuations would be disruptive, do you believe the United States has a coherent plan to respond to a prolonged electric blackout?

Response:

For the record, it was not the Secretary of Homeland Security who indicated that evacuation would be necessary (see my answer to question #1) it was the deputy FEMA administrator. His boss, however, the FEMA administrator, disagreed. Secretary Johnson was unable to refer to a particular plan (although he expressed the conviction that one must exist). He recommended having a battery-powered radio. I do not believe that the United States has a coherent plan to respond to a prolonged electric blackout. Indeed, I am convinced that it will almost inevitably fall to the U.S. military (specifically, NorthCom) to attempt maintaining some form of order. The former commander of NorthCom expressed concern to me that the army does not have manpower adequate to the task.

Post-Hearing Questions for the Record
Submitted to Mr. Scott Aaronson
From Senator Rob Portman

"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions"
May 18, 2016

1. Much has been said about protecting the U.S. electrical grid from direct attack. Even if the grid is protected, however, if the supply of power plant fuel is significantly degraded on a regional basis, wouldn't that also have negative impacts? To ensure electrical power supply security, shouldn't we ensure there also is power generation fuel supply chain security, including the transportation of coal and natural gas?

   EEI response:

   In the event that the power generation fuel supply chain is significantly degraded within a region, there could be negative reliability impacts to the energy grid. One of the electric sector's top priorities is maintaining a balanced energy mix, which includes clean and renewable energy sources and traditional ones, to help mitigate against such risk. America's electric companies rely on a variety of domestic energy sources to generate electricity, which helps to protect electric companies and their customers from contingencies such as resource unavailability, price fluctuations, and changes in regulatory practices that can drive up the cost of a particular resource. A balanced energy mix also helps to ensure stability and reliability in electricity supply and strengthens national security.

   The industry relies on a variety of energy resources for power generation. No individual source is capable of providing the energy to meet all of our nation's electricity demands. In 2015:

   - Coal provided 34.0 percent of our nation's electricity;
   - Natural gas supplied 32.5 percent;
   - Nuclear energy produced 19.4 percent;
   - Hydropower provided 5.9 percent of the supply;
   - Non-hydro renewables, including wind and solar energy, produced 7.1 percent; and
   - Fuel oil provided 0.7 percent of the generation mix.

   The electricity generation mix differs from state-to-state and region-to-region, depending on the availability and cost of resources located there. Major changes in the generation mix can have economic impacts, especially on a regional basis.

   With respect to the transportation of coal by rail and natural gas by pipeline, EEI works with the transportation sector and the downstream natural gas sector, through the Electricity Subsector Coordinating Council (ESCC) and other forums, to improve coordination of deliveries to match demand, improve planning and responses to major incidents, conduct

joint exercises, better understand and protect our mutual dependencies, and share information more effectively.

It is also important to focus on ways to assure the continued operation of the existing nuclear fleet for reliability purposes.

Post-Hearing Questions for the Record
Submitted to Mr. Scott Aaronson
From Senator Kelly Ayotte

"Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions"
May 18, 2016

Question 1:

During your testimony, you indicated that the U.S. electric grid would be shut down during a severe solar storm, although you noted that it was not clear who would make this decision. A 2010 Oak Ridge National Laboratory study established the threat from solar storms, but years later an arguably small percentage of vulnerable high voltage transformers have monitors for Geomagnetically Induced Current (GIC)—several hundred out of a total population of approximately 2,500. Moreover, in rulemaking comments to the Federal Energy Regulatory Commission (FERC), EEI and other trade associations have opposed mandatory installation of solar storm monitors.

a. **Given the potentially high societal costs that could result from unnecessarily shutting down the electric grid during solar storms due to poor situational awareness, and with delays by utilities in installing storm monitoring equipment, does EEI oppose mandatory standards requiring installation of GIC monitors?**

EEI Response:

Electric companies have added, and continue to add, GIC monitors to collect the information needed to determine how best to protect their assets. Once FERC approves the proposed North American Electric Reliability Corporation Reliability Standard (TPL-007-1), and companies have greater clarity about their obligations, even more GIC monitors will be installed. While additional monitoring, including GIC monitors, could benefit ongoing technical research, we do not believe it is appropriate to use mandatory standards to require installation of any particular type of monitors to encourage this research. The most effective approach is to allow grid asset owners and operators, who know their systems best, to install proper monitoring where it makes sense and provides the greatest net benefits, consistent with industry engineering norms and regulatory oversight.

b. **Would EEI support automated data sharing from deployed GIC monitors to the Department of Energy Operations Center?**

EEI Response:

Significant security challenges arise when considering sharing data from deployed GIC monitors because this information may identify the locations of critical and possibly vulnerable assets. If this information is disclosed, it can be used as a target map by adversaries. In the absence of a better understanding of how the Department of Energy (DOE) Operations Center would use and protect this data, EEI refrains from stating a position on whether to support sharing this information with the DOE Operations Center.

Question 2:

In rulemaking comments to FERC, EEI and other trade associations advocate for greater flexibility, and less compliance consequences, for imposing "loss of load" (i.e., blackouts) during solar storms.

a. Please state in clear terms the position of EEI on desired "flexibility" for utilities to impose blackouts during solar storms.

EEI Response:

EEI's comments to FERC recognized that the science surrounding geomagnetic storms remains immature and imperfect. Effective planning, modeling, and monitoring have only recently evolved to a point where the electric sector can begin to develop more robust strategies to protect the grid. Recognizing that even the most aggressive mitigation plans may prove inadequate for a very large and likely dynamically changing solar event, we believe Transmission and Generator Operators need the flexibility to act quickly to protect grid assets. As a last resort, conditions may require the temporary shedding of load in order to avoid more severe, long-term damage to critical assets and to maintain grid balance. As stated in our comments, Transmission Operators need the flexibility to make immediate and on-the-spot decisions in the best interests of protecting the grid and being able to restore power as quickly as possible, without having to take the time to consider potential compliance consequences; otherwise assets might be needlessly damaged as a result.

b. Is it better to cause deliberate blackouts during solar storms or to implement proactive protective measures that will not require intentional blackouts?

EEI Response:

EEI believes that it is generally preferable to implement proactive protective measures to avoid intentional blackouts, but, unfortunately, the solutions to this very complex problem are not so simple. This is not necessarily an either/or situation. Although there are a few equipment manufacturers that have developed hardware solutions that they believe to be effective, initial industry testing has found that these solutions may result in unintended operational problems that could outweigh their benefits. (*See ATC comments filed at FERC on RM15-11, July 27, 2015.)*

In addition, the Electric Infrastructure Security Council Electric Grid Protection Handbook (known as the "EIS Council E-PRO Handbook") discusses the complicated nature of mitigation. Specifically, on pages 138-139, a section titled "Risk of Increased GIC in Autotransformers" states, "it is important to note that GIC can actually increase at an autotransformer, even with a blocking device." The section goes on to explain the difference between so-called "autotransformers" and "full transformers" and how each reacts to GIC and certain mitigation strategies. Suffice to say, experts agree there are no simple or easy solutions, which is why the Electric Power Research Institute (EPRI) has undertaken its project to look at the existing protection and possible mitigation strategies to better understand the engineering challenges associated with electromagnetic pulse (EMP) mitigation; similar challenges apply with regard to geomagnetic disturbances (GMDs) caused by solar storms.

Regarding intentional blackouts, EEI recognizes such steps are drastic and should be considered only as a last resort in response to very low frequency events well beyond normal planning horizons. EEI agrees that intentional blackouts should be avoided if possible. But, such an option may be necessary in extraordinary circumstances to avoid even greater negative impacts from permanent

damage to critical long lead time assets, and may be preferable to rushing the deployment of unproven hardware solutions that could have unintended consequences on the system.

Question 3:

During the hearing, you indicated that the U.S. electric grid would be shut down during or before a severe solar storm, although it is unclear who would make this decision. Under most insurance policies, widespread load shedding in advance of a predicted solar storm could be considered an "intentional act" and therefore void policy coverage for resulting losses. Additionally, government authorities might be reluctant to order grid shutdowns based on 30-minute forecasts of impeding solar storms.

a. **Does EEI maintain that so-called "operational procedures" are a realistic solution to solar storm threats?**

EEI Response:

Yes.

b. **If so, why?**

EEI Response:

EEI believes that operational procedures supported by planning studies and equipment thermal assessments, as required in the proposed North American Electric Reliability Corporation (NERC) Reliability Standard (TPL-007-1), are effective measures to address GMD risk.

Question 4:

In rulemaking comments to FERC, EEI and other trade associations stated:

> **"In addition, Trade Associations also believe that the technology available to mitigate or control GIC caused by a GMD event of historic scale is only beginning to be developed. Existing technology such as "blocking devices" does not provide simple solutions, and is expensive. Such devices continue to be experimental in nature, and require very careful planning, installation, and operations considerations. For example, one recent study shows that adding blocking devices to reduce GIC in some transformers tends to elevate GIC in other transformers. The authors also make the point that blocking devices in the neutral grounding conductors of autotransformers cannot reduce GIC that flows in the series windings of autotransformers. As a result, even widespread application of blocking devices may be only marginally effective in reducing total system MVAr demand. Blocking devices may be very helpful in particular cases, but are not a panacea."**

Despite successful testing at the Idaho National Laboratory, utilities have generally declined to install blocking devices at an equipment cost of about $350,000 per transformer set protected.

a. **How many EEI members have research programs with operationally installed blocking devices?**

EEI Response:

EEI cannot comment on this question because it does not collect or maintain this type of information.

b. **In total, how many blocking devices have been installed by EEI members to protect large power transformers?**

EEI Response:

EEI cannot comment on this question because it does not collect or maintain this type of information.

c. In the FERC comment, EEI states that "blocking devices" for solar storm protection are "expensive." Can EEI confirm for the committee that commercially available blocking devices cost approximately $350,000 per installation?

EEI Response:

EEI does not collect or maintain this type of information, but would note that American Transmission Company's comments filed in response to FERC Docket No. RM15-11 (NOPR) stated the cost to install one of these devices would be at least $500,000 per installation.

Further, as noted above in the citations from the ATC experience and the EIS-Council's E-PRO Handbook, there remain no "plug-and-play" devices. In addition to the cost of each device, system re-configurations, other associated mitigation strategies, and ongoing operations and maintenance must be factored into the true cost of deployment of any device.

d. How would the cost of blocking devices compare to the societal costs of shutting down the electric grid during a severe solar storm?

EEI Response:

EEI does not have sufficient information to respond to this question and is unaware of any studies that provide such analysis.

e. Can the same protective hardware, if properly designed, protect against both solar storms and the E3 component of nuclear electromagnetic pulse?

EEI Response:

EEI does not have sufficient test data or expertise to effectively assess these devices but understands that Oak Ridge National Laboratory studied the impact of high-altitude nuclear electromagnetic pulse (HEMP) on electric power systems[1]. In the referenced report, the Lab concludes that the E3 component "impact will be quite similar to geomagnetic storm effects, but of a shorter duration and

---

[1] Oak Ridge National Laboratory Report titled, "Impacts of a Nominal Nuclear Electromagnetic Pulse on Electric Power Systems, Phase III, Final Report; ORNL/Sub/83-43374/2.

higher intensity." [2] The report goes on to say that "[l]ittle physical damage is expected from a nominal [E3[3]] event due to its short duration."[4]

EEI believes that any hardware solution applied to the bulk electric system should be thoroughly tested and validated before it is applied on a large scale. And, as previously noted, we would need assurance that blockers, in fact, work, and that they do not worsen the situation or create other unintended adverse consequences.

Question 5:

In the EEI position paper, "Electromagnetic Pulses (EMPs): Myths vs. Facts," EEI states as a "fact":

> **"High-Altitude Nuclear Blast EMP: A high-level EMP caused by the detonation of a nuclear weapon in the atmosphere is a high-consequence, low-likelihood threat that would have a potentially catastrophic impact on society. Further, since the planning and launching of a nuclear attack on U.S. critical infrastructure would be an act of war or terrorism, the federal government must be primarily responsible for preventing high-level EMPs as a matter of national security."**

Non-nuclear attacks on critical infrastructure could also be acts of war or terrorism, yet utilities are required to protect against them by following mandatory standards. Moreover, if designs for solar EMP and man-made EMP are included in plans for newly constructed control centers or transformers or generators, the costs of mitigation are reduced, compared to retrofit requirements.

a. **Please explain EEI's position that the federal government "must be primarily responsible" for preventing catastrophic impacts of high-altitude EMP attack, uniquely among grid security threats?**

EEI Response:

The federal government is primarily responsible for preventing—or defending or retaliating against—the detonation of a high-altitude nuclear weapon over the continental United States. Preventing the proliferation of nuclear materials and components that could possibly be used to construct weaponry is a top priority for the international community. Signatories of the Nuclear Non-Proliferation Treaty pledged to prevent the spread of nuclear weapons and work toward disarmament. The most effective way to prevent a high-altitude EMP attack is for the international community to strictly limit access to key nuclear-explosive materials (high-enriched uranium and plutonium) required to make nuclear weapons. And, the U.S. military is responsible for other, more direct means of nuclear weapons defense or deterrence.

---

[2] Oak Ridge National Laboratory Report; Impacts of a Nominal Nuclear Electromagnetic Pulse on Electric Power Systems (ORNL/Sub/83-43374/2); April 1991, Section 8 (Conclusions); Subsection 8.2 MHD-EMP(E3); Page 66.

[3] See ORNL/Sub/83-43374/2; in this ORNL report the E3 component is described in Section 2.2, Page 8 by the term MHD-EMP.

[4] See ORNL/Sub/83-43374/2); Section 8 (Conclusions); Subsection 8.2 MHD-EMP(E3); Page 66.

That said, the federal government obviously is not solely responsible for addressing the impacts of an attack on the power grid. The protection of critical infrastructure is a shared responsibility. Through existing efforts, such as the Electricity Subsector Coordinating Council (ESCC), and with further research, such as the Electric Power Research Institute's (EPRI's) EMP Project, the electric power industry will continue to work with the government to identify, test, and implement EMP mitigation solutions and incident response plans and procedures.

Question 6:

EEI also states as EMP "facts":

> **"The debate over the cost to protect the electric grid from EMPs also ignores the reality that other sectors of the economy likely will be affected by a nuclear EMP attack, including other critical infrastructure sectors upon which the electric sector depends to generate or distribute electricity. It makes little sense to protect the electric grid while ignoring these other critical infrastructure sectors.**
>
> **The best risk mitigation for an EMP event, especially one as severe as a high-altitude nuclear explosion, is prevention. The prevention or preemption of such attacks is within the purview of the nation's law enforcement, military, and intelligence functions."**

a. **Does EEI support or oppose partial protection of the nation's electric grid against the "E3" high-altitude nuclear electromagnetic pulse (HEMP), such as could be accomplished with neutral ground blocking devices?**

EEI Response:

EEI supports hardware solutions that have been proven from an engineering standpoint that could help to protect grid assets from the effects of both GMD and EMP. It has not yet been proven whether the current generation of products can be applied effectively without negative impacts on normal grid operations.

The focus of the EPRI EMP Project will be to study failure rates of grid and communication assets as well as potential mitigation solutions. If EPRI's findings indicate effective mitigation solutions with no unintended consequences for hardening grid assets, the industry will work with all stakeholders, including Congress, FERC, state PUCs, DOE, and DHS on implementation.

b. **Does EEI take the position that all defense against nuclear EMP should be the sole responsibility of governmental entities?**

EEI Response:

EEI believes the federal government is primarily responsible for preventing the detonation of a high-altitude nuclear weapon over the continental United States. EEI also believes that the protection of critical infrastructure is a shared responsibility between the private sector and the government. The electric power industry works in close coordination with federal, state, and local governments on incident response plans and procedures for a range of threats that could impact the grid.

c. Is it the position of EEI that government defenses against nuclear EMP can be so effective that no degree of electric grid protection would be appropriate or cost-effective?

EEI Response:

As I mentioned in my testimony, the electric power industry has a history of working together to restore power after an incident through mutual assistance networks where workers from across the sector help affected companies. The electric power industry also has robust spare equipment sharing programs—like the Spare Transformer Equipment Program (STEP), SpareConnect, and the newly announced Grid Assurance program—to improve grid resilience no matter the threat.

The electric power industry exercises disaster response scenarios regularly, and has conducted four national-level incident response exercises (GridEx III, Clear Path IV, Cascadia Rising, and Cyber Guard) since November 2015. One of the recommendations from the GridEx III exercise conducted by NERC was to develop a cyber mutual assistance program to coordinate resources for companies affected by cyber incidents. EEI is leading this effort.

EEI would emphasize there are not enough resources in the world to protect against every threat in every location, but the electric power industry is working to prevent incidents from having long-term or devastating impacts. As an industry, we are committed to constantly improving the security posture of the sector as threats evolve.

Question 7:

EEI states as an EMP "fact":

> **"Many EMP mitigation techniques remain unproven and are potentially more expensive than claimed by their promoters, many of whom stand to benefit from their deployment. Further, placing blocking devices on the grid could have unintended consequences for an event that is relatively unlikely to happen. For instance, some mitigation measures to prevent damage from an EMP could actually reduce the effectiveness of measures to address GMDs, which occur much more frequently."**

a. What are the specific nuclear EMP mitigation measures that would "actually reduce the effectiveness of measures to address Geomagnetic Disturbance (GMD)"?

EEI Response:

This is a question that cannot be answered fully at this time given current technical knowledge about EMP mitigation measures. What is certain is that this is a concern for the industry and that EPRI is looking at this issue as part of its current EMP research project. EEI hopes this effort will better inform the owners and operators of power grid infrastructure, as well as policymakers, of any potential harmful impacts related to EMP mitigation. EEI plans to share and act on the EPRI findings once that research is complete. As has been suggested throughout these responses, assuming as fact that there is a "silver bullet" solution ignores the significant engineering challenges created by introducing new, untested mitigation.

b. **Have these purported effectiveness reductions been verified by real-world tests?**

EEI Response:

EEI and many power grid engineers believe that EMP mitigation "could" reduce the effectiveness of GMD mitigation, but the final answer to this question remains unknown at this time. EEI's comments reflect industry concerns, which we recognized at that time needed to be researched more fully. This work is now ongoing at EPRI. Once this work is completed, EEI plans to make any necessary adjustments to industry practices and public communications.

Question 8:

In rulemaking comments to FERC, EEI and other trade associations stated:

"The Trade Associations do not support the Commission's proposed directive for mandatory supply chain requirements because the Trade Associations do not share the Commission's views regarding a perceived gap in the mandatory Reliability Standards regarding supply chain risks for CIP and cybersecurity procurement."

Russian penetrations of the North American Grid, combined with proven security holes in many vendor products, have demonstrated major gaps in cyber supply chain security. For example, Juniper firewalls are designed for use by electric utilities, but this equipment has been successfully penetrated in the supply chain.

a. **Why does EEI oppose mandatory supply chain protections, including formal certification of vendor products to protect electric utility interests and those of the American public?**

EEI Response:

Securing the supply chain is a joint responsibility between electric power companies and suppliers. Electric companies are buyers and users of cyber products or assets (e.g., firewalls). Companies that make these products are responsible for the security of their technologies in the research, development, design, and manufacturing stages of the supply chain. Likewise, electric power companies have responsibility in the acquisition, delivery, integration, operations, retirement, and disposal stages, but some of this responsibility is shared with technology and service providers. The existing CIP version 5 cybersecurity requirements, which are mandatory for electric companies, address the risk in these stages. For more details, please see EEI's comments filed with FERC in docket No. RM15-14-000.

Question 9:

In rulemaking comments to FERC, EEI and other trade associations stated:

"The final rule should not adopt directives inconsistent with NERC's risk-based approach, which rightly recognizes that the same protections required for high and medium impact BES Cyber Systems are not warranted for low impact assets."

a. **Given the December 2015 cyberattack in Ukraine on so-called "low impact assets" (distribution facilities)—which knocked out power to about 225,000 people and could have been designed to cause permanent equipment damage—does EEI oppose mandatory cybersecurity protection for electric grid distribution facilities?**

EEI Response:

Protecting the power grid from cyber-attacks requires risk management. It is simply not possible to eliminate all risk, especially when the threat is posed by a determined adversary. In determining whether additional regulations are needed, regulators and policymakers must carefully examine the risk and prioritize risk reduction measures and the available resources. It should be noted, however, that Sec. 61003 of the FAST Act, referenced in Question 17, also provides DOE new authority to order measures to protect or restore the reliability of critical electric infrastructure or defense critical electric infrastructure during a grid security emergency, including an EMP or GMD.

In addition, distribution facilities are intrastate operations subject to state regulation, whereas interstate transmission facilities and electric power generation participating in wholesale power markets are subject to federal regulation. New regulations focused on intrastate operations would raise broader state and federal jurisdictional questions and create potential regulatory conflicts and confusion, potentially undermining their clarity and effectiveness. These factors should be carefully weighed by regulators and policymakers when evaluating the need for new regulations. Furthermore, the risk of a cascading event is generally lower, and it can be easier to isolate a problem in the case of an attack or failure involving distribution.

b. Is it the position of EEI that the public utility commissions of the fifty states should independently decide how to protect distribution facilities against cyberattack?

EEI Response:

Electric companies have the primary responsibility and technical expertise to decide how best to protect their local distribution facilities with regulatory oversight by independent state public utility commissions.

Question 10:

In rulemaking comments to FERC, EEI and other trade associations stated:

"In the NOPR, the Commission proposes to direct NERC to develop modifications to Reliability Standard CIP-006-6 to require protections for communication network components and data communicated between "all bulk electric system Control Centers." Although we agree that modifications seeking to address protections for communication network components and data communicated between Control Centers with high and medium impact BES Cyber Systems may improve the reliability of the bulk electric system, such modifications should not be extended to low impact Control Centers."

a. Given the December 2015 cyberattack in Ukraine on both control centers and electric grid substations that would be considered "low impact" under the NERC CIP standards, does EEI oppose mandatory cybersecurity protection for communications of "low-impact Control Centers" with substations?

EEI Response:

EEI does not oppose the Commission's directive issued on January 21, 2016 – Order No. 822. In this directive, FERC required NERC to modify the CIP standards to protect "communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers

that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."

Question 11:

The 2014 and 2015 cybersecurity attacks against the U.S. electric grid revealed targeting of so-called "low-impact Control Centers" precisely because such portals represent one of the most vulnerable ways to unbalance power flows and cause cascading outages.

a. **In light of actual cybersecurity experience in both Ukraine and the U.S., is it the position of EEI that such "low-impact Control Centers" should be exempt from mandatory cybersecurity regulation?**

EEI Response:

EEI members are currently implementing the CIP version 5 requirements (i.e., mandatory cybersecurity regulation) for low-impact Control Centers.

Question 12:

Please explain why electric utilities have opted to not install hardware devices to protect rotating equipment such as electricity generators and pipeline compressor motors against Aurora-type cyberattacks, even when the protective devices would be provided free of charge by the U.S. Department of Defense.

EEI Response:

EEI does not have specific knowledge or records regarding how companies may have mitigated vulnerable systems against Aurora-type cyber-attacks, given the confidentiality of such efforts.

More generally, vulnerabilities to an Aurora-type attack, as well as mitigation options, can vary depending on the configuration, installed hardware, and operating characteristics of affected systems. Security is also a key component to any protection against Aurora-type attacks. It should also be recognized that Bulk Electric System generators are subject to the regulatory NERC CIP Cyber Security Standards. Finally, mitigating against this type of vulnerability requires specific engineering and detailed analysis based on the particular system in question.

Following a NERC Alert concerning the Aurora vulnerability, electric companies provided information to NERC concerning the measures that they had taken or planned to mitigate the risk. The hardware mitigation device that this question refers to may assist in mitigating certain aspects of the Aurora vulnerability, but may also bring potentially negative operational impacts.

Question 13:

In rulemaking comments to FERC, EEI and other trade associations asserted that utilities should be able to preempt mandatory physical security requirements for critical grid facilities serving military bases:

> **"For example, should the Commission purport to delegate the power to add or subtract critical facilities under the criteria of the standard to the Department of Defense ("DOD"), would the DOD be prevented from adding a substation that serves what it deems a critical defense facility such as a military base, without regard to whether that facility meets applicability threshold under the proposed standard (based on the statutory standard), that the substation, if rendered inoperable or damaged could result in "instability, uncontrolled separation or Cascading within an Interconnection"? (CIP-014-1, R1). How would the Commission ensure that the**

DOD proposed additions (or subtractions) to an entity's list of covered facilities were within the parameters of the proposed standard and in fact complied with the underlying jurisdictional limitations of Section 215*? If the DOD did add a substation because it serves a military base and not because analysis shows that it could lead to instability, uncontrolled separation or cascading, what due process remedy would the Registered Entity owner of the substation have to dispute that addition?* (Emphasis added)"

a. **Given recent physical threats to electric grid facilities from ISIS and other terrorist organizations, does EEI oppose special protection for critical grid facilities serving military bases?**

EEI Response:

Vigilance against such threats is important, which is why EEI members use a variety of tools and coordination among the industry and with government partners. EEI member companies that serve military facilities coordinate closely with these facilities to evaluate the risk and ensure the appropriate protections are in place.

Question 14:

Data centers for U.S. Cyber Command, responsible for defense of the nation against cyberattack, rely on commercial electric grid power. Operations of the National Security Agency, responsible for intelligence on active cybersecurity threats, also depend on commercial electric grid power.

a. **Does EEI believe that utilities serving U.S. Cyber Command and the National Security Agency should have the right to dispute designation of these facilities as "critical" to the nation's defense?**

EEI Response:

EEI members that serve military facilities coordinate closely with these facilities to evaluate the risk and ensure the appropriate protections are in place.

Question 15:

Due to the difficulty of siting electric generation plants, including obtaining all necessary approvals and permits, it is common for multiple large generation plants to be in close physical proximity and therefore susceptible to a single physical attack. The current NERC Physical Security standard, CIP-014-1, exempts generation facilities from mandatory physical security standards.

a. **Given recent threats from ISIS and other terrorist groups, does EEI support or oppose mandatory standards for physical protection of electricity generation facilities?**

EEI Response:

The purpose of CIP-014 is to identify and protect facilities that "if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or

cascading within an Interconnection." In fact, the North American transmission system is planned such that the failure of no individual generation site can produce such widespread results.

EEI members address protection for all of their facilities in a variety of ways, including security, redundancy, and incident response and recovery measures. In managing risk to their facilities, EEI members must evaluate the threat, consequences, and likelihood of an attack, as well as the vulnerability and relative costs and benefits of risk management measures. If federal intelligence, defense, or law enforcement agencies are aware of specific threats to generation facilities, EEI encourages them to share this threat information with EEI and its members to appropriately manage this risk and take specific actions where warranted.

Question 16:

A draft of the "2016 EEI Corporate Goals" was published by the Huffington Post. Under "Grid Security and Business Continuity Issues," EEI states as a goal: "Ensure federal grid security legislation preserves the existing regulatory structure and facilitates industry-government coordination."

a. **Please explain why "preserving the existing regulatory structure" and facilitating "industry-government coordination" are important goals for EEI.**

EEI Response:

Under section 215 of the Federal Power Act, enacted by Congress in the Energy Policy Act of 2005, the electric power sector is subject to mandatory and enforceable reliability standards; these include regulations governing cyber and physical security, as well as geomagnetic disturbances, and other standards to help ensure reliable operation of the power grid.

NERC, as authorized by Congress, works with electric power industry experts, regional reliability entities, and government representatives to develop reliability and security standards that apply across the North American grid, including parts of Canada and Mexico. While NERC develops the standards, FERC must approve them and can direct NERC to make changes or develop new standards. Together, NERC and FERC have a shared responsibility to enforce these mandatory standards, helping to ensure a reliable energy grid.

It is important to preserve this carefully constructed international regulatory structure created by Congress because development of the most effective, highly technical standards affecting the operation of the grid requires a collaborative process that employs the expertise of asset owners and operators to ensure standards are technically and operationally sound and do not result in unintended consequences.

Question 17:

Under "Grid Security and Business Continuity Issues," EEI states as a 2016 goal: "Enhance FERC-NERC cooperation in order to avoid FERC collection of sensitive energy information." On December 4, 2015, President Obama signed into law the Fixing America's Surface Transportation (FAST) Act (Public Law 114-94), which established government protections for sensitive energy information.

a. Will EEI prevent FERC from collecting energy information that would allow FERC to review and approve appropriate regulatory standards for the electric utility industry?

EEI Response:

An April 2014 report by the DOE Inspector General raised an "immediate concern" that FERC staff had improperly disclosed information regarding critical energy infrastructure that had been furnished by electric companies to FERC officials. This raised significant concerns among owners and operators of critical infrastructure whose systems could have been compromised by this breach.

The FAST Act authority passed by Congress last year is a positive step to ensure sensitive information is better protected and that there are consequences for its improper disclosure. EEI is pleased that FERC has filed a Notice of Proposed Rulemaking to implement the new authority, and we look forward to working with the Commission to ensure Critical Energy Infrastructure Information is protected.

Finally, EEI will continue to work with FERC to ensure that the Commission has the information it needs to serve as an effective regulator.

○